Cisco Nexus 7000 Series NX-OS Quality of Service Configuration Guide

Last Modified: 2016-05-11

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

The preface contains the following sections:

Audience

This publication is for network administrators who configure and maintain Cisco Nexus devices.

Document Conventions

Note As part of our constant endeavor to remodel our documents to meet our customers' requirements, we have modified the manner in which we document configuration tasks. As a result of this, you may find a deviation in the style used to describe these tasks, with the newly included sections of the document following the new format.

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.

Convention	Description
{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.
`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.

This document uses the following conventions:

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Related Documentation for Cisco Nexus 7000 Series NX-OS Software

The entire Cisco Nexus 7000 Series NX-OS documentation set is available at the following URL:

https://www.cisco.com/c/en/us/support/switches/nexus-7000-series-switches/series.html#~tab-documents

Release Notes

The release notes are available at the following URL:

http://www.cisco.com/en/US/products/ps9402/prod_release_notes_list.html

Configuration Guides

These guides are available at the following URL:

http://www.cisco.com/en/US/products/ps9402/products_installation_and_configuration_guides_list.html

The documents in this category include:

- *Cisco Nexus 7000 Series NX-OS Configuration Examples*
- *Cisco Nexus 7000 Series NX-OS FabricPath Configuration Guide*
- *Cisco Nexus 7000 Series NX-OS Fundamentals Configuration Guide*
- *Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide*
- *Cisco Nexus 7000 Series NX-OS IP SLAs Configuration Guide*
- *Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide*
- *Cisco Nexus 7000 Series NX-OS LISP Configuration Guide*
- *Cisco Nexus 7000 Series NX-OS MPLS Configuration Guide*
- *Cisco Nexus 7000 Series NX-OS Multicast Routing Configuration Guide*
- *Cisco Nexus 7000 Series NX-OS OTV Configuration Guide*
- *Cisco Nexus 7000 Series NX-OS Quality of Service Configuration Guide*
- *Cisco Nexus 7000 Series NX-OS SAN Switching Guide*
- *Cisco Nexus 7000 Series NX-OS Security Configuration Guide*
- *Cisco Nexus 7000 Series NX-OS System Management Configuration Guide*
- *Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide*
- *Cisco Nexus 7000 Series NX-OS Verified Scalability Guide*
- *Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*
- *Cisco Nexus 7000 Series NX-OS Virtual Device Context Quick Start*
- *Cisco Nexus 7000 Series NX-OS OTV Quick Start Guide*
- *Cisco NX-OS FCoE Configuration Guide for Cisco Nexus 7000 and Cisco MDS 9500*
- *Cisco Nexus 2000 Series Fabric Extender Software Configuration Guide*

Command References

These guides are available at the following URL:

http://www.cisco.com/en/US/products/ps9402/prod_command_reference_list.html

The documents in this category include:

- *Cisco Nexus 7000 Series NX-OS Command Reference Master Index*
- *Cisco Nexus 7000 Series NX-OS FabricPath Command Reference*
- *Cisco Nexus 7000 Series NX-OS Fundamentals Command Reference*
- *Cisco Nexus 7000 Series NX-OS High Availability Command Reference*
- *Cisco Nexus 7000 Series NX-OS Interfaces Command Reference*
- *Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference*
- *Cisco Nexus 7000 Series NX-OS LISP Command Reference*
- *Cisco Nexus 7000 Series NX-OS MPLS Configuration Guide*
- *Cisco Nexus 7000 Series NX-OS Multicast Routing Command Reference*
- *Cisco Nexus 7000 Series NX-OS OTV Command Reference*
- *Cisco Nexus 7000 Series NX-OS Quality of Service Command Reference*
- *Cisco Nexus 7000 Series NX-OS SAN Switching Command Reference*
- *Cisco Nexus 7000 Series NX-OS Security Command Reference*
- *Cisco Nexus 7000 Series NX-OS System Management Command Reference*
- *Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference*
- *Cisco Nexus 7000 Series NX-OS Virtual Device Context Command Reference*
- *Cisco NX-OS FCoE Command Reference for Cisco Nexus 7000 and Cisco MDS 9500*

Other Software Documents

You can locate these documents starting at the following landing page:

https://www.cisco.com/c/en/us/support/switches/nexus-7000-series-switches/series.html#~tab-documents

- *Cisco Nexus 7000 Series NX-OS MIB Quick Reference*
- *Cisco Nexus 7000 Series NX-OS Software Upgrade and Downgrade Guide*
- *Cisco Nexus 7000 Series NX-OS Troubleshooting Guide*
- *Cisco NX-OS Licensing Guide*
- *Cisco NX-OS System Messages Reference*
- *Cisco NX-OS Interface User Guide*

Documentation Feedback

To provide technical feedback on this document, or to report an error or omission, please send your comments to: .

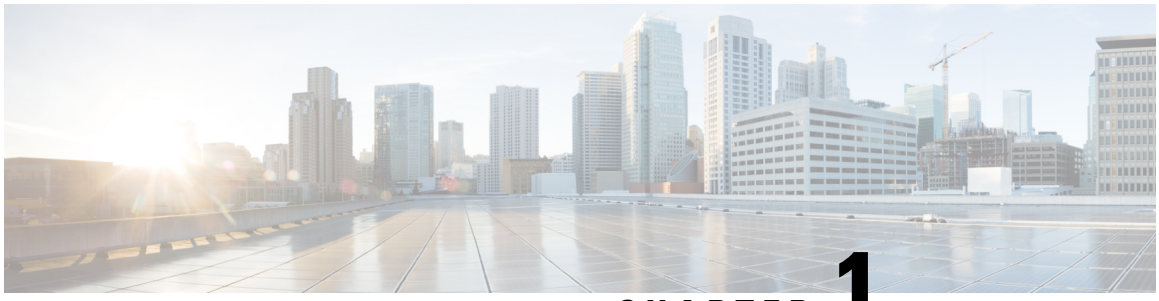
We appreciate your feedback.

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

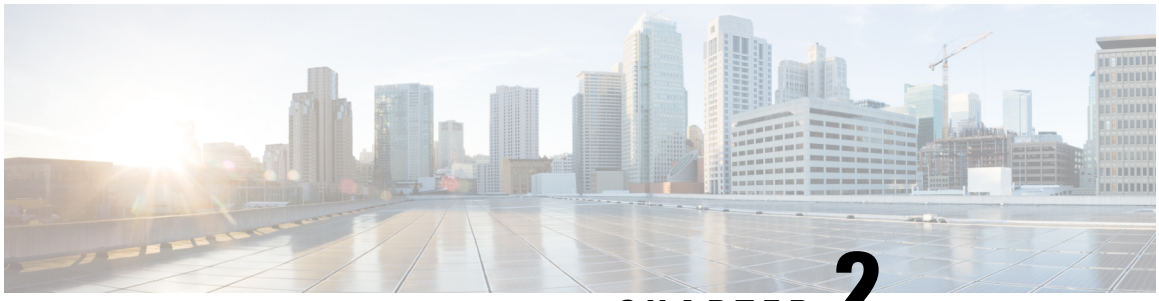
New and Changed Information

The table below summarizes the new and changed features for this document and shows the releases in which each feature is supported. Your software release might not support all the features in this document. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release.

Table 1: New and Changed QoS Features

Feature	Description	Changed in Release
Support for M3 modules	Support for M3 series modules.	7.3(0)DX(1)
Shared buffer queuing on the F3 Series modules	Support for shared memory buffer queues on the F3 Series modules only.	6.2(10)
Fabric QoS Mapping	The Fabric QoS Mapping feature allows copying the default configuration and modifying the copied system queues that perform flow control on fabric traffic within the Cisco NX-OS device.	6.2(2)
4q8q policy templates that support 8 egress queues	Four 4q8q policy templates that support eight egress queues on the Cisco Nexus 7710 switch and Cisco Nexus 7718 switch only.	6.2(2)
Local Policy-Based Routing (PBR)	You can now configure local policy-based routing.	6.2(2)
default-nq-8e-4q4q- policy template for F2 modules	The default-nq-8e-4q4q-policy template supports four ingress buffers.	6.1.3

Feature	Description	Changed in Release
DSCP mapping for F2 modules	Support for DSCP mapping for F2 modules .	6.1(1)
Network QoS policy	You can now configure a network qos policy, which defines the characteristics of each CoS that is applicable network wide, across virtual device contexts (VDCs), and switches.	5.1(1)
Priority flow control (PFC)	You can now configure PFC, which prevents frame loss that is due to congestion.	5.1(1)
Fabric Extender (FEX) support	You can now configure QoS policies on the FEX interfaces.	5.1(1)
QoS dynamic variable lists	The qos-dynamic variable lists already configured class-map and policy-map names.	4.2(1)
Support for Session Manager	Allows you to verify the configuration and required resources prior to committing them to the running configuration.	4.2(1)
Match IPv6 ACLs.	You can now match IPv6, as well as IPv4, addresses.	4.1(2)
Only same variable for mutation mapping	You can match only the same variable with different values for mutation mapping.	4.1(2)



CHAPTER 2

Overview

This chapter describes the configurable Cisco NX-OS quality of service (QoS) features on the Cisco NX-OS device.

QoS allows you to classify the network traffic, police and prioritize the traffic flow, and help avoid traffic congestion in a network.

Licensing Requirements

For a complete explanation of Cisco NX-OS licensing recommendations and how to obtain and apply licenses, see the *Cisco NX-OS Licensing Guide*.

Information 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 provide congestion avoidance. The control of traffic is based on the fields in the packets that flow through the system. You use the Modular QoS CLI (MQC) to create the traffic classes and policies of the QoS features.

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

- QoS policies include the policing feature and the marking features.
- Queuing policies use the queuing and scheduling features as well as a limited set of the marking feature.

Note The system-defined QoS features and values that are discussed in another chapter of this configuration guide apply globally to the entire switch and cannot be modified. For complete information on virtual device contexts (VDCs), see the Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide.

Caution Before you attempt a downgrade from Cisco NX-OS Release 5.2(x) or newer release to any release prior to Release 5.2(1), you should clear the QoS MIB and MPLS QoS defaults by using the clear qos mpls-snmp command. The downgrade might fail if the defaults are not cleared.

Before you downgrade from Cisco NX-OS Release 5.2(x) or 5.1(x) or newer release to Cisco NX-OS Release 5.0(x) or an earlier release, remove all system QoS and QoS policies configured on F-Series I/O modules. Use the **clear qos policies** command to remove the defaults for F-Series modules. An internal process failure can result if the QoS policies are not removed prior to the downgrade.

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 and outgoing 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 limiting, marking, or dropping packets.
3. Apply policies to a port, port channel, VLAN, or a 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.

Classification

You use classification to partition traffic into classes. You classify the traffic based on the port characteristics (class of service [CoS] field) or the packet header fields that include IP precedence, Differentiated Services Code Point (DSCP), Layer 2 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 IP precedence, DSCP and CoS, and internal labels that can be used in subsequent actions. Marking is used to identify the traffic type for policing, queuing, and scheduling traffic (only CoS is used in scheduling).

Mutation

Mutation is the changing of packet header QoS fields. You can map IP precedence, DSCP, or CoS values to all incoming or outgoing packets. You can use mutation in policies that contain policing commands, but you cannot use mutation in queuing and scheduling commands. You use configurable, user-defined table maps for mutation.

Policing

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

Three colors, or conditions, are determined by the policer depending on the data rate parameters supplied: conform (green), exceed (yellow), or violate (red). You can configure only one action for each condition. When the data rate exceeds the user-supplied values, packets are either marked down or dropped. You can define single-rate, dual-rate, and color-aware policers.

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. Color-aware policers assume that traffic has been previously marked with a color.

Queuing and Scheduling

The queuing and scheduling process allows you to control the bandwidth allocated to traffic classes, so 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 CoS field. The WRED algorithm allows you to perform proactive queue management to avoid traffic congestion.

You can schedule 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.

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 as well as a limited set of the marking objects.

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

The Cisco NX-OS device processes the QoS policies that you define based on whether they are applied to ingress or egress packets. The system performs actions for QoS policies only if you define them under the type **qos** service policies.

Note You can apply only ingress traffic actions for type QoS policies on Layer 2 interfaces. You can apply both ingress and egress traffic actions for type QoS policies on Layer 3 interfaces

Sequencing of Ingress Traffic Actions

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

1. Queuing and scheduling
2. Mutation
3. Classification
4. Marking
5. Policing

Sequencing of Egress Traffic Actions

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

1. Classification
2. Marking
3. Policing
4. Mutation
5. Queuing and scheduling

Note Mutation occurs much closer to the beginning of the traffic actions on the ingress packets, and any further classification and policing is based on the changed QoS values. Mutation occurs at the end of the traffic actions on the egress packets, right before 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.

Note For complete information on high availability, see the *Cisco Nexus 7000 Series NX-OS High Availability and Redundancy Guide*.

QoS Feature Configuration with MQC

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

Table 2: MQC Configuration Commands

MQC Command	Description
class-map	Defines a class map that represents a class of traffic.
table-map	Defines a table map that represents a mapping from one set of field values to another set of field values. You can reference a table map from a policy map.
policy-map	Defines a policy map that represents a set of policies to be applied to a set of class maps. Policy maps can reference table maps.

You can modify or delete MQC objects, except system-defined objects, when the objects are not associated with any interfaces. For information on system-defined MQC objects, see "Using Modular QoS CLI."

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

Table 3: Interface Command to Attach a Policy Map to an Interface

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

For information on how to use MQC, see "Using Modular QoS CLI."

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.

For information about monitoring QoS statistics, see "Monitoring QoS Statistics."

Default QoS Behavior

The QoS queuing features are enabled by default. Specific QoS-type features, 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 default settings for various interface modes is shown in the table below.

Trust DSCP/CoS by Default	Ingress	Egress (After Traffic is Routed)
SVI	CoS	DSCP
Routed Interface	DSCP	DSCP
Layer 2 Interface	CoS[1]	DSCP

[1] When the Layer 2 Interface is an access port, it is considered as no CoS. CoS is set to 0 in the case when access to the trunk interface with bridged traffic, even if DSCP bits are set.

Note When traffic is routed, the DSCP value is used (by default) to derive the egress queue. If the egress interface is the trunk, the CoS is derived from the DSCP value of the routed packet.

For more information on the system-defined, default queuing policies and the default values that apply to each interface, see “Using Modular QoS CLI.”

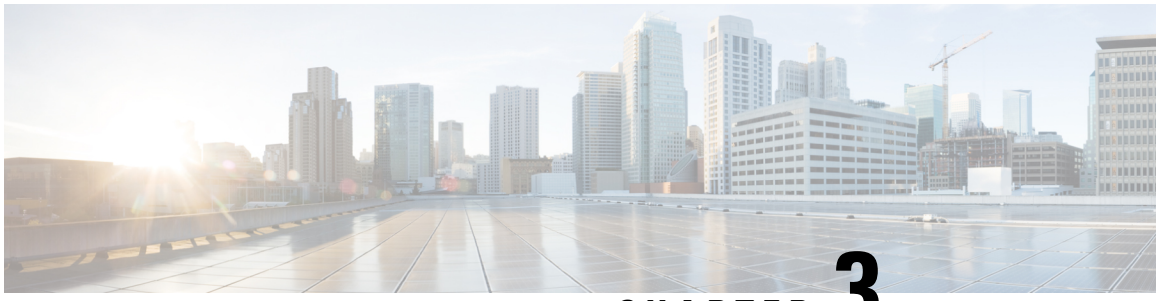
The device enables other QoS features, policing and marking, only when you apply a policy map to an interface.

QoS Policies on Fabric Extenders

The Cisco Nexus 2000 Series Fabric Extender (FEX) is a remote line card that you can connect to the Cisco Nexus 7000 Series switch. The FEX has 48 1-Gbps front-panel or server-facing ports, which are satellite ports. The FEX has four uplink ports that you can use to connect it to the Cisco Nexus 7000 Series switch. The four ports on the Cisco Nexus 7000 Series switch that connect to the uplink ports are fabric ports. Only QoS policies can be configured on the server-facing FEX ports. Currently, queuing on the FEX interfaces is not supported.

Starting with Cisco Nexus OS Release 6.2.(2), the configured MTU for the FEX ports is controlled by the network QoS policy. To change the MTU configured on the FEX ports, you must modify the network QoS policy to change when the fabric port MTU is also changed.

For more information on FEX, see the *Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 6.x*, *Cisco Nexus 7000 Series NX-OS Fundamentals Configuration Guide, Release 6.x*, and *Cisco Nexus 7000 Series NX-OS Fundamentals Command Reference*.



CHAPTER 3

Using Modular QoS CLI

This chapter describes how to configure Modular QoS CLI (MQC) objects that can be used for configuring QoS features using the Cisco NX-OS software.

Finding Feature Information

Your software release might not support all the features documented in this module. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the "New and Changed Information"chapter or the Feature History table in this chapter.

Information About MQC

MQC provides a language to define QoS policies.

For more information about MQC commands, see the *Cisco Nexus 7000 Series NX-OS Quality of Service Command Reference*.

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 and VLANs.

MQC provides three command types to define traffic classes and policies:

- class-map—Defines a class map that represents a class of traffic based on packet-matching criteria. Class maps are referenced in policy maps.

Note When you configure match all for a QoS class map by entering the **class-map type qos match-all** command, the match-all option does not work. Instead, the match criteria is always treated as match any.

- table-map—Defines a table map that represents a mapping from one set of packet field values to another set of packet fields. Table maps are referenced in policy maps.
- policy-map—Defines a policy map that represents a set of policies to be applied on a class-by-class basis to class maps.

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

- network qos—Defines the characteristics of CoS properties network wide (across switches and VDCs).
- 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.

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

On Fabric Extender (FEX) interfaces, you can configure only the type qos policies. However, you cannot configure the type qos policies that refer to classes that match with the access control lists (ACLs) that are configured for the FEX external interfaces.

The type queuing policies are currently not supported on FEX interfaces.

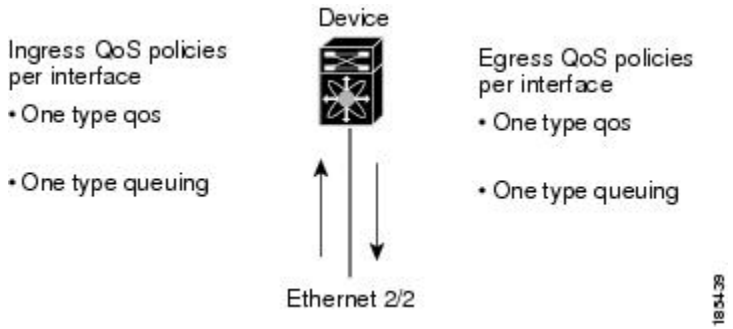
You can view all or individual values for MQC objects by using the **show table-map**, **show class-map**, and **show policy-map** commands.

Caution In interface configuration mode, the Cisco Nexus 7000 Series switch might accept QoS and ACL commands irrespective of the line card on which the interface host is up or down. However, you cannot enter interface submode when the line card is down because the Cisco Nexus 7000 Series switch does not accept any preconfiguration information.

Using an MQC Object

You configure QoS and queuing policies using the MQC class-map, policy-map, and table-map objects. You cannot use table maps in queuing policies. After you configure class maps and policy maps, you can attach one policy map of each type to each of the ingress or egress directions of an interface. The figure below lists the maximum QoS and queuing policies that you can define on each interface.

Figure 1: Maximum QoS Policies Per Interface



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 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. You use class-default to perform mutations (mutation is a method for translating QoS values in the packet header prior to traffic classification).

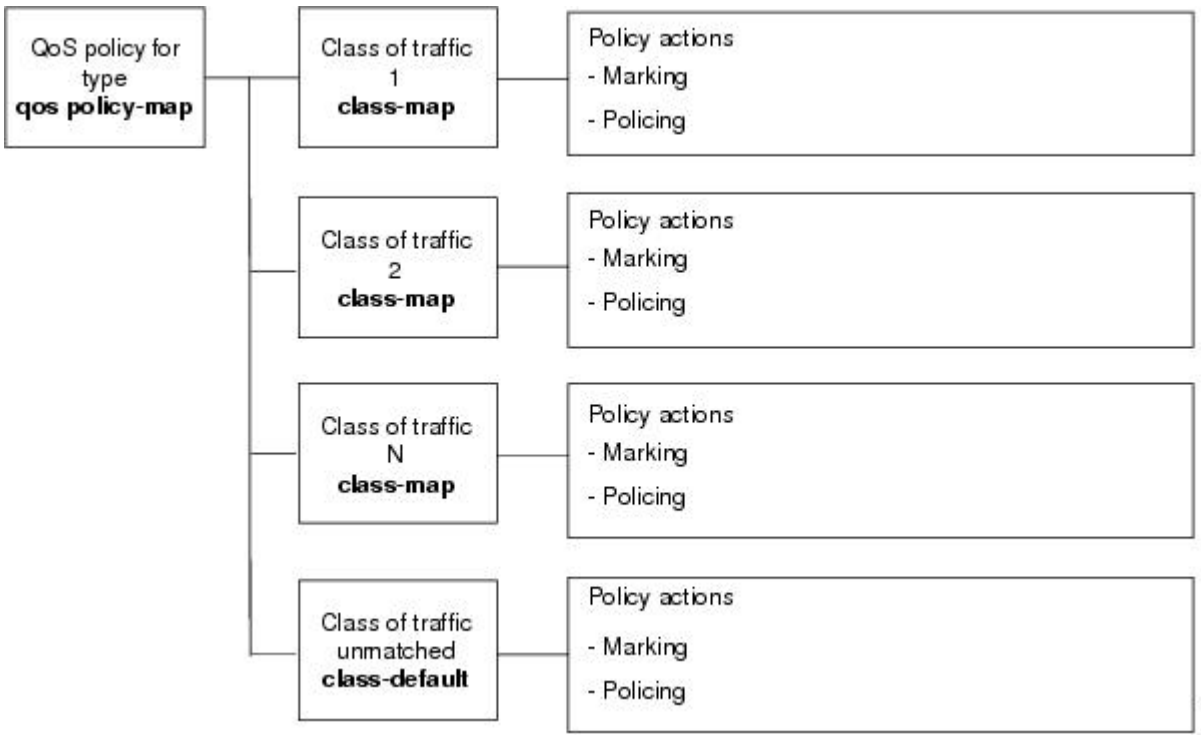
Note You can access user-defined MQC objects only in the VDC in which they were created. You can access the system-defined MQC objects in all VDCs.

Type qos Policies

You use type qos policies to mark, to apply mutations, to set the ingress port trust state, and to police packets.

The figure below shows the QoS policy structure with the associated MQC objects of type qos without mutation.

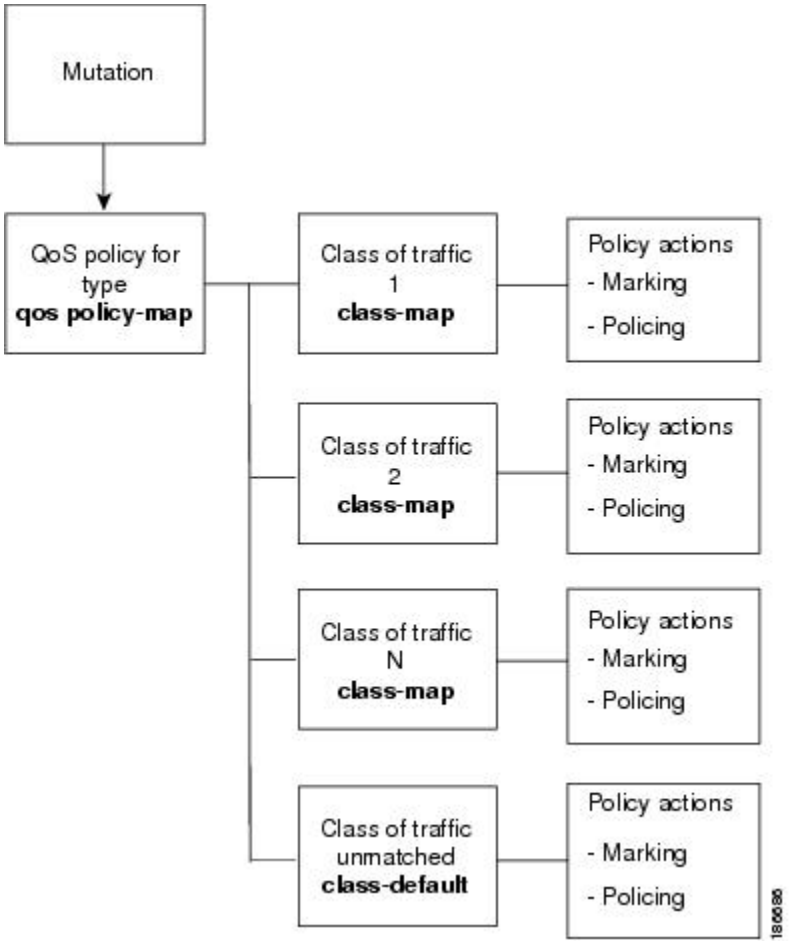
Figure 2: QoS Policy Diagram Showing Type qos MQC Object Usage Without Mutation



Note The MQC objects are shown in bold.

The figure below shows the QoS policy structure with mutation.

Figure 3: QoS Policy Diagram Showing Type qos MQC Object Usage with Mutation



Note The MQC objects are shown in bold.

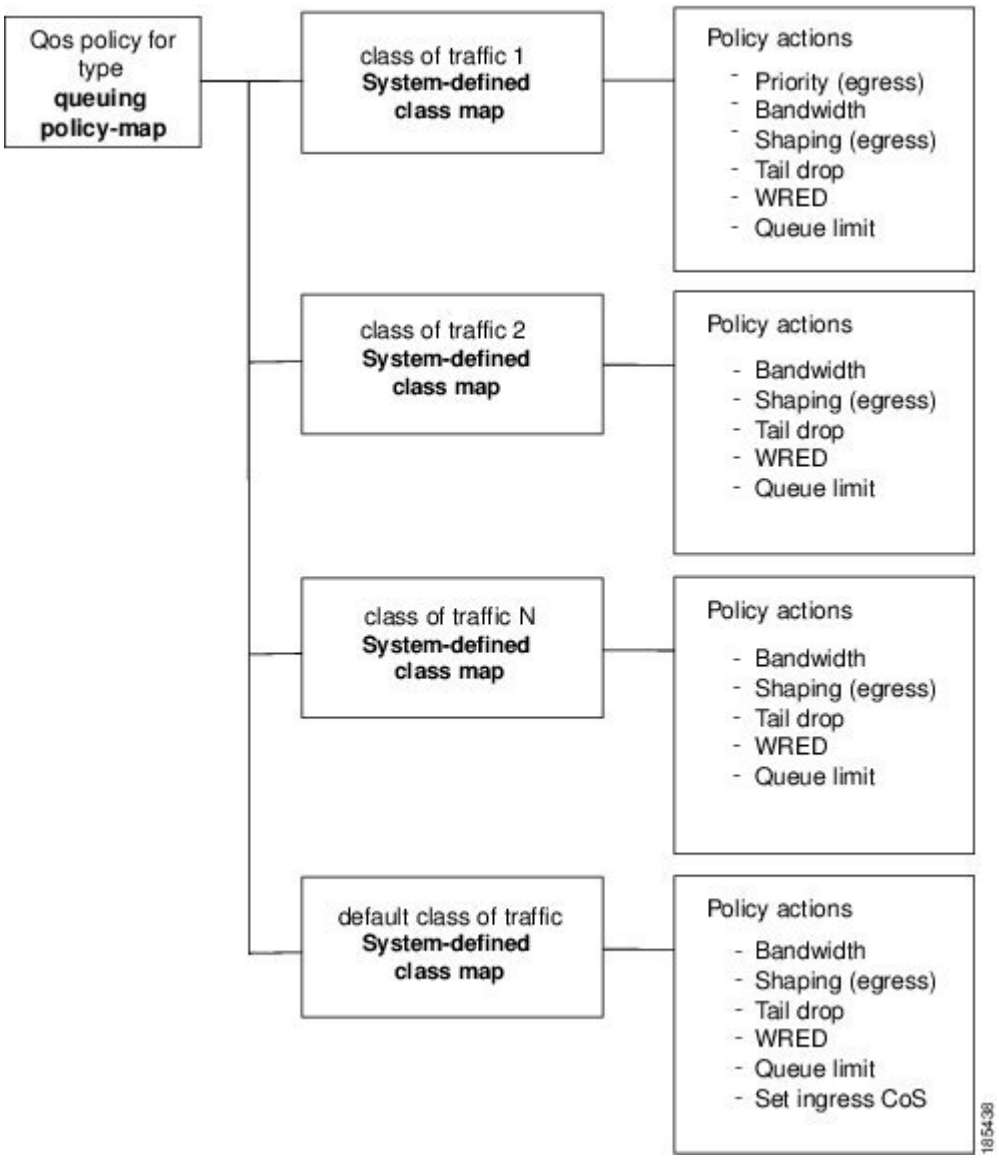
Type Queuing Policies

You use type queuing policies to mark, shape, and queue packets. Marking is limited to the CoS field and does not support the use of table maps.

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

Note MQC table-map objects cannot be used in policies of type queuing.

Figure 4: QoS Policy Diagram Showing Type Queuing MQC Object Usage



Note See "Queuing and Scheduling" for more information on configuring these parameters.

System-Defined MQC Objects

Note The system-defined MQC objects that are shown in the table below are the default. All of these values apply across all VDCs.

When you configure QoS features, and the system requests MQC objects, you can use one of the system-defined objects shown in the table below.

Table 4: System-Defined MQC Objects

Table	Description
System-Defined Type qos Class Maps	Type qos class maps
System-Defined Type queuing Class Maps	Type queuing class maps
System-Defined Table Maps	Table maps
System-Defined Queuing Policy Maps	Policy maps

Type qos class maps that are defined by the system are listed in the table below.

Note You cannot reference the conform-color-in, conform-color-out, exceed-color-in, or exceed-color-out class maps in a policy map.

Table 5: 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. You can use class-default for mutation.
conform-color-in	Type qos conform color class map in the input direction. This color-aware class map makes a policer color-aware for a conform action.
conform-color-out	Type qos conform color class map in the output direction. This color-aware class map makes a policer color-aware for a conform action.
exceed-color-in	Type qos exceed color class map in the input direction. This color-aware class map makes a policer color-aware for an exceed action.
exceed-color-out	Type qos exceed color class map in the output direction. This color-aware class map makes a policer color-aware for an exceed action.

Type queuing class maps that are defined by the system are listed in the table below.

Table 6: System-Defined Type queuing Class Maps

Class Map Queue Name	Description	Default CoS Values
1 Gigabit Module Ingress: 2 queues with 4 thresholds per queue		

Class Map Queue Name	Description	Default CoS Values
2q4t-in-q1	Ingress queue 1 of 2q4t type	5-7
2q4t-in-q-default	Ingress default queue of 2q4t type	0-4
1 Gigabit Module Egress: 1 strict priority queue and 3 normal queues with 4 thresholds per queue		
1p3q4t-out-pq1 [1]	Egress priority queue of 1p3q4t type	5-7
1p3q4t-out-q2	Egress queue 2 of 1p3q4t type	—
1p3q4t-out-q3	Egress queue 3 of 1p3q4t type	—
1p3q4t-out-q-default	Egress default queue of 1p3q4t type	0-4
10 Gigabit Module Ingress: 8 queues with 2 thresholds per queue		
8q2t-in-q1	Ingress queue 1 of 8q2t type	5-7
8q2t-in-q2	Ingress queue 2 of 8q2t type	—
8q2t-in-q3	Ingress queue 3 of 8q2t type	—
8q2t-in-q4	Ingress queue 4 of 8q2t type	—
8q2t-in-q5	Ingress queue 5 of 8q2t type	—
8q2t-in-q6	Ingress queue 6 of 8q2t type	—
8q2t-in-q7	Ingress queue 7 of 8q2t type	—
8q2t-in-q-default	Ingress default queue of 8q2t type	0-4
10 Gigabit Module Egress: 1 strict priority queue and 7 normal queues with 4 thresholds per queue		
1p7q4t-out-pq1 [1]	Egress priority queue of 1p7q4t type	5-7
1p7q4t-out-q2	Egress queue 2 of 1p7q4t type	—
1p7q4t-out-q3	Egress queue 3 of 1p7q4t type	—
1p7q4t-out-q4	Egress queue 4 of 1p7q4t type	—
1p7q4t-out-q5	Egress queue 5 of 1p7q4t type	—
1p7q4t-out-q6	Egress queue 6 of 1p7q4t type	—
1p7q4t-out-q7	Egress queue 7 of 1p7q4t type	—
1p7q4t-out-q-default	Egress default queue of 1p7q4t type	0-4

[1] These are either priority or normal queues. If you use the priority keyword in your configuration, these queues are used as priority queues. Otherwise, they are used as normal queues.

Table maps that are defined by the system are listed in the table below. The default mapping of values in the tables maps is contained in RFC 2597. These table maps are not configurable.

Table 7: System-Defined Table Maps

Table Map Name	Description
cir-markdown-map	Table map used to mark down packets that exceed the committed information rate (CIR). **Note** Enter the **show table-map** command to display the default mapping.
pir-markdown-map	Table map used to mark down packets that violate the peak information rate (PIR). **Note** Enter the **show table-map** command to display the default mapping.
cos-discard-class-map	Table map used to map the CoS value to the discard-class value.
cos-dscp-map	Table map used to map the CoS value to the DSCP value.
cos-precedence-map	Table map used to map the CoS value to the precedence value.
dscp-cos-map	Table map used to map the DSCP value to the CoS value.
dscp-precedence-map	Table map used to map the DSCP value to the precedence value.
dscp-discard-class-map	Table map used to map the DSCP value to the discard-class value.
precedence-dscp-map	Table map used to map the precedence value to the DSCP value.
precedence-cos-map	Table map used to map the precedence value to the CoS value.
precedence-discard-class-map	Table map used to map the precedence value to the discard-class value.
discard-class-cos-map	Table map used to map the discard-class value to the CoS value.
discard-class-prec-map	Table map used to map the discard-class value to the precedence value.
discard-class-dscp-map	Table map used to map the discard-class value to the DSCP value.

Policy maps that are defined by the system are listed in the table below.

Table 8: System-Defined Queuing Policy Maps

Queuing Policy Map Name	Description
default-in-policy	Input 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-in-policy class type queuing in-q1 queue-limit percent 50 bandwidth percent 80 class type queuing in-q-default queue-limit percent 50 bandwidth percent 20
default-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-out-policy class type queuing out-pq1 priority level 1 queue-limit percent 16 class type queuing out-q2 queue-limit percent 1 class type queuing out-q3 queue-limit percent 1 class type queuing out-q-default queue-limit percent 82 bandwidth remaining percent 25

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, table-map, or policy-map object, use the **no** form of the command that you used to create the object.

For the commands that you can use in the MQC object mode, see the following configuration chapters:

- Configuring Classification
- Configuring Marking
- Configuring Mutation Mapping
- Configuring Policing
- Configuring Queuing and Scheduling

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 listed in Table 6: System-Defined Type queuing Class Maps, on page 15

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **class-map** [**type qos**] [**match-any** | **match-all**] *class-map-name*	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. **Note** When you configure match all for a QoS class map by entering the class-map type qos match-all command, the match-all option does not work. Instead, the match criteria is always treated as match any.
Step 3	switch(config-cmap-qos)# **exit**	Exits class-map qos mode and enters global configuration mode.
Step 4	(Optional) switch(config)# **class-map** [**type qos**] {**conform-color-in** | **conform-color-out** | **exceed-color-in** | **exceed-color-out**}	Accesses the class map of type qos for one of the system-defined color maps, and then enters color-map mode. **Note** This command is only used when color-aware policing is required.
Step 5	switch(config-color-map)# **exit**	Exits color-map mode, and then enters global configuration mode.

	Command or Action	Purpose
Step 6	switch(config)# **class-map type queuing match-any** {*class-queuing-name* | *WORD*}	Creates or accesses the class map of type queuing, and then enters class-map queuing mode. Class queuing names are listed in Table 6: System-Defined Type queuing Class Maps, on page 15. **Note** The match on WORD is used for defining hierarchical class maps. The argument, WORD, is supported only on the F-Series Modules.
Step 7	switch(config-cmap-que)# **exit**	Exits class map queuing mode and enters global configuration mode.
Step 8	(Optional) switch(config)# **show class-map** [**type qos**] [*class-map-name* | **conform-color-in** | **conform-color-out** | **exceed-color-in** | **exceed-color-out**]	Displays information about all configured class maps or a selected class map of type qos.
Step 9	(Optional) switch(config)# **show class-map type queuing** [*class-queuing-name*]	Displays information about all configured class maps or a selected class map of type queuing. Class queuing names are listed in Table 6: System-Defined Type queuing Class Maps, on page 15.
Step 10	(Optional) switch(config)# **copy running-config startup-config**	Saves the running configuration to the startup configuration.

Configuring or Modifying a Table Map

You can create or modify a table map that you can reference in policy maps. For information on configuring table maps, see “Configuring Marking.”

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **table-map** *table-map-name*	Creates or accesses the table map and then enters table-map mode. Table map names can contain alphabetic, hyphen, or underscore characters, are case sensitive, and can be up to 40 characters.
Step 3	switch(config-tmap)# **exit**	Exits table-map mode and enters global configuration mode.

	Command or Action	Purpose
Step 4	switch(config)# **table-map** {**cir-markdown-map** | **pir-markdown-map**}	Accesses one of the system-defined markdown table maps, and then enters markdown-map mode.
Step 5	switch(config-mrkdwn-map)# **exit**	Exits table-map mode and enters global configuration mode.
Step 6	(Optional) switch(config)# **show table-map** [*table-map-name* | **cir-markdown-map** | **pir-markdown-map**}	Displays information about all configured table maps or a selected table map.
Step 7	(Optional) switch(config)# **copy running-config startup-config**	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.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **policy-map** [**type qos**] [**match-first**] {*qos-policy-map-name* | **qos-dynamic**}	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	switch(config-tmap)# **exit**	Exits policy-map mode and enters global configuration mode.
Step 4	switch(config)# **policy-map type queuing** [**match-first**] {*queuing-policy-map-name* | **qos-dynamic**}	Creates or accesses the policy map of type queuing and then enters policy-map mode. You can specify a policy-map name. Policy-map names can contain alphabetic, hyphen, or underscore characters, are case sensitive, and can be up to 40 characters.
Step 5	switch(config-tmap)# **exit**	Exits policy-map mode and enters global configuration mode.
Step 6	(Optional) switch(config)# **show policy-map** [**type qos**] [*policy-map-name* | **qos-dynamic**]	Displays information about all configured policy maps or a selected policy map of type qos.
Step 7	(Optional) switch(config)# **show policy-map type queuing** [*policy-map-name* | **qos-dynamic**]	Displays information about all configured policy maps or a selected policy map of type queuing.

	Command or Action	Purpose
Step 8	(Optional) switch(config)# **copy running-config startup-config**	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.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	**Option** / **Description** **class-map** [**type qos**] [**match-any** | **match-all**] *class-map-name* — 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. **table-map** *table-map-name* — Creates or accesses the table map, and then enters table-map mode. The table-map name can contain alphabetic, hyphen, or underscore characters, is case sensitive, and can be up to 40 characters **policy-map** [**type qos**] [**match-first**] {*qos-policy-map-name* | **qos-dynamic**} — 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.	

	Command or Action	Purpose
Step 3	switch(config-cmap)# **description** *string*	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	switch(config-cmap)# **exit**	Exits table-map mode and enters global configuration mode.
Step 5	(Optional) switch(config)# **copy running-config startup-config**	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-map-name* | **conform-color-in** | **conform-color-out** | **exceed-color-in** | **exceed-color-out**]	Displays information about all configured class maps or a selected class map of type qos.
show class-map type queuing [*class-queuing-name*]	Displays information about all configured class maps or a selected class map of type queuing. Class queuing names are listed in Table 6: System-Defined Type queuing Class Maps, on page 15.
show table-map [*table-map-name* | **cir-markdown-map** | **pir-markdown-map**]	Displays information about all configured table maps or a selected table map.
show policy-map [**type qos**] [*policy-map-name* | **qos-dynamic**]	Displays information about all configured policy maps or a selected policy map of type qos.
show policy-map type queuing [*policy-map-name* | **qos-dynamic**]	Displays information about all configured policy maps or a selected policy map of type queuing.

For detailed information about the fields in the output from these commands, see the *Cisco Nexus 7000 Series NX-OS Quality of Service Command Reference*.

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, VLANs, or tunnels as described in this section.

Note

- You must enable the tunnel feature by entering the **feature tunnel** command and configure the tunnel before you attach policies.
- On Fabric Extender (FEX) interfaces, you can configure only the type qos policies. However, you cannot configure the type qos policies that refer to classes that match with the access control lists (ACLs) that are configured for the FEX external interfaces.
- The type queuing policies are currently not supported on FEX interfaces.

The system-defined type queuing class maps (see Table 6: System-Defined Type queuing Class Maps, on page 15) are attached to each interface unless you specifically attach a different class map.

Note The device restricts QoS policies to one per interface per direction (ingress or egress) for each of the policy types qos and queuing.

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 policy type queuing is supported for each Layer 2 port- and Layer 2 port-channel interface in both the ingress and egress direction. Egress type qos policies are not allowed on Layer 2 port or Layer 2 port-channel interfaces.
- One ingress and one egress QoS policy are supported for each Layer 3 and Layer 3 port-channel interface.
- One ingress and one egress QoS policy are supported for each VLAN.
- One ingress and one egress queuing policy are supported for each Layer 2 port-, Layer 2 port-channel, Layer 3 port-, and Layer 3 port-channel interface.
- 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. For the default queuing policies, see Table 8: System-Defined Queuing Policy Maps, on page 18.

The interface where a QoS policy is applied is summarized in the table below. 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.

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, tunnel, or VLAN, use the **service-policy** command. You can specify whether the policies defined in the policy map are applied to the input or output stream of packets on the interface.

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

Attaching a QoS Policy Action to an Interface or Tunnel

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **interface** {[**ethernet** *slot/port-list*] | [**tunnel** *number-list*]}	Enters interface mode on the Ethernet or tunnel interface. • *slot/port-list* is a space-separated list of slots and ports. • *number-list* is a space-separated list of tunnels.
Step 3	switch(config-if)# **service-policy** [**type qos**] {**input** | **output**} {*policy-map-name*} [**no-stats**]	Adds the policy map to the input or output packets of an interface. Only one input policy and one output policy can be attached to an interface.
Step 4	switch(config-if)# **exit**	Exits interface configuration mode and enters global configuration mode.
Step 5	(Optional) switch(config)# **show policy-map** [**interface** *interface* | **vlan** *vlan_id*] [**input** | **output**] [**type qos** | **queuing**] [**class** [**type qos** | **queuing**] *class-map-name*]	Displays information about policy maps that are applied to all interfaces or the specified interface. You can limit what the device displays to input or output policies, qos or queuing polices, and to a specific class.

	Command or Action	Purpose
Step 6	(Optional) switch(config)# **copy running-config startup-config**	Saves the running configuration to the startup configuration.

Attaching a QoS Policy Action to a VLAN

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **vlan configuration** *vlan-id-list*	Enters VLAN configuration mode. *vlan-id-list* is a space-separated list of VLANs.
Step 3	switch(config-vlan-config)#**service-policy** [**type qos**] {**input** | **output**} {*policy-map-name*} [**no-stats**]	Adds the policy map to the input or output packets of a VLAN. Only one input policy and one output policy can be attached to a VLAN.
Step 4	switch(config-if)# **exit**	Exits VLAN configuration mode and enters global configuration mode.
Step 5	(Optional) switch(config)# **show policy-map** [**interface** *interface* | **vlan** *vlan_id*] [**input** | **output**] [**type qos** | **queuing**] [**class** [**type qos** | **queuing**] *class-map-name*]	Displays information about policy maps that are applied to all interfaces or the specified interface. You can limit what the device displays to input or output policies, qos or queuing polices, and to a specific class.
Step 6	(Optional) switch(config)# **copy running-config startup-config**	Saves the running configuration to the startup configuration.

Session Manager Support for QoS

Beginning in Cisco NX-OS Release 4.2, 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 7000 Series NX-OS System Management Configuration Guide, Release 6.x*.

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.

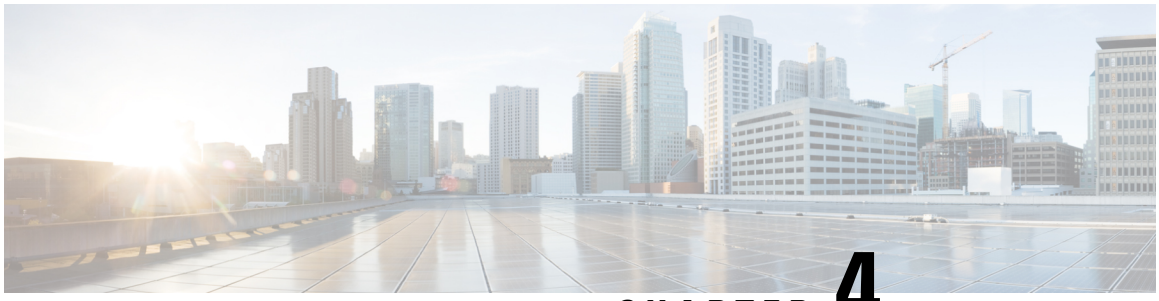
Feature History for Using Modular QoS CLI

The table below summarizes the new and changed features for this document and shows the releases in which each feature is supported. Your software release might not support all the features in this document. For the

latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release.

Table 9: Feature History for Modular QoS CLI

Feature Name	Release	Feature Information
No changes from Release 4.2(1)	5.1(1)	—
Support for Session Manager	4.2(1)	Allows you to verify the configuration and required resources prior to committing them to the running configuration.



CHAPTER 4

Configuring Classification

This chapter describes how to configure classification on the Cisco NX-OS device.

Finding Feature Information

Your software release might not support all the features documented in this module. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the "New and Changed Information"chapter or the Feature History table in this chapter.

Information 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 table below.

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.

Classification Criteria	Description
QoS group	Locally significant QoS values that can be manipulated and matched within the system. The range is from 1 to 126.
Discard class	Locally significant values that can be matched and manipulated within the system. The range is from 0 to 63.
ACL	IP ACL or MAC ACL name.
Protocol	Standard Layer 2 protocol such as Address Resolution Protocol (ARP) or Connectionless Network Service (CLNS).
Packet length	Size range of Layer 3 packet lengths.
IP RTP	Identify applications using Real-time Transport Protocol (RTP) by UDP port number range.
Class map	Criteria specified in a named class-map object.

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.

Some match criteria relate only to ingress or egress traffic. For example, the internal label QoS group has no meaning on ingress traffic because it has not yet been assigned a value.

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.

When you configure match all for a QoS class map by entering the **class-map type qos match-all** command, the match-all option does not work. Instead, the match criteria is always treated as match any.

You can reuse class maps within the same virtual device context (VDC) when defining the QoS policies for different interfaces that process the same types of traffic.

Note For more information on class maps, see “Using Modular QoS CLI”.

Prerequisites for Classification

Classification has the following prerequisites:

- You must be familiar with the concepts in “Using Modular QoS CLI”.

- You are logged on to the switch.
- You are in the correct VDC. A VDC is a logical representation of a set of system resources. You can use the **switchto vdc** command with a VDC number.

Guidelines and Limitations

Classification has the following configuration guidelines and limitations:

- You can specify a maximum of 1024 match criteria in a class map.
- You can configure a maximum of 4096 classes for use in a single policy map.
- When you match on an ACL, the only other match you can specify is the Layer 3 packet length in a match-all class.
- 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.
- You can classify traffic on Layer 2 ports based on either the port policy or VLAN policy of the incoming packet but not both. Either the port policy or the VLAN policy takes effect but not both. If both are present, the device acts on the port policy and ignores the VLAN policy.
- The **match cos** command is not supported in the egress direction.
- When you configure an access-list (ACL) using the **fragments deny-all** command and reference that ACL in a quality of service (QOS) policy, the fragments are dropped. To avoid this fragments droppage, use the **fragments permit-all**command. This will ensure smooth traffic and fragments are not dropped and the defined action in the QOS policy is performed.
- If a QoS policy is configured with one type of match criteria, a different type of match criteria cannot be used. The following error message will be returned:

```
ERROR: Unable to perform the action due to incompatibility:
Module 1, 2, 3, 4, 5, 6, 7, 8, 11, 12, 13, 14, 15, 16, 17, 18 returned status
"Policies with classes containing combined 'match dscp', 'match cos',
'match precedence' or 'match qos-group' are not supported.
Only the same match type is supported between classes.
```

- When you display the queuing statistics, the statistics for cbqosmib is shown per action, not per class level.
- Queuing cbqosmib will only be pulled when the following actions are configured: queue-limit, random-detect, bandwidth, and priority.
- For F1 module proxy-forwarded traffic, ACL classification is matched against the layer 3 protocols shown in the following table.
- **show policy-map interface** *[interface type]* **type queuing** uses L2 MTU (Frame length) and counts as a full packet length.
- **show policy-map interface** *[interface type]* **type qos** uses L3 MTU (Packet length).

Table 10: Protocol Number and Associated Layer 3 Protocol

Protocol Number	Layer 3 Protocol
1	ICMP
2	IGMP
4	IPv4 Encapsulation
6	TCP
17	UDP

Note Layer 3 protocols not listed in the table are classified as protocol number 4 (IPv4 Encapsulation).

Configuring Traffic Classes

Configuring ACL Classification

Note The device does not support the **no** form of the **match access-group name** command.

You can classify traffic by matching packets based on existing ACLs. The permit and deny ACL keywords are ignored in the matching. QoS does not use the permit-deny functions of ACLs. You can classify by either IPv4 or IPv6.

Support is available for controlling deny access control entry ([**no**] **hardware access-list allow deny ace**) in the CLI. For more information about this support, see the *Cisco Nexus 7000 Series NX-OS Security Configuration Guide*.

Note Tunneled IP packets are matched unless the tunneling protocol is also IP, and then the match applies to the outer IP header and not the encapsulated IP header.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **class-map** [**type qos**] [**match-any** | **match-all**] *class-map-name*	Creates or accesses the class map named class-map-name and enters class-map mode. The *class map name* can contain alphabetic,

	Command or Action	Purpose
		hyphen, or underscore characters, is case sensitive, and can be up to 40 characters.
Step 3	switch(config-cmap-qos)# **match access-group name** *acl-name*	Configures the traffic class by matching packets based on the acl-name. The **permit** and **deny** ACL keywords are ignored in the matching. The device does not support the **no** form of this command.

Example

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

```
switch# show class-map class_acl
```

Configuring a Deny ACE

You can configure the device to support deny access control entries (ACEs) in a sequence for the following sequence-based features: VACL, policy-based routing (PBR), and QoS. When deny ACEs are enabled, the traffic that matches a deny ACE (an ACL rule with the **deny** keyword) in a class-map-acl is recursively matched against subsequent class-map-acls until it hits a permit ACE.

Before you begin

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# [**no**] **hardware access-list allow deny ace**	Enables support for deny ACEs in a sequence.
Step 3	(Optional) switch(config)# **show running-config aclmgr**	Displays the ACL configuration.
Step 4	(Optional) switch(config)# **copy running-config startup-config**	Saves this configuration change.

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 table below:

Table 11: Standard DSCP Values

Value	List of DSCP Values
af11	AF11 dscp (001010)—decimal value 10
af12	AF12 dscp (001100)—decimal value 12
af12	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
af31	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
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 Tunneled IP packets are matched unless the tunneling protocol is also IP, and the match applies to the outer IP header and not the encapsulated IP header.

Procedure

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

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 table below shows the precedence values.

Table 12: Precedence Values

Value	List of Precedence Values
0-7	IP precedence value
critical	Critical precedence (5)
flash	Flash precedence (3)

Value	List of Precedence Values
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)

Note Tunneled IP packets are matched unless the tunneling protocol is also IP, and the match applies to the outer IP header and not the encapsulated IP header.

Procedure

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

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. For more information, see the "Configuring ACL Classification" section.

You can classify traffic based on the protocol arguments described in the table below.

Table 13: match Command Protocol Arguments

Argument	Description
arp	Address Resolution Protocol (ARP)
bridging	Bridging
cdp	Cisco Discovery Protocol (CDP)
clns	Connectionless Network Service (CLNS)
clns_es	CLNS End Systems
clns_is	CLNS Intermediate System
dhcp	Dynamic Host Configuration (DHCP)
isis	Intermediate system to intermediate system (IS-IS)
ldp	Label Distribution Protocol (LDP)
netbios	NetBIOS Extended User Interface (NetBEUI)

A maximum of eight different protocols (in the table above) can be matched at a time.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **class-map** [**type qos**] [**match-any** | **match-all**] *class-map-name*	Creates or accesses the class map named class-map-name and enters class-map mode. The *class map name* can contain alphabetic, hyphen, or underscore characters, is case sensitive, and can be up to 40 characters.
Step 3	switch(config-cmap-qos)# **match** [**not**] **protocol** {**arp** | **bridging** | **clns** | **clns_is** | **dhcp** | **isis** | **netbios** | **cdp** | **clns_es** | **ldp**}	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	switch(config-cmap-qos)# **exit**	Exits global class-map queuing mode, and enters configuration mode.
Step 5	(Optional) switch(config)# **copy running-config startup-config**	Saves this configuration change.

Example

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

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

Configuring QoS Group Classification

You can classify traffic based on the value of the QoS group internal label, which is not part of the packet payload or any packet header. You can set the value of the QoS group within a policy map by using the **set qos-group** command as described in the "Configuring QoS Group Marking" section.

Note You match on the QoS group only in egress policies because its value is undefined until you set it in an ingress policy.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **class-map** [**type qos**] [**match-any** | **match-all**] *class-map-name*	Creates or accesses the class map named class-map-name and enters class-map mode. The *class map name* can contain alphabetic, hyphen, or underscore characters, is case sensitive, and can be up to 40 characters.
Step 3	switch(config-cmap-qos)# **match** [**not**] **qos-group** *multi-range-qos-group-values*	Configures the traffic class by matching packets based on a list of QoS group values. Values can range from 1 to 126. Use the **not** keyword to match on values that do not match the specified range.
Step 4	switch(config-cmap-qos)# **exit**	Exits global class-map queuing mode, and enters configuration mode.
Step 5	(Optional) switch(config)# **copy running-config startup-config**	Saves this configuration change.

Example

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

```
switch# show class-map class_qos_group
```

Configuring Discard Class Classification

You can classify traffic based on the value of the discard class internal label, which is not part of the packet payload or any packet header. You can set the value of the discard class within a policy map using the **set discard-class** command as described in the "Configuring Discard Class Marking" section.

You match on the discard class only in egress policies because its value is undefined until you set it in an ingress policy.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **class-map** [**type qos**] [**match-any** | **match-all**] *class-map-name*	Creates or accesses the class map named class-map-name and enters class-map mode. The *class map name* can contain alphabetic, hyphen, or underscore characters, is case sensitive, and can be up to 40 characters.
Step 3	switch(config-cmap-qos)# **match** [**not**] **discard-class** *multi-range-discard-class-values*	Configures the traffic class by matching packets based on the list of discard-class values. Values can range from 0 to 63. The default discard class value is 0. Use the **not** keyword to match on values that do not match the specified range.
Step 4	switch(config-cmap-qos)# **exit**	Exits global class-map queuing mode, and enters configuration mode.
Step 5	(Optional) switch(config)# **copy running-config startup-config**	Saves this configuration change.

Example

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

```
switch# show class-map class_discard_class
```

Configuring Layer 3 Packet Length Classification

You can classify Layer 3 traffic based on various packet lengths.

Note This feature is designed for IP packets only.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **class-map** [**type qos**] [**match-any** | **match-all**] *class-map-name*	Creates or accesses the class map named class-map-name and enters class-map mode. The *class map name* can contain alphabetic, hyphen, or underscore characters, is case sensitive, and can be up to 40 characters.
Step 3	switch(config-cmap-qos)# **match** [**not**] **packet length** *packet-length-list*	Configures the traffic class by matching packets based on various packet lengths. Values can range from 1 to 9198. Use the **not** keyword to match on values that do not match the specified range.
Step 4	switch(config-cmap-qos)# **exit**	Exits global class-map queuing mode, and enters configuration mode.
Step 5	(Optional) switch(config)# **copy running-config startup-config**	Saves this configuration change.

Example

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

```
switch# show class-map class_packet_length
```

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.

Note The **match cos** command is not supported in the egress direction.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **class-map** [**type qos**] [**match-any** | **match-all**] *class-map-name*	Creates or accesses the class map named class-map-name and enters class-map mode. The *class map name* can contain alphabetic,

	Command or Action	Purpose
		hyphen, or underscore characters, is case sensitive, and can be up to 40 characters.
Step 3	switch(config-cmap-qos)# **match** [**not**] **cos** *cos-list*	Configures the traffic class by matching packets based on 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.
Step 4	switch(config-cmap-qos)# **exit**	Exits global class-map queuing mode, and enters configuration mode.
Step 5	(Optional) switch(config)# **copy running-config startup-config**	Saves this configuration change.

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.

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

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **class-map** [**type qos**] [**match-any** | **match-all**] *class-map-name*	Creates or accesses the class map named class-map-name and enters class-map mode. The *class map name* can contain alphabetic, hyphen, or underscore characters, is case sensitive, and can be up to 40 characters.
Step 3	switch(config-cmap-qos)# **match** [**not**] **ip rtp** *udp-port-value*	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.

	Command or Action	Purpose
		Use the **not** keyword to match on values that do not match the specified range.
Step 4	switch(config-cmap-qos)# **exit**	Exits global class-map queuing mode, and enters configuration mode.
Step 5	(Optional) switch(config)# **copy running-config startup-config**	Saves this configuration change.

Example

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

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

Configuring Class Map Classification

You must create a referenced class map prior to its reference. You can configure only one level of nesting of class maps. You cannot reference a class map that references another class map.

Before you delete a referenced class map, you should delete all references to that class map.

You can classify traffic based on the match criteria in another class map. You can reference the same class map in multiple policies.

Follow these guidelines while configuring the class-map classification:

- To perform a logical OR with the class map specified in the **match class-map** command, use the **match-any** keyword. The **match-any** or **match-all** specification of the matched class map is ignored.
- To perform a logical AND with the class map specified in the **match class-map** command, use the **match-all** keyword. The **match-any** or **match-all** specification of the matched class map is ignored.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **class-map** [**type qos**] [**match-any** | **match-all**] *class-map-name*	Creates or accesses the class map named class-map-name and enters class-map mode. The *class map name* can contain alphabetic, hyphen, or underscore characters, is case sensitive, and can be up to 40 characters.
Step 3	switch(config-cmap-qos)# **match** [**not**] **class-map** *class-map-name*	Configures the traffic class by matching packets based on the match criteria in another class map. Because **match-all** is the default for the **class-map** command, the match criteria specified in class_map3 are ANDed with the match criteria in class_class_map.

	Command or Action	Purpose
		Use the **not** keyword to match on values that do not match the specified range.
Step 4	switch(config-cmap-qos)# **exit**	Exits global class-map queuing mode, and enters configuration mode.
Step 5	(Optional) switch(config)# **copy running-config startup-config**	Saves this configuration change.

Example

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

```
switch# show class-map class_class_map
```

Verifying the Classification Configuration

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

```
switch# show class-map
...
```

Configuration Examples for Classification

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

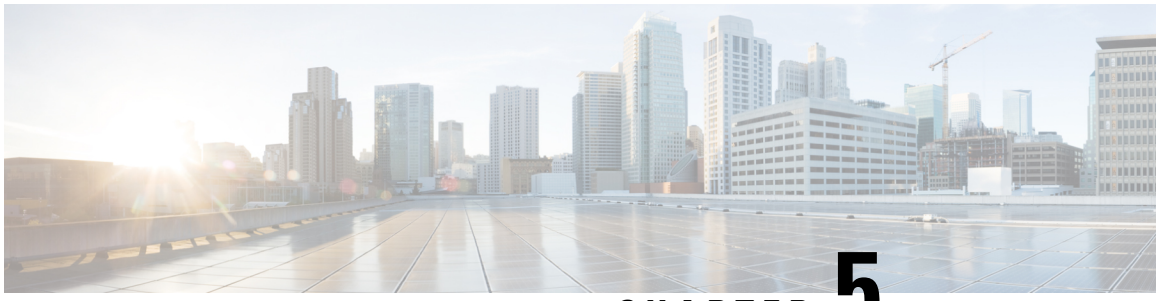
```
class-map class_dscp
  match dscp af21, af32
  exit
class-map class_cos
  match cos 4, 5-6
  exit
```

Feature History for Classification

The table below summarizes the new and changed features for this document and shows the releases in which each feature is supported. Your software release might not support all the features in this document. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release.

Table 14: Feature History for Classification

Feature Name	Release	Feature Information
No changes from Release 4.2(1)	5.1(1)	—
Classification	4.2(1)	You can now match IPv4 and IPv6 ACLs.



CHAPTER 5

Configuring Marking

This chapter describes how to configure the marking features on the Cisco NX-OS device that you can use to define the class of traffic to which the packet belongs.

Finding Feature Information

Your software release might not support all the features documented in this module. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the "New and Changed Information"chapter or the Feature History table in this chapter.

Information 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 CoS in Layer 2, and IP precedence and Differentiated Service Code Point (DSCP) in Layer 3. The QoS group and discard class are two labels local to the system that you can assign intermediate marking values. You can use these two labels to determine the final values marked in a packet.

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 table below.

Table 15: Configurable Marking Features

Marking Feature	Description
DSCP	Layer 3 DSCP. **Note** If you manipulate this **dscp value**, you cannot manipulate **discard class** values, and vice-versa.
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.
CoS	Layer 2 class of service (CoS).
QoS group	Locally significant QoS values that can be manipulated and matched within the system. The range is from 1 to 126.
Discard class	Locally significant values that can be matched and manipulated within the system. The range is from 0 to 63. If you manipulate this **discard class** value, you cannot manipulate **dscp values** and vice-versa.
Ingress and egress ports	Status of the marking applies to incoming or outgoing packets.
Using table maps	Method to use table maps for marking.

Unless noted as a restriction, you can apply marking features to both incoming and outgoing packets.

Prerequisites for Marking

Marking has the following prerequisites:

- You must be familiar with Using Modular QoS CLI, on page 9
- You are logged on to the switch.
- You are in the correct VDC. A VDC is a logical representation of a set of system resources. You can use the **switchto vdc** command with a VDC number.

Guidelines and Limitations

Marking has the following configuration guidelines and limitations:

- The **set cos** command can only be used in ingress policies when no other **set** commands are used for the same packet for egress.
- The **set qos-group** command can only be used in ingress policies.
- The **set discard-class** command can only be used in ingress policies.
- When PIM is enabled on the switch virtual interface (SVI), you cannot mark the Layer 2 switched multicast traffic on that VLAN.
- Egress QoS policies on Layer 2 ports are not supported on VDCs of any module type.
- A VLAN configuration with an egress QoS policy is not supported on VDCs that consist of F1 modules or any module plus an F1 module. However, a VLAN configuration with an egress QoS policy is supported on VDCs of the following module types:
  - M1 and/or M2 plus an F2e
  - M1
  - M2 and F3
  - M3 and F3
  - F2 and/or F2e
  - F3
- Egress policies on VLAN configurations do not support set match on CoS.
- Egress policies on VLAN configurations do not support set QoS group or discard class.
- Proxy-routed marking from F1 and/or F2e modules to M modules is not supported on the Layer 2 ingress port. However, marking that is applied under the VLAN is supported on the Layer 2 ingress port.
- To achieve scalability with remarking QoS policy on large number of interfaces, disable the QoS statistics on policy level. Enter the **no qos statistics** command, which disables global statistics, or enter the **service-policy type qos output DSCP no-stats** command per policy. The scalability configuration will not exist if policers are used.

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.

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

Note If you configure this value, you cannot configure the discard-class value (see the "Configuring Discard Class Marking" section).

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 table below.

Table 16: Standard DSCP Values

Value	List of DSCP Values
af11	AF11 dscp (001010)—decimal value 10
af12	AF12 dscp (001100)—decimal value 12
af12	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
af31	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
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

Value	List of DSCP Values
cs7	CS7 (precedence 7) dscp (111000)—decimal value 56
default	Default dscp (000000)—decimal value 0
ef	EF dscp (101110)—decimal value 46

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **policy-map** [**type qos**] [**match-first**] {*qos-policy-map-name* | **qos-dynamic**}	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	switch(config-pmap)# **class** [**type qos**] {*class-map-name* | **qos-dynamic** | **class-default**} [**insert-before** *before-class-map-name*]	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	switch(config-pmap-c-qos)# **set dscp** *dscp-value*	Sets the DSCP value to *dscp-value*. Standard values are shown in the table above. 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.

The table below shows the precedence values.

Table 17: 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)

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **policy-map** [**type qos**] [**match-first**] {*qos-policy-map-name* | **qos-dynamic**}	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	switch(config-pmap-qos)# **class** [**type qos**] {*class-map-name* | **qos-dynamic** | **class-default**} [**insert-before** *before-class-map-name*]	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	switch(config-pmap-c-qos)# **set precedence** *precedence-value*	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 table above.

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.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **policy-map** [**type qos**] [**match-first**] {*qos-policy-map-name* | **qos-dynamic**}	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	switch(config-pmap-qos)# **class** [**type qos**] {*class-map-name* | **qos-dynamic** | **class-default**} [**insert-before** *before-class-map-name*]	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	switch(config-pmap-c-qos)# **set cos** *cos-value*	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 QoS Group Marking

You can set the value of the internal label QoS group, which is only locally significant. You can reference this value in subsequent policy actions or classify traffic that is referenced in egress policies by using the **match qos-group** class-map command.

Note You can set the QoS group only in ingress policies.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **policy-map** [**type qos**] [**match-first**] {*qos-policy-map-name* | **qos-dynamic**}	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	switch(config-pmap-qos)# **class** [**type qos**] {*class-map-name* | **qos-dynamic** | **class-default**} [**insert-before** *before-class-map-name*]	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	switch(config-pmap-c-qos)# **set qos-group** *qos-group-value*	Sets the QoS group value to *qos-group-value*. The value can range from 1 to 126.

Example

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

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

Configuring Discard Class Marking

If you configure this value, you cannot configure the DSCP value. See the “Configuring DSCP Marking” section.

You can set the value of the internal label discard class, which is locally significant only. You can reference this value in subsequent policy actions or classify traffic that is referenced in egress policies by using the **match discard-class** class-map command.

Note You can set the discard class only in ingress policies.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **policy-map** [**type qos**] [**match-first**] {*qos-policy-map-name* | **qos-dynamic**}	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	switch(config-pmap-qos)# **class** [**type qos**] {*class-map-name* | **qos-dynamic** | **class-default**} [**insert-before** *before-class-map-name*]	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	switch(config-pmap-c-qos)# **set discard-class** *qos-group-value*	Sets the discard class value to *discard-class-value*. The value can range from 0 to 63. **Note** For information on using table maps with marking, see the "Configuring Marking Using Table Maps" section.

Example

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

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

Configuring Ingress and Egress Marking

You can apply the marking instructions in a QoS policy map to ingress or egress packets by attaching that QoS policy map to an interface. To select ingress or egress, you specify either the **input** or **output** keyword in the **service-policy** command. For detailed instructions, see the "Attaching and Detaching a QoS Policy Action" section.

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.
- If the default policy-map policy is used, DSCP maps to a relevant CoS value and the queuing works correctly.
- If a customer policy is used, you must manually set the DSCP value to map to a CoS value so that the traffic is queued to the correct queue.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **policy-map** [**type qos**] [**match-first**] {*qos-policy-map-name* | **qos-dynamic**}	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	switch(config-pmap-qos)# **class** [**type qos**] {*class-map-name* | **qos-dynamic** | **class-default**} [**insert-before** *before-class-map-name*]	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	switch(config-pmap-c-qos)# **set dscp** *dscp-value*	Sets the DSCP value to *dscp-value*. Valid values are shown in Table 16: Standard DSCP Values, on page 48.
Step 5	switch(config-pmap-c-qos)# **exit**	Returns to policy-map configuration mode.
Step 6	switch(config-pmap-qos)# **class** [**type qos**] {*class-map-name* | **qos-dynamic** | **class-default**} [**insert-before** *before-class-map-name*]	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 7	switch(config-pmap-c-qos)# **set dscp** *dscp-value*	Sets the DSCP value to *dscp-value*. Valid values are shown in Table 16: Standard DSCP Values, on page 48.
Step 8	switch(config-pmap-c-qos)# **exit**	Returns to policy-map configuration mode.

	Command or Action	Purpose
Step 9	switch(config-pmap-qos)# **class** [**type qos**] {*class-map-name* | **qos-dynamic** | **class-default**} [**insert-before** *before-class-map-name*]	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 10	switch(config-pmap-c-qos)# **set dscp** *dscp-value*	Sets the DSCP value to *dscp-value*. Valid values are shown in Table 16: Standard DSCP Values, on page 48.
Step 11	switch(config-pmap-c-qos)# **exit**	Returns to policy-map configuration mode.
Step 12	switch(config)# **interface ethernet** {*slot/port*}	Enters interface mode to configure the Ethernet interface.
Step 13	switch(config-if)#**service-policy** [**type qos**] {**input** | **output**} {*policy-map-name* | **qos-dynamic**} [**no-stats**]	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
```

Configuring Table Maps for Use in Marking

You can use the system-defined table maps to define the mapping of values from one variable to another from a source QoS field to a destination QoS field. For the list of system-defined table maps, see “Using Modular QoS CLI.” The source and destination fields are determined by the context of the table map in the set and police commands. For information about table maps, see the “Configuring Marking Using Table Maps” section.

The system-defined table maps are not configurable. To display the current values, enter the **show table map** command.

Use the **default** command to define the destination value of unmapped source values. By default, unmapped values are copied to the destination value, so that the destination value is the same as the source value. The ignore variable for the **default** command is no longer supported.

Note You can use only one of the system-defined table maps in this procedure. For information on the system-defined table maps, see “Using Modular QoS CLI.”

Configuring Marking Using Table Maps

You can use the system-defined table maps to perform marking in the **set** and **police** policy map class commands.

Note For the list of system-defined table maps, see "Using Modular QoS CLI."

A source field and destination field are specified in the command that maps to the source and destination values supplied in the referenced table map. The QoS fields that can be used in these commands are listed in the table below.

Table 18: QoS Table Map Fields

QoS Table Map Field	Description
CoS	Class of service field in the 802.1Q header.
DSCP	Differentiated Services Code Point in the IP header.
IP precedence	Bits 0–2 of the IPv4 ToS field.
Discard class	Locally significant values that can be matched and manipulated within the system. The range is from 0 to 63.

By using the system-defined table maps, you cannot change unlike values, but you can only change one value to another when it is the same variable. You can use the markdown system-defined table maps for the **exceed** or **violate** action of the **police** command by using the same syntax as the set command.

Note The internal label QoS group is not supported through table maps.

Note Marking down in the police command requires the use of a table map.

For information on the police command, see "Configuring Policing."

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **policy-map** [**type qos**] [**match-first**] {*qos-policy-map-name* | **qos-dynamic**}	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.

	Command or Action	Purpose
Step 3	switch(config-pmap-qos)# **class** [**type qos**] {*class-map-name* | **qos-dynamic** | **class-default**} [**insert-before** *before-class-map-name*]	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	switch(config-pmap-c-qos)# **set** {**cos** | **dscp** | **discard-class** | **precedence** | **discard-class**} {**cos** | **dscp** | **discard-class** | **precedence** | **discard-class**} *table-map-name*	Sets the first packet field to the value of the second packet field based on the mapping values specified in the referenced *table-map-name*. **Note** The table-map-name must be the name of one of the system-defined table maps, which are not configurable, listed in "Using Modular QoS CLI." You cannot use the name of a user-defined table in this procedure.
Step 5	switch(config-pmap-c-qos)# **exit**	Returns to policy-map configuration mode.

Example

This example shows how to display the policy1 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 table-map	Displays all table maps.
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
```

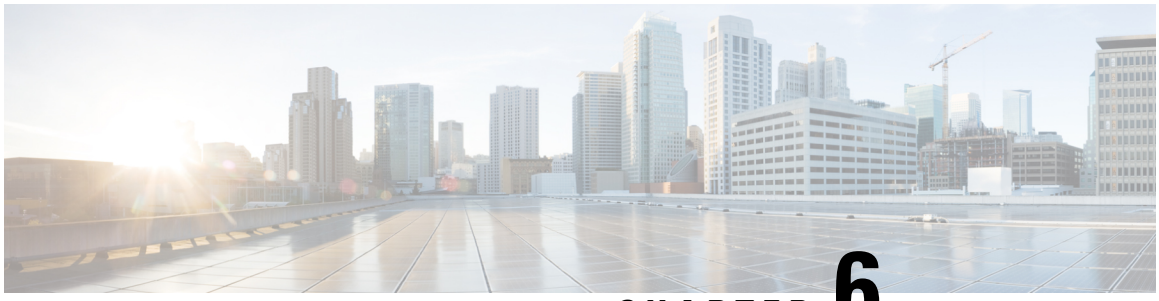
```
  set dscp 0
policy-map type queuing untrust_1Gport_policy
 class type queuing 2q4t-in-q-default
  set cos 0
policy-map type queuing untrust_10Gport_policy
 class type queuing 8q2t-in-q-default
  set cos 0
```

Feature History for Marking

The table below summarizes the new and changed features for this document and shows the releases in which each feature is supported. Your software release might not support all the features in this document. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release.

Table 19: Feature History for Marking

Feature Name	Release	Feature Information
set cos command	5.0(3)	Support for **set cos** command in ingress policies.



CHAPTER 6

Configuring Mutation Mapping

This chapter describes how to configure the mutation of packet values used to define traffic classes on the Cisco NX-OS device.

Finding Feature Information

Your software release might not support all the features documented in this module. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the "New and Changed Information"chapter or the Feature History table in this chapter.

Information About Mutation Mapping

Mutation mapping is a method of modifying a quality of service (QoS) field in all packets on an interface. On ingress, mutation mapping occurs before traffic classification and all other actions. On egress, mutation mapping occurs after traffic classification and before the other actions. You can apply mutation mapping to the class of service (CoS), Differentiated Service Code Point (DSCP), IP precedence packet fields, or to the internal field discard class.

You cannot configure system-defined mutation maps. You can only configure those maps that modify the same source and destination variable.

You use a hierarchical policy map to configure mutation mapping. In the mutation mapping policy map, you specify the field to mutate and the policy map to apply with the mutation.

Note The device supports hierarchical policies only for mutation mapping.

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

1. Queuing and scheduling
2. Mutation
3. Classification
4. Marking
5. Policing

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

1. Classification
2. Marking
3. Policing
4. Mutation
5. Queuing and scheduling

Note Mutation occurs much closer to the beginning of the traffic actions on the ingress packets, and any further classification and policing is based on the changed QoS values. Mutation occurs at the end of the traffic actions on the egress packets, right before queuing and scheduling.

Prerequisites for Mutation Mapping

Mutation mapping has the following prerequisites:

- You must be familiar with the “Using Modular QoS CLI” section.
- You are logged on to the switch.
- You are in the VDC. A VDC is a logical representation of a set of system resources. You can use the **switchto vdc** command with a VDC number.

Guidelines and Limitations

Mutation mapping has the following configuration guidelines and limitations:

- You use a hierarchical policy for mutation mapping. Hierarchical policies are not supported for any other use.
- The device supports only one level of hierarchy.

- You can configure up to 14 table maps for use in ingress interfaces and up to 15 table maps for use in egress interfaces.
- Before you delete a referenced policy map, you must first remove all references to that policy map.
- You can use only like parameters (for example, cos-cos) when you create a mutation map. Mutation maps with dissimilar types (for example, cos-dscp) are not supported.

Configuring Mutation Mapping

To configure mutation mapping, you create a hierarchical policy map that uses the class-default traffic class to capture all packets and apply mutation mapping to them. You use the **service-policy** command to specify the policy map to apply with mutation mapping.

Note You can set only similar values when you create a mutation map. For example, you can set cos-cos or dscp-dscp; you cannot set cos-dscp or dscp-precedence.

To configure mutation mapping:

1. Create the policy map to apply in the mutation mapping hierarchical policy. For information about configuring policy maps, see "Configuring Policing" or "Configuring Queuing and Scheduling."
2. Create the table map to use in the mutation mapping hierarchical policy. For information about configuring table maps, see the "Configuring Marking Using Table Maps" section.
3. Configure the mutation mapping hierarchical policy as described in this section.
4. Apply the service policy to the interface. For information about attaching policies to interfaces, see "Using Modular QoS CLI."

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **policy-map** [**type qos**] [**match-first**] {*qos-policy-map-name* | **qos-dynamic**}	Creates or accesses the specified 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	switch(config-pmap-qos)# **class class-default**	Configures **class-default** to capture all traffic in this policy map.
Step 4	switch(config-pmap-c-qos)# **set** {**cos** | **discard-class** | **dscp** | **precedence**} {**cos** | **discard-class** | **dscp** | **precedence**} **table** *table-map-name*	Sets the first packet field to the value of the second packet field based on the mapping values in the specified table map. For mutation mapping, both fields must have the same value. The specified table map must already exist.

	Command or Action	Purpose
		Note You can only set same fields when in mutation mapping (for example, dscp-dscp). The example shows how to use mutation mapping on the DSCP field based on the mapping values in table map dscp_mutation.
Step 5	switch(config-pmap-c-qos)# **service-policy** [**type qos**] {*policy-map-name* | **qos-dynamic**} [**no-stats**]	Defines the policy map to apply with the mutation map. The specified policy map must already exist and cannot contain a service-policy command. **Note** Classification within this service policy is based on the mutated value, not on the original value in the packet. **Note** The service-policy command can only be used for mutation mapping.
Step 6	(Optional) switch(config-pmap-c-qos)# **show policy-map** [**type** {**qos** | **queuing**}] [*policy-map-name* | **qos-dynamic**]	Displays information about all configured policy maps or the specified policy map.
Step 7	(Optional) switch(config-pmap-c-qos)# **copy running-config startup-config**	Saves the running configuration to the startup configuration.

Verifying the Mutation Mapping Configuration

To display the mutation mapping configuration information, perform the following task:

Command	Purpose
show policy-map [**type** {**qos** | **queuing**}] [*policy-map-name* | **qos-dynamic**]	Displays information about all configured policy maps or the specified policy map.

For detailed information about the fields in the output from these commands, see the *Cisco Nexus 7000 Series NX-OS Quality of Service Command Reference*.

Configuration Examples for Mutation Mapping

The following example shows how to configure a mutation:

Note If the child service policy (in this example, child_qos_policy) is not configured in the parent policy map (in this example, parent_policy_for_mutation), all packets will be changed according to the mutation map.

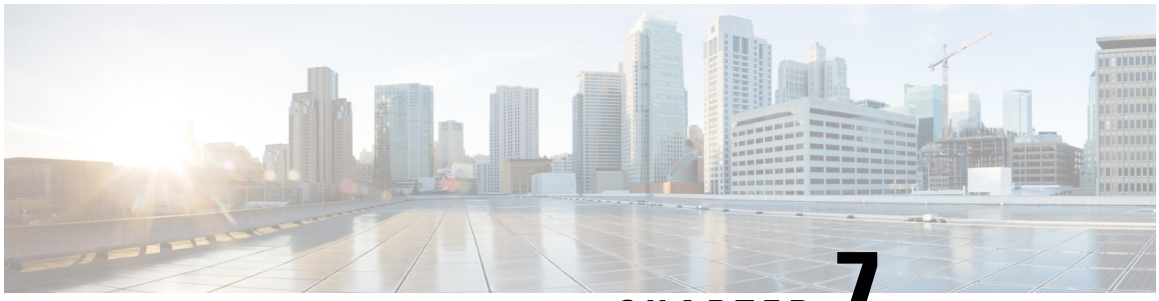
```
class-map type qos match-all dscp0-12
  match dscp 0-12
  match protocol dhcp

class-map type qos match-all dscp13-63
  match dscp 13-60

table-map mutate_dscp
  default copy
  from 0 to 0
  from 1 to 1
  from 2 to 1
  from 63 to 46

policy-map type qos child_qos_policy
  class dscp0-12
   police cir 10 mbps bc 200 ms pir 20 mbps be 200 ms conform transmit exceed set dscp
dscp table cir-markdown-map violate drop
  class dscp13-63
   police cir 20 mbps bc 200 ms pir 40 mbps be 200 ms conform transmit exceed set dscp
dscp table cir-markdown-map violate drop
  class class-default
   police cir 5 mbps bc 200 ms conform transmit violate drop

policy-map type qos parent_policy_for_mutation
  class class-default
   set dscp dscp table mutate_dscp
   service-policy type qos child_qos_policy
```

Feature History for Mutation Mapping

The table below summarizes the new and changed features for this document and shows the releases in which each feature is supported. Your software release might not support all the features in this document. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release.

Table 20: Feature History for Mutation Mapping

Feature Name	Release	Feature Information
No changes from Release 4.1(2)	5.1(1)	——
Mutation Mapping	4.1(2)	You can only use similar variables for mutation mapping.



CHAPTER 7

Configuring Policing

This chapter describes how to configure policing of traffic classes on the Cisco NX-OS device.

Finding Feature Information

Your software release might not support all the features documented in this module. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the "New and Changed Information"chapter or the Feature History table in this chapter.

Information 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, dual-rate, and color-aware policers.

Single-rate policers monitor the committed information rate (CIR) of traffic. Dual-rate policers monitor both CIR and peak information rate (PIR) of traffic. In addition, the system monitors associated burst sizes. Three colors, or conditions, are determined by the policer for each packet depending on the data rate parameters supplied: conform (green), exceed (yellow), or violate (red).

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.

Color-aware policers assume that traffic has been previously marked with a color. This information is then used in the actions taken by this type of policer.

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

Shared Policers

QoS applies the bandwidth limits specified in a shared policer cumulatively to all flows in the matched traffic. A shared policer applies the same policer to more than one interface simultaneously.

For example, if you configure a shared policer to allow 1 Mbps for all Trivial File Transfer Protocol (TFTP) traffic flows on VLAN 1 and VLAN 3, the device limits the TFTP traffic for all flows combined on VLAN 1 and VLAN 3 to 1 Mbps.

The following are guidelines for configuring shared policers:

- You create named shared policers by entering the qos shared-policer command. If you create a shared policer and create a policy using that shared policer and attach the policy to multiple ingress ports, the device polices the matched traffic from all the ingress ports to which it is attached.
- You define shared policers in a policy map class within the police command. If you attach a named shared policer to multiple ingress ports, the device polices the matched traffic from all the ingress ports to which it is attached.
- Shared policing works independently on each module.

Prerequisites for Policing

Policing has the following prerequisites:

- You must be familiar with “Using Modular QoS CLI.”
- You are logged on to the switch.
- You are in the correct VDC. A VDC is a logical representation of a set of system resources. You can use the **switchto vdc** command with a VDC number.

Guidelines and Limitations

Policing has the following configuration guidelines and limitations:

- F1 modules do not support policing.
- Each module polices independently, which might affect QoS features that are being applied to traffic that is distributed across more than one module. The following are examples of these QoS features:
  - Policers applied to a port channel interface.

    - Egress policers applied to a Layer 3 interface. The device performs egress policing decisions at the ingress module.
    - Policers applied to a VLAN.

- All policers in either the ingress or egress direction must use the same mode. For example, if the color-aware mode is needed for a class, all classes in that policy in the same direction must be in the color-aware mode.
- An interface policer does not work for the Layer 2 traffic data and control traffic in native VLAN in the following scenarios:
    - When the **native vlan** (ID other than 1) command is configured on the interface and the native VLAN ID is missing in the configuration.
    - If the **vlan dot1q tag native exclude control** command is configured.
- The police rate for traffic between two different port ASIC instances on a module is set differently for all modules in Cisco Nexus 7000 Series.
    - When traffic is between two different instances on an M1 module, the police rate is shared between the instances. If you add another interface as a third instance, the same police rate is shared as was between the two existing instances. For example, if a police rate of 5 Mbps is shared between two instances and an interface on a third instance is added, then the police rate of 5 Mbps is shared among all three instances.
    - When the traffic is between two different instances (on all modules in Cisco Nexus 7000 Series), the police rate is not shared between the instances. The police rate is shared only among the interfaces on the same instance. For example, if a police rate of 5 Mbps is set for the interfaces on one instance, this 5 Mbps police rate is not shared with interfaces on another instance.
    - In M3 modules, MQC supports a *shared-policer* construct, which allows traffic from multiple targets to share a common policer. The only restriction is that the policing rate for a *shared-policer* can be supported only within a single decision engine instance.
- The traffic is policed if the policer is applied as follows on M1 and F2 modules when the **mac packet-classify** command is not enabled:
    - Layer 2 traffic is matched when the policer is configured with MAC access list.
    - Layer 3 traffic is matched when the policer is configured with IP access list.
    - Layer 2 and Layer 3 traffic are matched when the policer is configured with MAC access list and IP access list.
- When the policer is applied on M1 or F2 modules having Layer 2 and Layer 3 traffic with MAC and IP access list, only the Layer 2 traffic matched with MAC access list is classified if the **mac packet-classify** command is enabled.
- When the port mode is changed, from **switchport** to **no switchport** or vice versa, the policy-map configured on the interface will revert to system default, after the interface is bounced or the switch is reloaded.

Configuring Policing

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

The type of policer created by the device is based on a combination of the police command arguments described in the table below.

Note You must specify the identical value for pir and cir to configure 1-rate 3-color policing.

Table 21: 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.
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, and the Gigabit per second (gbps) rate is not supported for this parameter.
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 to 80 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, and the Gigabit per second (gbps) rate is not supported for this parameter. **Note** You must specify a value for **pir** before the device displays this argument.

Argument	Description
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 table below (Policer Actions for Conform). 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.

Note For information on the color-aware police command arguments, see the "Configuring Color-Aware Policing" section.

Although all the arguments in the table above 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 next table.

Table 22: 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**
cir and **pir**	1-rate, 3-color	≤ **cir**, **conform**; ≤ **pir**, **exceed**; else **violate** **Note** You must specify identical values for **cir** and **pir**.
cir and **pir**	2-rate, 3-color	≤ **cir**, **conform**; ≤ **pir**, **exceed**; else **violate**

The policer actions that you can specify are described in the following two tables.

Table 23: 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.

Action	Description
set dscp dscp table {*cir-markdown-map* | *pir-markdown-map*}	Sets the specified fields from a table map and transmits the packet. For more information on the system-defined or default table maps, see "Configuring Marking." This action is available only when the packet exceeds the parameters (use the cir-markdown-map) or violates the parameters (use the pir-markdown-map). **Note** If the packet has a CoS value configured on VLAN, then the CoS value is used to set the value for the DSCP field.

Table 24: 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 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.
set-discard-class-transmit	Sets the discard-class internal label to a specified value and transmits the packet. This action can be used only in ingress 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 "Configuring Marking."

The data rates used in the police command are described in the table below.

Table 25: 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 table below.

Table 26: Burst Sizes for the police Command

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

Note You must specify the identical value for **pir** and **cir** to configure 1-rate 3-color policing.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **policy-map** [**type qos**] [**match-first**] {*qos-policy-map-name* | **qos-dynamic**}	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	switch(config-pmap-qos)# **class** [**type qos**] {*class-map-name* | **qos-dynamic** | **class-default**} [**insert-before** *before-class-map-name*]	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.

	Command or Action	Purpose
Step 4	switch(config-pmap-c-qos)# **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** | **set-discard-class-transmit**} [**exceed** {**drop** | **set dscp dscp table** {*cir-markdown-map*}} [**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, data rates, and link speeds are described in the tables above. **Note** You must specify identical values for **cir** and **pir**.
Step 5	switch(config-pmap-c-qos)# **exit**	Exits policy-map class configuration mode and enters policy-map mode.
Step 6	switch(config-pmap-qos)# **exit**	Exits policy-map mode and enters global configuration mode.
Step 7	(Optional) switch(config)# **show policy-map** [**type qos**] [*policy-map-name* | **qos-dynamic**]	Displays information about all configured policy maps or a selected policy map of type qos.
Step 8	(Optional) switch(config)# **copy running-config startup-config**	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 Color-Aware Policing

Color-aware policing implies that the QoS DSCP field in a class of traffic has been previously marked with values that you can use in a policer. This feature allows you to mark traffic at one node in a network and then take action based on this marking at a subsequent node.

For information on the police command, see the “Configuring 1-Rate and 2-Rate, 2-Color and 3-Color Policing” section.

You can use one or more of the four police command class maps conform-color or exceed-color to perform color-aware policing. These keywords require a class-map name that is used to classify packets. Based on the match criteria that you specify in the class maps, the traffic is classified into one of these two classes or class-default if there is no match. The policer then takes the following action:

- Packets that belong to the **conform-color** class are policed with the **cir** and **pir** arguments to the **police** command.

- Packets that belong to the **exceed-color** class are policed only against the **pir** argument to the **police** command. If **pir** is not specified, the **cir** values are used.
- Packets that end up in class-default because they fail to match either the **conform-color** or **exceed-color** class will immediately take the violate action.

A color other than class-default cannot be assigned to the violate action because according to RFC 2697 and RFC 2698, all packets must be assigned a color.

You can set the DSCP value for color-aware policing to a specified value. The list of valid DSCP values is shown in the table below.

Table 27: Color-Aware Policing Valid 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
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

Value	List of DSCP Values
cs7	CS7 (precedence 7) dscp (111000)—decimal value 56
default	Default dscp (000000)—decimal value 0
ef	EF dscp (101110)—decimal value 46

After you apply color-aware policing, all matching packets in the device are policed according to the specifications of the color-aware policer.

To configure color-aware policing:

1. Create the class map. For information about configuring class maps, see "Configuring Classification."
2. Create a policy map. For information about policy maps, see this chapter and "Using Modular QoS CLI."
3. Configure the color-aware class map as described in this section.
4. Apply the service policy to the interfaces. For information about attaching policies to interfaces, see "Using Modular QoS CLI."

Note The rates specified in the shared policer are shared by the number of interfaces to which you apply the service policy. Each interface does not have its own dedicated rate as specified in the shared policer.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **class-map** {**conform-color-in** | **conform-color-out** | **exceed-color-in** | **exceed-color-out**}	Accesses the color-aware class map, and enters color-map mode. When you enter this command, the system returns the following message: `Warning: Configuring match for any DSCP values in this class-map will make ALL policers in the system color-aware for those DSCP values.`
Step 3	switch(config-color-map)# **match dscp** *dscp-value*	Specifies the DSCP value to match for color-aware policers. See the table above for a list of valid values.
Step 4	switch(config-color-map)# **policy-map** [**type qos**] [**match-first**] {*qos-policy-map-name* | **qos-dynamic**}	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.

	Command or Action	Purpose
Step 5	switch(config-pmap-qos)# **class** [**type qos**] {*class-map-name* | **qos-dynamic** | **class-default**} [**insert-before** *before-class-map-name*]	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 6	switch(config-pmap-c-qos)# **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** | **set-discard-class-transmit**} [**exceed** {**drop** | **set dscp dscp table** {*cir-markdown-map*}} [**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, data rates, and link speeds are described in Configuring 1-Rate and 2-Rate, 2-Color and 3-Color Policing, on page 68 above.
Step 7	switch(config-color-map)# **exit**	Exits color-map mode and then enters global configuration mode.
Step 8	(Optional) switch(config)# **show policy-map** [**type qos**] [*policy-map-name* | **qos-dynamic**]	Displays information about all configured policy maps or a selected policy map of type qos.
Step 9	(Optional) switch(config)# **copy running-config startup-config**	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 Ingress and Egress Policing

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

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 Configuring 1-Rate and 2-Rate, 2-Color and 3-Color Policing, on page 68.

The example in this section shows you how to use a table map to perform a markdown.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **policy-map** [**type qos**] [**match-first**] {*qos-policy-map-name* | **qos-dynamic**}	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	switch(config-pmap-qos)# **class** [**type qos**] {*class-map-name* | **qos-dynamic** | **class-default**} [**insert-before** *before-class-map-name*]	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	switch(config-pmap-c-qos)# **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** | **set-discard-class-transmit**} [**exceed** {**drop** | **set dscp dscp table** {*cir-markdown-map*}} [**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, data rates, and link speeds are described in Configuring 1-Rate and 2-Rate, 2-Color and 3-Color Policing, on page 68 above.
Step 5	switch(config-pmap-c-qos)# **exit**	Exits policy-map class configuration mode and enters policy-map mode.
Step 6	switch(config-pmap-qos)# **exit**	Exits policy-map mode and enters global configuration mode.
Step 7	(Optional) switch(config)# **show policy-map** [**type qos**] [*policy-map-name* | **qos-dynamic**]	Displays information about all configured policy maps or a selected policy map of type qos.
Step 8	(Optional) switch(config)# **copy running-config startup-config**	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 Shared Policers

The shared-policer feature allows you to apply the same policing parameters to several interfaces simultaneously. You create a shared policer by assigning a name to a policer, and then applying that policer to a policy map that you attach to the specified interfaces. The shared policer is also referred to as the named aggregate policer in other Cisco documentation.

Note After you configure the shared policer, you can use the shared-policer name to configure any type of shared policing, as described in the "Configuring 1-Rate and 2-Rate, 2-Color and 3-Color Policing" section, the "Configuring Color-Aware Policing" section, the "Configuring Ingress and Egress Policing" section, and the "Configuring Markdown Policing" section.

To configure shared policing:

1. Configure the shared policer as described in this section.
2. Create the class map. For information about configuring class maps, see "Configuring Classification."
3. Create a policy map. For information about policy maps, see this chapter and "Using Modular QoS CLI."
4. Reference the shared policer to the policy map as described in this section.
5. Apply the service policy to the interfaces. For information about attaching policies to interfaces, see "Using Modular QoS CLI."

Note The rates specified in the shared policer are shared by the number of interfaces to which you apply the service policy. Each interface does not have its own dedicated rate as specified in the shared policer.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **qos shared-policer** [**type qos**] *shared-policer-name* [**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** *conform-action*	Creates or accesses the shared policer. The shared-policer-name can contain alphabetic, hyphen, or underscore characters, is case sensitive, and can be up to 40 characters. 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

	Command or Action	Purpose
	[**exceed** {**drop** | **set dscp dscp table** *cir-markdown-map*} [**violate** {**drop** | **set dscp dscp table** *pir-markdown-map*}]]}}	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, data rates, and link speeds are described in Configuring 1-Rate and 2-Rate, 2-Color and 3-Color Policing, on page 68 above.
Step 3	switch(config)# **policy-map** [**type qos**] [**match-first**] {*qos-policy-map-name* | **qos-dynamic**}	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 4	switch(config-pmap-qos)# **class** [**type qos**] {*class-map-name* | **qos-dynamic** | **class-default**} [**insert-before** *before-class-map-name*]	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 5	switch(config-pmap-c-qos)# **police aggregate shared-policer-name**	Creates a reference in the policy map to *shared-policer-name*.
Step 6	switch(config-pmap-c-qos)# **exit**	Exits policy-map class configuration mode and enters policy-map mode.
Step 7	switch(config-pmap-qos)# **exit**	Exits policy-map mode and enters global configuration mode.
Step 8	(Optional) switch(config)# **show policy-map** [**type qos**] [*policy-map-name* | **qos-dynamic**]	Displays information about all configured policy maps or a selected policy map of type qos.
Step 9	(Optional) switch(config)# **copy running-config startup-config**	Saves the running configuration to the startup configuration.

Example

This example shows how to display the test1 shared-policer configurations:

```
switch# show qos shared-policer test1
```

Verifying the Policing Configuration

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

show policy-map	Displays information about policy maps and policing.
show qos shared-policer [**type qos**] [*policer-name*]	Displays information about all shared 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 1-rate, 3-color policer:

```
configure terminal
 policy-map policy3
  class one_rate_3_color_policer
   police cir 256000 pir 256000 conform transmit exceed set dscp dscp table
cir-markdown-map violate drop
```

The following example shows how to configure policing for a 2-rate, 3-color policer:

```
configure terminal
 policy-map policy4
  class two_rate_3_color_policer
   police cir 256000 pir 256000 conform transmit exceed set dscp dscp table
cir-markdown-map violate drop
```

The following example shows how to configure policing for a color-aware policer for specified DSCP values:

```
configure terminal
  class-map conform-color-in
   match dscp 0-10
policy-map policy5
  class one_rate_2_color_policer
   police cir 256000 conform transmit violate drop
```

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

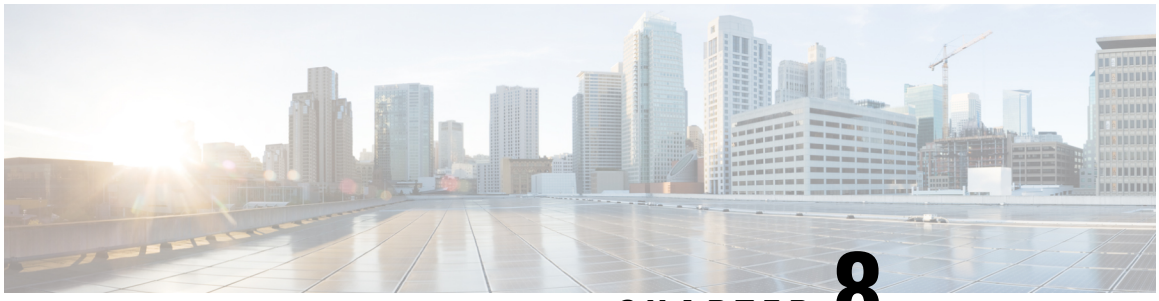
```
configure terminal
 qos shared-policer type qos udp_10mbps cir 10 mbps pir 20 mbps conform transmit exceed
set dscp dscp table cir-markdown-map violate drop
 policy-map type qos udp_policy
  class type qos udp_qos
   police aggregate udp_10mbps
```

Feature History for Policing

The table below summarizes the new and changed features for this document and shows the releases in which each feature is supported. Your software release might not support all the features in this document. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release.

Table 28: Feature History for Policing

Feature Name	Release	Feature Information
No changes from Release 4.1(2)	5.1(1)	——



CHAPTER 8

Configuring Fabric QoS Mapping

This chapter describes how to configure the Fabric QoS mapping feature within the Cisco NX-OS device.

Finding Feature Information

Your software release might not support all the features documented in this module. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the "New and Changed Information"chapter or the Feature History table in this chapter.

Information About Fabric QoS Mapping

The Fabric QoS Mapping feature allows copying the default configuration and modifying the copied system queues that perform flow control on fabric traffic within the Cisco NX-OS device, thus enabling the choice of parameters for fabric queuing based on the network, traffic, and requirements for traffic prioritization.

Note Default policies cannot be modified. The user-defined policies configured on the fabric cannot be modified.

Fabric queuing policies are controlled by COS-to-queue (cos2q) mappings, ingress queuing policies, and egress queuing policies applied on the QEngine of M1 and M2 line cards.

COS-to-Queue Fabric Mapping

The following are the four system-defined queues available for cos2q mapping:

- system-pq1

- system-q2
- system-q3
- system-q-default

The COS value indicates the Data Centre Ethernet (DCE) cos2q mapping of the active QoS network. The default COS value allocation for each system-defined queue is as follows:

The table below describes the system-defined queues that you can use to perform cos2q fabric mapping.

Table 29: System-Defined Queue Types

Queue Type	Default COS Value
system-pq1	5,6,7
system-q2	3,4
system-q3	2
system-q-default	0,1

For information about configuring cos2q fabric mapping, see the “Configuring Cos2q Fabric Mapping” section.

Ingress Buffer Policy

In the ingress direction, the queue limit for the system-q-default queue can be configured for burst-optimized, default, mesh-optimized, or percent.

For information about configuring ingress buffer policy for policy maps, see the “Configuring Ingress Buffer Policy” section.

Egress Queue Bandwidth Allocation

In the egress direction, priority and bandwidth can be configured for the system-defined queues. Only the system-pq1 queue can take the priority. If system-pq1 is configured for priority, the remaining 3 system queues can be configured based on bandwidth percentage. If system-pq1 is not configured for priority, all 4 system-defined queues share the bandwidth configured for each.

For information about configuring egress queue bandwidth allocation for policy maps, see the “Configuring Egress Queue Bandwidth Allocation” section.

Guidelines and Limitations

- When you are working with fabric QoS mapping, all the ports on M Series modules much be allocated to the default VDC.
- M3 modules do not support fabric QoS mapping.

Configuring Fabric QoS Mapping

User-defined Fabric QoS Mapping is configured in the following sequence:

- Copying a default policy to create a user-defined policy for fabric mapping
- Configuring cos2q fabric mapping
- Configuring ingress buffer policy for fabric mapping
- Configuring egress buffer queue bandwidth allocation for fabric mapping
- Configuring the new policy on fabric

You can copy a default policy to create a new policy for fabric mapping and modify the QoS configuration.

If a user-defined policy is not applied on fabric, the default policies will be considered in ingress and egress directions.

Note Only the users who have access to the default VDC or the admin VDC can copy the default policy and modify the default fabric QoS configuration on the copied policy.

Copying a Default Policy

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **qos copy policy-map type fabric-queuing system-in-policy** {**prefix** | **suffix**} *prefix-or-suffix-name*	Copies the default input policy to create a user defined input policy with the specified prefix or suffix.
Step 3	switch(config)# **qos copy policy-map type fabric-queuing system-out-policy** {**prefix** | **suffix**} *prefix-or-suffix-name*	Copies the default output policy to create a user defined output policy with the specified prefix or suffix.

Configuring Cos2q Fabric Mapping

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.

	Command or Action	Purpose
Step 2	switch(config)# **class-map type queuing** {**system-pq1** | **system-q-default** | **system-q2** | **system-q3**}	Configures the class map of type queuing, specifies the class map name as the selected system-defined queue and then enters class-map queuing mode.
Step 3	switch(config-cmap-que)# **match cos** *value-range*	Sets the CoS value range matched by this queue. You can specify a range of values by using a hyphen between the beginning and ending values and a comma between values. The range is from 0 to 7.
Step 4	switch(config-cmap-que)# **exit**	Exits class-map queue mode and enters global configuration mode.
Step 5		Repeat Steps 2 to 4 to configure additional system-defined queues

Configuring Ingress Buffer Policy

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **policy-map type queuing** *ingress-policy-name*	Configures the policy map of type queuing with the user-defined ingress policy and enters policy-map mode.
Step 3	switch(config-pmap-sys)# **class type queuing system-q-default**	Specifies the class type queue as system-q-default and enters policy-map class system mode.
Step 4	switch(config-pmap-c-sys)# **queue-limit** {**default** | **burst-optimized** | **mesh-optimized** | **percent** *percent_of_queuelimit*}	Configures the queue limit for the system queue.
Step 5	switch(config-pmap-c-sys)# **exit**	Exits policy-map class system mode and enters global configuration mode.

Configuring Egress Queue Bandwidth Allocation

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.

	Command or Action	Purpose
Step 2	switch(config)# **policy-map type queuing** *ingress-policy-name*	Configures the policy map of type queuing with the user-defined ingress policy and enters policy-map mode.
Step 3	switch(config-pmap-sys)# **class type queuing system-pq1**	Specifies the class type queue as system-pq1 and enters policy-map class system mode.
Step 4	switch(config-pmap-c-sys)# **priority level 1**	Configures the priority for system-pq1 as level 1.
Step 5	switch(config-pmap-c-sys)# **exit**	Exits policy-map class system mode and enters global configuration mode.
Step 6	switch(config-pmap-sys)# **class type queuing system-q-default**	Specifies the class type queue as system-q-default and enters policy-map class system mode.
Step 7	switch(config-pmap-c-sys)# **bandwidth** [**remaining**] **percent** *percent*	Configures bandwidth for system-q-default.
Step 8	switch(config-pmap-c-sys)# **exit**	Exits policy-map class system mode and enters global configuration mode.
Step 9	(Optional)	Repeat Steps 6 to 8 to assign bandwidth or bandwidth remaining for additional system-defined queues.

Configuring the New User-defined Policy on Fabric

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **system fabric**	Enters system fabric mode
Step 3	switch(config-sys-mfab)# **service-policy type queuing input** *ingress-policy-name*	Configures the specified user-defined input policy on the fabric.
Step 4	switch(config-sys-mfab)# **service-policy type queuing output** *egress-policy-name*	Configures the specified user-defined output policy on the fabric.
Step 5	switch(config-sys-mfab)# **exit**	Exits system fabric mode and enters global configuration mode.
Step 6	(Optional) switch(config)# **show policy-map system fabric**	Displays information about the system fabric configuration.

Configuration Examples for Fabric QoS Mapping

Example: Copying Default Policy to Create a new User-defined Ingress and Egress Policy

The following example shows how to create user-defined policies with the suffix '-in' for ingress policy and '-out' for egress policy:

```
Switch# configure terminal
Switch(config)# qos copy policy-map type fabric-queuing system-in-policy suffix -in
Switch(config)# qos copy policy-map type fabric-queuing system-out-policy suffix -out
```

Example: Configuring Cos2q Fabric Mapping

The following example shows how to configure Cos2q fabric mapping for all the system-defined queues:

```
Switch# configure terminal
Switch(config)# class-map type queuing system-pq1
Switch(config-cmap-que)# match cos 0
Switch(config-cmap-que)# exit
Switch(config)# class-map type queuing system-q-default
Switch(config-cmap-que)# match cos 1
Switch(config-cmap-que)# exit
Switch(config)# class-map type queuing system-q2
Switch(config-cmap-que)# match cos 2
Switch(config-cmap-que)# exit
Switch(config)# class-map type queuing system-q3
Switch(config-cmap-que)# match cos 3
Switch(config-cmap-que)# exit
```

Example: Configuring the User-defined Policy on Fabric

The following example shows how to configure the user-defined system-in-policy and system-out-policy on fabric:

```
Switch# configure terminal
Switch(config)# system fabric
Switch(config-sys-mfab)# service-policy type queuing input system-in-policy-in
Switch(config-sys-mfab)# service-policy type queuing output system-out-policy-out
Switch(config-sys-mfab)# exit
```

Example: Verifying System Fabric Configuration

The following sample output from the show policy-map system fabric command displays the input and output policy applied on fabric:

```
Switch# show policy-map system fabric

Service-policy (queuing) input: system-in-policy-in
```

```
  Class-map (queuing): system-q-default (match-any)
    queue-limit percent 60
  Class-map (queuing): system-pq1 (match-any)

  Class-map (queuing): system-q2 (match-any)

  Class-map (queuing): system-q3 (match-any)

Service-policy (queuing) output: system-out-policy-out

  Class-map (queuing): system-q-default (match-any)
    bandwidth remaining percent 5

  Class-map (queuing): system-pq1 (match-any)
    priority level 1

  Class-map (queuing): system-q2 (match-any)
    bandwidth remaining percent 5

  Class-map (queuing): system-q3 (match-any)
    bandwidth remaining percent 5
```

Example: Verifying the QoS Mapping on Fabric

The following excerpts of the sample output from the show policy-map type queuing command displays the QoS mapping on fabric:

```
Switch# show policy-map type queuing

Type queuing policy-maps
========================
policy-map type queuing system-in-policy
 class type queuing system-q-default
  queue-limit default
 class type queuing system-pq1
 class type queuing system-q2
 class type queuing system-q3
.
.
.
policy-map type queuing system-out-policy
 class type queuing system-q-default
  bandwidth remaining percent 33
 class type queuing system-pq1
  priority level 1
 class type queuing system-q2
  bandwidth remaining percent 33
 class type queuing system-q3
  bandwidth remaining percent 33
.
.
.
policy-map type queuing fab_in-system-in-policy
 class type queuing system-q-default
  queue-limit percent 60
 class type queuing system-pq1
 class type queuing system-q2
 class type queuing system-q3
policy-map type queuing fab_out-system-out-policy
 class type queuing system-q-default
```

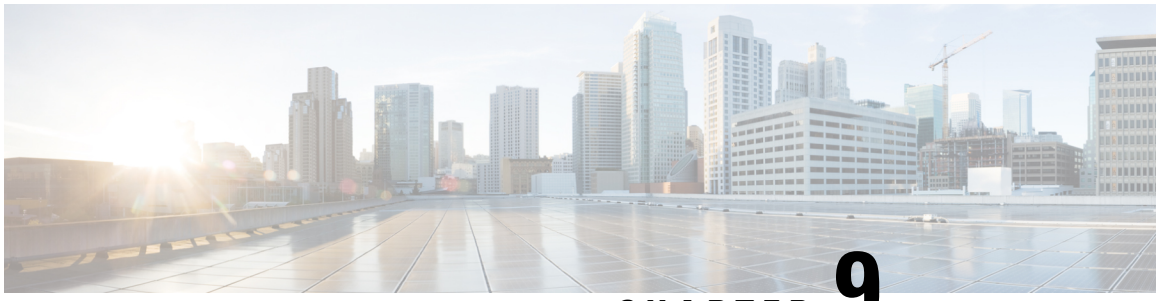
```
  bandwidth remaining percent 5
class type queuing system-pq1
```

Feature History for Fabric QoS Mapping

The table below summarizes the new and changed features for this document and shows the releases in which each feature is supported. Your software release might not support all the features in this document. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release.

Table 30: Feature History for Fabric QoS Mapping

Feature Name	Release	Feature Information
Fabric QoS Mapping	6.2(2)	This feature was introduced.



CHAPTER 9

Configuring Queuing and Scheduling on M-Series I/O Modules

This chapter describes how to configure the QoS queuing and scheduling features on M-Series I/O modules of the Cisco NX-OS device.

Finding Feature Information

Your software release might not support all the features documented in this module. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the "New and Changed Information"chapter or the Feature History table in this chapter.

Information 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.

Table 31: System-Defined Queue Types

Queue Type	Direction	Description
2q4t	Input	2 queues with 4 WRED or tail drop thresholds per queue
1p3q4t	Output	1 strict priority plus 3 normal queues with 4 WRED or tail-drop thresholds per queue
8q2t	Input	8 queues with 2 tail drop thresholds per queue
1p7q4t	Output	1 strict priority queue plus 7 normal queues with 4 WRED or tail drop thresholds per queue
1p7qlt	Output	1 strict priority queue plus 7 normal queues with 1WRED or tail drop thresholds per queue
1p3q1t	Output	1 strict priority queue plus 3 normal queues with 1 WRED or tail drop thresholds per queue
2p2q1t	Output	2 strict priority queues plus 2 normal queues with 1 WRED or tail drop thresholds per queue
2p6q1t	Output	2 strict priority queues plus 6 normal queues with 1 WRED or tail drop thresholds per queue
3p1q1t	Output	3 strict priority queues plus 1 normal queue with 1 WRED or tail drop thresholds per queue
3p5qlt	Output	3 strict priority queues plus 5 normal queues with 1 WRED or tail drop thresholds per queue

The queues match on the class of service (CoS) field. The device ensures that every CoS value from 0 to 7 maps to a queue for each queue type. Only one queue for a queue type can be assigned with a specific CoS value. For more information about the system-defined queues, see Table 6: System-Defined Type queuing Class Maps, on page 15 .

DSCP-to-queue mapping is disabled by default. Use the **hardware qos dscp-to-queue ingress** command to enable DSCP mapping on the modules. The table below describes the system-defined DSCP queuing class-maps with the default DSCP values.

Table 32: System-Defined Queuing Class Maps with Default DSCP Values

Class Map Queue Name	Description	Default DSCP Value
8q2t-in-q1	Ingress queue 1 of type 8q2t	40-63
8q2t-in-q2	Ingress queue 2 of type 8q2t	—
8q2t-in-q3	Ingress queue 3 of type 8q2t	—
8q2t-in-q4	Ingress queue 4 of type 8q2t	—
8q2t-in-q5	Ingress queue 5 of type 8q2t	—
8q2t-in-q6	Ingress queue 6 of type 8q2t	—
8q2t-in-q7	Ingress queue 7 of type 8q2t	—
8q2t-in-q-default	Ingress default queue of type 8q2t	0-39

Setting Ingress Port CoS

You can set the CoS field in all ingress packets for untrusted ports. By default, ports are trusted and the CoS field is not modified. You can use this method to configure the port state to trusted or untrusted.

For information about configuring ingress port CoS, see the “Configuring Ingress Port CoS” section.

Modifying Class Maps

You can modify the CoS values that are matched by system-defined queuing class maps, which modify the CoS-to-queue mapping. Table 6: System-Defined Type queuing Class Maps, on page 15 lists the default system-defined CoS values. Each CoS value appears only once in the queues of the same type.

If you want to change the system-default queuing class maps, you must also change the queuing policies applied on the interfaces because any changes in the queuing class maps causes traffic disruptions and might also cause packet drops.

Caution When you modify a system-defined queuing class map, the changes occur immediately and it might disrupt traffic on all virtual device contexts (VDCs).

Note For traffic crossing Layer 3, the queue mapping CoS-to-queue occurs automatically.

For information about configuring class maps, see the “Modifying Queuing Class Maps for COS” section.

Note Starting from Cisco NX-OS Release 6.2(2), DSCP-to-queue mapping on ingress class maps is supported on M Series 10G modules. However, the DSCP-to-queue mapping on all egress class maps is not supported.

Congestion Avoidance

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

- Apply WRED to a class of traffic, which allows the device to drop packets based on the CoS field. WRED is designed to work with TCP traffic.
- Apply tail drop to a class of traffic, which allows the device to drop packets based on the CoS field.
- Apply WRED to a class of traffic, which allows the device to drop packets based on the DSCP field. WRED is designed to work with TCP traffic.
- Apply tail drop to a class of traffic, which allows the device to drop packets based on the DSCP field.

For information about configuring congestion avoidance, see the "Modifying Queuing Class Maps for DSCP" section.

Congestion Management

For ingress packets, you can configure congestion management by specifying a bandwidth that allocates a minimum data rate to a queue.

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 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 by DSCP Values" section.

Virtualization Support

A VDC is a logical representation of a set of system resources. Other than configuring class maps, queuing and scheduling apply only to the VDC where the commands are entered. For information about configuring class maps, see the "Modifying Queuing Class Maps for COS" section.

For information about configuring VDCs, see the *Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*.

Prerequisites for Queuing and Scheduling

Queuing and scheduling have the following prerequisites:

- You must be familiar with the "Using Modular QoS CLI" chapter.
- You are logged on to the switch.
- You are in the correct VDC. A VDC is a logical representation of a set of system resources. You can use the **switchto vdc** command with a VDC number.

Guidelines and Limitations

Queuing and scheduling have the following configuration guidelines and limitations:

- If a no-drop class is paused and the IP traffic is received with the CoS value of the no-drop class, IP traffic is queued in default queue due to the dscp-to-queue mapping behaviour. This is applicable to Cisco Nexus 7700 Series switches by default. Note that the dscp-to-queue mapping can be disabled.
-
- Configure system-defined class maps with care because the changes occur immediately and traffic might be disrupted on all VDCs.
- Defining the CoS with the **match cos** command is not supported for custom configured class maps.
- Specifying DSCP values for a class map with the **match dscp** command is not supported for custom configured class maps.
- When you are working with 10-Gigabit Ethernet ports in the shared mode, the egress queuing policy applies to all the ports in the port group. With the 10-Gigabit Ethernet ports in shared mode, all the ports in the port group must be in the same VDC. For information about the shared and dedicated modes, see the *Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide*. For information about the port groups, see the *Cisco Nexus 7000 Series Hardware Installation and Reference Guide*.
- You cannot set either the queue limit or WRED on ingress 10-Gigabit Ethernet ports except for the 8 port, 10-Gigabit Ethernet I/O module.
- To ensure accurate hardware programming on Cisco M1 Series modules, when you add a physical interface to a port-channel, which already has a queuing policy applied, you must remove the queuing policy and reapply. Without this reapplication, queuing policy will not be correctly applied on all the interfaces. Otherwise, you must ensure that the queuing policy is applied on the port-channel interface only after all the physical ports are bundled into the port-channel.
- On Cisco M1 series modules, it may not be possible to configure actual values for traffic shaping. For example, on a 1 Gigabit interface with 65% average shaping, the output rate on the interface goes only up to 450Mbps, whereas with 70%, it goes to 850Mbps.
- When changing egress Class of Service (CoS) to queue mapping, ensure that you specify 2 or 3 seconds as the minimum time limit between changes. Otherwise, continuous traffic drop might occur.
- The Cisco M3 series modules do not support per-queue counters for egress drops (multicast, unknown unicast, or broadcasts). The egress drops will be per port and per Q-Default counter.
- Only 8e templates are supported on Cisco M3 series modules.
- In Cisco Nexus 7700 switches, the Cisco M3 series module supports only network-qos policies based on the 8e-4q8q template.
- The Cisco M3 series module supports only the network-qos template. This template contains all the CoS values that match the MTU size.
- All data traffic will be enqueued to the default queue of dot1q-tunnel port because this port is untrusted by default.

Configuring Queuing and Scheduling

Queuing and scheduling are configured by creating policy maps of type queuing that you apply to either traffic direction of an 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.

Additional considerations are as follows:

- Changes to system class maps take effect immediately across all VDCs.

  The specified CoS values immediately map to the new queues.

- 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. For example, if you change COS-to-queue mapping for the M1 10G egress interface type, all M1 10G ports in all VDCs experience a brief disruption.

- 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, then the traffic mapping to that queue might experience performance degradation.

- If you change the CoS-to-queue mapping by modifying the queuing class maps, you must ensure that a new queuing policy was applied to all ports of that type that use the new queues.

- If you change the DSCP-to-ingress-queue mapping by modifying the queuing class maps, you must ensure that a new queuing policy is applied to all ports of that type that use the new queues.

- By default, nonused queues do not have an allocated buffer. Allocate buffers to these queues to avoid tail drop.

- Changes to system class-maps are made only on the default VDC.

For information about configuring policy maps and class maps, see “Using Modular QoS CLI.”

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, shaping, and bandwidth, in output queues, and you can configure bandwidth in input queues.

We recommend that you modify the CoS value before you create a policy map. You can modify the CoS values that are matched by device-defined class map queues. You must assign each CoS value from 0 to 7 to one or more of the queues for each queue type. Each CoS value is used only once in each queue type.

We recommend that you modify the DSCP value before you create a policy map. You can modify the DSCP values that are matched by device-defined class map queues. You must assign each DSCP value from 0 to 63 to one or more of the queues for each queue type. Each DSCP value is used only once in each queue type.

The system-defined policy maps default-in-policy and default-out-policy are attached to all ports to which you do not apply a queuing policy map. The default policy maps cannot be configured. For more information about the default policy maps, see Table 8: System-Defined Queuing Policy Maps, on page 18.

This example shows that if you downgrade from Release 4.0(3) to Release 4.0(2) and enter the **show running-configuration** command, the input default queuing policy has an unknown enum in the display:

```
switch# show running-config
version 4.0(2)
```

```
…
…
policy-map type queuing default-in-policy
class type queuing unknown enum 0
queue-limit percent 50
bandwidth percent 80
class type queuing unknown enum 0
queue-limit percent 50
bandwidth percent 20
```

If you copy and paste this configuration into any Cisco NX-OS release, the device sends errors while executing all the commands starting from the **policy-map type queuing default-in-policy** command. You can ignore these errors because they do not affect the performance of the device.

Configuring Ingress Port CoS

To make a port untrusted, set the CoS value to a static value.

Note

- By default, ports are trusted (trust CoS) and the CoS field is not modified. When you configure the ingress port CoS value, the port becomes untrusted.
- For the untagged bridged traffic, a Cisco Nexus 7000 Series device ignores the Differentiated Services Code Point (DSCP) and queues on ingress and egress directions, if the CoS value is 0.
- By default, Layer 3 ports trust DSCP and also copy the DSCP value to CoS.

You use the ingress default queues from the system-defined queue classes for the type of module to which you want to apply the policy map. For the list of system-defined class maps for each type of module, see Table 6: System-Defined Type queuing Class Maps, on page 15.

The CoS values set using this procedure apply to all packets that ingress the specified interfaces, not just to the class-default packets. If you set the CoS value, the device modifies the value before ingress queuing and scheduling so the CoS-modified packets are classified differently.

Note If you want to change the system-defined queuing class maps, you must either modify the configured queuing policies or create new queuing policies and attach these policies to the affected interfaces. If you fail to do so, you can render the default queuing or the configured queuing policies invalid, which might affect the interfaces in multiple VDCs.

Note When DSCP is enabled and configured on a queue, and if the port is untrusted, and an ingress port cos is configured, DSCP is considered for queuing.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.

	Command or Action	Purpose
Step 2	switch(config)# **policy-map type queuing** [**match-first**] {*policy-map-name* | **que-dynamic**}	Configures the policy map of type queuing, and then enters policy-map mode for the policy-map name that you specify. Policy-map names can contain alphabetic, hyphen, or underscore characters, are case sensitive, and can be up to 40 characters.
Step 3	switch(config)# **class type queuing** *class-queuing-name*	Configures the class map of type queuing, and then enters policy-map class queuing mode. **Note** To configure port CoS, you can use only an ingress default system-defined queue type.
Step 4	switch(config-pmap-c-que)# **set cos** *value*	Sets the CoS field in all ingress packet to the value specified. The range is from 0 to 7.
Step 5	switch(config-pmap-c-que)# **exit**	Exits policy-map queue mode, and enters global configuration mode.
Step 6	(Optional) switch(config)# **show policy-map type queuing** [*policy-map-name* | **que-dynamic**]	Displays information about all configured policy maps or a selected policy map of type queuing.
Step 7	(Optional) switch(config)# **copy running-config startup-config**	Saves the running configuration to the startup configuration.

Modifying Queuing Class Maps for COS

You can modify the CoS values that are matched by system-defined class maps. See Table 6: System-Defined Type queuing Class Maps, on page 15 which lists the default system-defined CoS values.

The system-defined class maps can be changed only from the default VDC. Changes occur immediately and are applied to all ports on all VDCs that use the modified class map.

Note When you modify a system-defined class map, the changes occur immediately and might disrupt traffic on all VDCs that use the modified class map.

Note Defining the CoS with the match cos command is not supported for custom configured class-maps.

The device automatically modifies the CoS values that you configured in other queues so that each CoS value appears only once in the queues of the same type.

Before you begin

Ensure that you are in the default VDC for the device.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **class-map type queuing match-any** {*class-queuing-name* | *WORD*}	Configures the class map of type queuing, and then enters class-map queuing mode. The match on WORD is used for defining hierarchical class-maps in a queuing policy. The argument, *WORD*, is supported only on the F-Series Modules.
Step 3	switch(config-cmap-que)# **match cos** *value-range*	Sets the CoS value range matched by this queue. You can specify a range of values by using a hyphen between the beginning and ending values and a comma between values. The range is from 0 to 7. **Note** Repeat Steps 2 and 3 to modify CoS values for additional queues.
Step 4	switch(config-pmap-c-que)# **exit**	Exits policy-map queue mode, and enters global configuration mode.
Step 5	(Optional) switch(config)# **show policy-map type queuing** [*policy-map-name* | **que-dynamic**]	Displays information about all configured policy maps or a selected policy map of type queuing.
Step 6	(Optional) switch(config)# **copy running-config startup-config**	Saves the running configuration to the startup configuration.

Modifying Queuing Class Maps for DSCP

You can modify the DSCP values that are matched by system-defined class maps. The system-defined class maps can be changed only from the default VDC. Changes occur immediately and are applied to all ports on all VDCs that use the modified class map.

To allow the modifications to be implemented, the DSCP-to-queue mapping must be enabled. If you have not enabled the DSCP-to-queue mapping earlier, you can use the **hardware qos dscp-to-queue ingress module type** command to enable DSCP-to-queue mapping.

To disable the DSCP mapping, use the **no hardware qos dscp-to-queue ingress** command.

Note When you modify a system-defined class map, the changes occur immediately and might disrupt traffic on all VDCs that use the modified class map.

The device automatically modifies the DSCP values that you configured in other queues so that each DSCP value appears only once in the queues of the same type.

Before you begin

Ensure that you are in the default VDC for the device.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	(Optional) switch(config)# **hardware qos dscp-to-queue ingress module type** {**all** | **f-series** | **m-series**}	Enables the dscp-to-queue mapping on the specified module(s). Use the **hardware qos dscp-to-queue ingress module type** command if you have not enabled dscp-to-queue mapping.
Step 3	switch(config)# **class-map type queuing match-any** *class-queuing-name*	Configures the class map of type queuing, and then enters class-map queuing mode.
Step 4	switch(config-cmap-que)# **match dscp** *value-range*	Sets the DSCP value range matched by this queue. You can specify a range of values by using a hyphen between the beginning and ending values and a comma/space between values. The range is from 0 to 63. **Note** Repeat Steps 5 and 6 to modify DSCP values for additional queues
Step 5	switch(config-cmap-que)# **exit**	Exits class-map queue mode, and enters global configuration mode.

Configuring Congestion Avoidance

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

Note WRED and tail drop cannot be configured in the same class.

Configuring Tail Drop by COS Values

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

Note You cannot configure the queue size on ingress 10-Gigabit Ethernet ports except for the 8-port, 10-Gigabit Ethernet I/O module.

You use the system-defined queue classes for the type of module to which you want to apply the policy map. See Table 6: System-Defined Type queuing Class Maps, on page 15.

Note WRED and tail drop cannot be configured in the same class.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **policy-map type queuing** [**match-first**] {*policy-map-name* | **que-dynamic**}	Configures the policy map of type queuing, and then enters policy-map mode for the policy-map name that you specify. Policy-map names can contain alphabetic, hyphen, or underscore characters, are case sensitive, and can be up to 40 characters.
Step 3	switch(config)# **class type queuing** *class-queuing-name*	Configures the class map of type queuing, and then enters policy-map class queuing mode.
Step 4	switch(config-pmap-c-que)# **queue-limit cos** *value* {*threshold* [**packets** | **bytes** | **kbytes** | **mbytes** | **ms** | **us**] | *percent percent_of_queuelimit*}	Assigns a tail drop threshold based on the queue size or percentage of the buffer memory that is used by the queue. The device drops packets that exceed the specified threshold. You can configure the threshold by the number of packets, number of bytes, or the duration of time at the underlying interface minimum guaranteed link rate. The default threshold is in packets. The size is from 1 to 83886080. The duration is from 1 to 83886080. The percentage is from 1 to 100. **Note** Repeat Step 4 to assign tail drop thresholds for other CoS values. Repeat Steps 3 through 5 to assign tail drop thresholds for other queue classes.
Step 5	switch(config-pmap-c-que)# **exit**	Exits policy-map queue mode, and enters global configuration mode.
Step 6	(Optional) switch(config)# **show policy-map type queuing** [*policy-map-name* | **que-dynamic**]	Displays information about all configured policy maps or a selected policy map of type queuing.
Step 7	(Optional) switch(config)# **copy running-config startup-config**	Saves the running configuration to the startup configuration.

Configuring Tail Drop by DSCP Values

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

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **policy-map type queuing** {*queuing-policy-map-name*}	Configures the policy map of type queuing, and then enters policy-map mode for the policy-map name you specify.
Step 3	switch(config)# **class type queuing** *class-queuing-name*	Configures the class map of type queuing, and then enters policy-map class queuing mode.
Step 4	switch(config-pmap-c-que)# **queue-limit dscp** *value* {*queue-size* | **percent** *percent_of_queuelimit*}	Assigns a tail drop threshold based on the queue size or percentage of the buffer memory that is used by the queue. The device drops packets that exceed the specified threshold. Repeat Step 4 to assign tail drop thresholds for other DSCP values. Repeat Steps 3 through 5 to assign tail drop thresholds for other DSCP queue classes.
Step 5	switch(config-pmap-c-que)# **exit**	Exits policy-map queue mode, and enters global configuration mode.
Step 6	(Optional) switch(config)# **show policy-map type queuing** [*policy-map-name*	Displays information about all configured policy maps or a selected policy map of type queuing.
Step 7	(Optional) switch(config)# **copy running-config startup-config**	Saves the running configuration to the startup configuration.

Configuring WRED by COS Values

Before configuring WRED, ensure that the CoS values are there (see the “Modifying Queuing Class Maps for COS” section.

You can configure WRED on both ingress and 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 CoS value are dropped.

Note You cannot configure WRED on ingress 10-Gigabit Ethernet ports except for the 8-port 10-Gigabit Ethernet I/O module.

You can configure WRED thresholds by the CoS value, and configure a single WRED threshold to use on all CoS values that you do not specifically configure.

Note WRED and tail drop cannot be configured in the same class.

You use the system-defined queue classes for the type of module to which you want to apply the policy map.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **policy-map type queuing** [**match-first**] {*policy-map-name* | **que-dynamic**}	Configures the policy map of type queuing, and then enters policy-map mode for the policy-map name that you specify. Policy-map names can contain alphabetic, hyphen, or underscore characters, are case sensitive, and can be up to 40 characters.
Step 3	switch(config)# **class type queuing** *class-queuing-name*	Configures the class map of type queuing, and then enters policy-map class queuing mode.
Step 4	switch(config-pmap-c-que)# **random-detect cos-based** [**aggregate** [**minimum-threshold**] {*min-threshold* [**packets** | **bytes** | **kbytes** | **mbytes** | **ms** | **us**] | **percent** *min-percent-of-qsize*} [**maximum-threshold**] {*max-threshold* [**packets** | **bytes** | **kbytes** | **mbytes** | **ms** | **us**] | **percent** *min-percent-of-qsize*}]	Configures WRED for all CoS values not configured by a CoS-specific random-detect command. You can specify minimum and maximum thresholds used to drop packets from the queue. You can configure thresholds by the number of packets, number of bytes, the duration of time at the underlying interface minimum guaranteed link rate, or as the percentage of queue size. The minimum and maximum thresholds must be of the same type. If no aggregate arguments are supplied, no aggregate WRED is configured. The default threshold is in packets. The thresholds are from 1 to 83886080. The percentage range is from 1 to 100. **Note** You must enter this command, even if you enter the command with no values. **Note** You can specify only one **random-detect cos-based** command in a class.
Step 5	(Optional) switch(config-pmap-c-que)# **random-detect** {**cos** *cos-list* [**minimum-threshold**] {*min-threshold* [**packets** | **bytes** | **kbytes** | **mbytes** | **ms** | **us**] | **percent**	Configures WRED for specific CoS values. You can specify minimum and maximum thresholds used to drop packets from the queue. You can configure thresholds by the number of packets,

	Command or Action	Purpose
	min-percent-of-qsize} [**maximum-threshold**] {*max-threshold* [**packets** | **bytes** | **kbytes** | **mbytes** | **ms** | **us**] | **percent** *min-percent-of-qsize*}}	number of bytes, the duration of time at the underlying interface minimum guaranteed link rate, or as the percentage of the queue size. The minimum and maximum thresholds must be of the same type. The default threshold is in packets. Thresholds are from 1 to 83886080. The percentage range is from 1 to 100. Optional: repeat Step 5 to configure WRED for other CoS values. Optional: repeat Steps 3 through 6 to configure WRED for other queuing classes.
Step 6	switch(config-pmap-c-que)# **exit**	Exits policy-map queue mode, and enters global configuration mode.
Step 7	(Optional) switch(config)# **show policy-map type queuing** [*policy-map-name* | **que-dynamic**]	Displays information about all configured policy maps or a selected policy map of type queuing.
Step 8	(Optional) switch(config)# **copy running-config startup-config**	Saves the running configuration to the startup configuration.

Configuring WRED by DSCP Values

Before configuring WRED, ensure that the DSCP values are present (see the "Modifying Queuing Class Maps for DSCP" section).

You can configure WRED on ingress 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 DSCP value are dropped.

You cannot configure WRED on ingress 10-Gigabit Ethernet ports except for the 8-port 10-Gigabit Ethernet I/O module.

You can configure WRED thresholds by the DSCP value, and configure a single WRED threshold to use on all DSCP values that you do not specifically configure.

Note WRED and tail drop cannot be configured in the same class.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **policy-map type queuing** [**match-first**] {*policy-map-name* | **que-dynamic**}	Configures the policy map of type queuing, and then enters policy-map mode for the policy-map name that you specify. Policy-map names can contain alphabetic, hyphen, or underscore

	Command or Action	Purpose
		characters, are case sensitive, and can be up to 40 characters.
Step 3	switch(config)# **class type queuing** *class-queuing-name*	Configures the class map of type queuing, and then enters policy-map class queuing mode.
Step 4	switch(config-pmap-c-que)# **random-detect dscp-based** [**aggregate** [**minimum-threshold**] {*min-threshold* [**packets** | **bytes** | **kbytes** | **mbytes** | **ms** | **us**] | **percent** *min-percent-of-qsize*} [**maximum-threshold**] {*max-threshold* [**packets** | **bytes** | **kbytes** | **mbytes** | **ms** | **us**] | **percent** *min-percent-of-qsize*}]	Configures WRED for all DSCP values not configured by a DSCP-specific random-detect command. You can specify minimum and maximum thresholds used to drop packets from the queue. You can configure thresholds by the number of packets, number of bytes, the duration of time at the underlying interface minimum guaranteed link rate, or as the percentage of queue size. The minimum and maximum thresholds must be of the same type. If no aggregate arguments are supplied, no aggregate WRED is configured. The default threshold is in packets. The thresholds are from 1 to 52428800. The percentage range is from 1 to 100. **Note** You must enter this command, even if you enter the command with no values. **Note** You can specify only one **random-detect cos-based** command in a class.
Step 5	(Optional) switch(config-pmap-c-que)# **random-detect** {**dscp** *dscp-value* [**minimum-threshold**] {*min-threshold* [**packets** | **bytes** | **kbytes** | **mbytes** | **ms** | **us**] | **percent** *min-percent-of-qsize*} [**maximum-threshold**] {*max-threshold* [**packets** | **bytes** | **kbytes** | **mbytes** | **ms** | **us**] | **percent** *min-percent-of-qsize*}}	Configures WRED for specific DSCP values. You can specify minimum and maximum thresholds used to drop packets from the queue. You can configure thresholds by the number of packets, number of bytes, the duration of time at the underlying interface minimum guaranteed link rate, or as the percentage of the queue size. The minimum and maximum thresholds must be of the same type. The default threshold is in packets. Thresholds are from 1 to 52428800. The percentage range is from 1 to 100. Optional: repeat Step 5 to configure WRED for other DSCP values. Optional: repeat Steps 3 through 6 to configure WRED for other DSCP queuing classes.
Step 6	switch(config-pmap-c-que)# **exit**	Exits policy-map queue mode, and enters global configuration mode.

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 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 "Configuring Tail Drop by COS Values" section and "Configuring Tail Drop by DSCP Values" section.
- WRED for preferential packet drops based on CoS. For more information, see the "Configuring WRED by COS Values" section and "Configuring WRED by DSCP Values" section.

Configuring Bandwidth and Bandwidth Remaining

You can configure the bandwidth and bandwidth remaining on both ingress and egress queues to allocate a minimum percentage of the interface bandwidth to a queue. You use the system-defined ingress or egress queue class for the type of module to which you want to apply the policy map. For the list of system-defined ingress or egress queue classes for each module, see Table 6: System-Defined Type queuing Class Maps, on page 15.

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

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **policy-map type queuing** [**match-first**] {*policy-map-name* | **que-dynamic**}	Configures the policy map of type queuing, and then enters policy-map mode for the policy-map name that you specify. Policy-map names can contain alphabetic, hyphen, or underscore characters, are case sensitive, and can be up to 40 characters.
Step 3	switch(config)# **class type queuing** *class-queuing-name*	Configures the class map of type queuing, and then enters policy-map class queuing mode.
Step 4	switch(config-pmap-c-que)# **bandwidth** {**rate** [**bps** | **kbps** | **mbps** | **gbps**] | **percent**} • **bandwidth remaining percent** *percent*	Assigns a minimum rate of the interface bandwidth to an output queue. You can configure a data rate by the bit rate or as the

	Command or Action	Purpose
	Assigns the percentage of the bandwidth that remains to this queue. The range is from 0 to 100.	percentage of the underlying interface link rate. The default units are kbps. The data rate is from 1 to 10,000,000,000. The percentage range is from 1 to 100. You can use only the **percent** keyword for interfaces set to autonegotiate. Repeat Steps 3 to 4 to assign bandwidth or bandwidth remaining for other queuing classes.
Step 5	switch(config-pmap-c-que)# **exit**	Exits policy-map queue mode, and enters global configuration mode.
Step 6	(Optional) switch(config)# **show policy-map type queuing** [*policy-map-name* | **que-dynamic**]	Displays information about all configured policy maps or a selected policy map of type queuing.
Step 7	(Optional) switch(config)# **copy running-config startup-config**	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 "Using Modular QoS CLI."

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 list of available system-defined class maps for each module, see Table 6: System-Defined Type queuing Class Maps, on page 15.

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.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **policy-map type queuing** [**match-first**] {*policy-map-name* | **que-dynamic**}	Configures the policy map of type queuing, and then enters policy-map mode for the policy-map name that you specify. Policy-map names can contain alphabetic, hyphen, or underscore characters, are case sensitive, and can be up to 40 characters.

	Command or Action	Purpose
Step 3	switch(config-pmap-c-que)# **class type queuing** *class-queuing-name*	Configures the class map of type queuing, and then enters policy-map class queuing mode. You must select one of the system-defined priority queues.
Step 4	switch(config-pmap-c-que)# **priority** [**level** *value*]	Selects this queue as a priority queue. Only one priority level is supported.
Step 5	switch(config-pmap-c-que)# **class type queuing** *class-queuing-name*	Configures the class map of type queuing, and then enters policy-map class queuing mode. 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	switch(config-pmap-c-que)# **bandwidth remaining percent** *percent*	Assigns the percentage of the bandwidth that remains to this queue. The range is from 0 to 100. Repeat Steps 5 to 6 to assign bandwidth remaining for the other nonpriority queues.
Step 7	switch(config-pmap-c-que)# **exit**	Exits policy-map queue mode, and enters global configuration mode.
Step 8	(Optional) switch(config)# **show policy-map type queuing** [*policy-map-name* | **que-dynamic**]	Displays information about all configured policy maps or a selected policy map of type queuing.
Step 9	(Optional) switch(config)# **copy running-config startup-config**	Saves the running configuration to the startup configuration.

Configuring Shaping

Note The device forces the shape rate to the closest value in the following percentage intervals: 100, 50, 33, 25, 12.5, 6.25, 3.13, or 1.07.

You can configure shaping on an egress queue to impose a maximum rate on it. You use the system-defined egress queue class for the type of module to which you want to apply the policy map. For the list of available system-defined class maps for each module, see Table 6: System-Defined Type queuing Class Maps, on page 15.

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

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **policy-map type queuing** [**match-first**] {*policy-map-name* | **que-dynamic**}	Configures the policy map of type queuing, and then enters policy-map mode for the policy-map name that you specify. Policy-map names can contain alphabetic, hyphen, or underscore characters, are case sensitive, and can be up to 40 characters.
Step 3	switch(config-pmap-c-que)# **class type queuing** *class-queuing-name*	Configures the class map of type queuing, and then enters policy-map class queuing mode. You must select one of the system-defined priority queues.
Step 4	switch(config-pmap-c-que)# **shape** [**average**] {*rate* [**bps** | **kbps** | **mbps** | **gbps**] | **percent** *percent*}	Assigns a maximum rate on an output queue. You can configure a data rate by the bit rate or as a percentage of the underlying interface link rate. The default bit rate is in bits per second (bps). The data rate is from 8000 bps to 10 gbps. The percentage range is from 1 to 100. **Note** You can use only the **percent** keyword for interfaces set to autonegotiate. Repeat Steps 3 to 4 to configure shaping for other queuing classes.
Step 5	switch(config-pmap-c-que)# **exit**	Exits policy-map queue mode, and enters global configuration mode.
Step 6	(Optional) switch(config)# **show policy-map type queuing** [*policy-map-name* | **que-dynamic**]	Displays information about all configured policy maps or a selected policy map of type queuing.
Step 7	(Optional) switch(config)# **copy running-config startup-config**	Saves the running configuration to the startup configuration.

Configuring Queue Limits

You can configure the queue limit on both ingress and egress queues. The device drops any packets that exceed the queue limit. You use the system-defined queue classes for the type of module to which you want to apply the policy map. See Table 6: System-Defined Type queuing Class Maps, on page 15.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.

	Command or Action	Purpose
Step 2	switch(config)# **policy-map type queuing** [**match-first**] {*policy-map-name* | **que-dynamic**}	Configures the policy map of type queuing, and then enters policy-map mode for the policy-map name that you specify. Policy-map names can contain alphabetic, hyphen, or underscore characters, are case sensitive, and can be up to 40 characters.
Step 3	switch(config-pmap-que)# **class type queuing** *class-queuing-name*	Configures the class map of type queuing, and then enters policy-map class queuing mode. You must select one of the system-defined priority queues.
Step 4	switch(config-pmap-c-que)# **queue-limit** {*threshold* [**packets** | **bytes** | **kbytes** | **mbytes** | **ms** | **us**] | **percent** *percent_of_queuelimit*}	Assigns a queue limit based on the queue size or percentage of the buffer memory used by the queue. The device will drop packets that exceed the specified threshold. You can configure the threshold by the number of packets, number of bytes, or the duration of time at the underlying interface minimum guaranteed link rate. The default threshold is in packets. The size is from 1 to 83886080. The duration is from 1 to 83886080. The percentage range is from 1 to 100.
Step 5	switch(config-pmap-c-que)# **exit**	Exits class-map queue mode and enters policy-map queue mode.
Step 6	switch(config-pmap-que)# **exit**	Exits policy-map queue mode and enters global configuration mode.
Step 7	(Optional) switch(config)# **show policy-map type queuing** [*policy-map-name* | **que-dynamic**]	Displays information about all configured policy maps or a selected policy map of type queuing.
Step 8	(Optional) switch(config)# **copy running-config startup-config**	Saves the running configuration to the startup configuration.

Enabling DSCP to Queue Mapping

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **hardware qos dscp-to-queue ingress module type** {**all** | **f-series** | **m-series** }	Enables the dscp-to-queue mapping on the specified module(s).

	Command or Action	Purpose
		Note Starting with Cisco NX-OS Release 8.0(1), use the **f-series** keyword to enable dscp-to-queue mapping on M3-Series I/O modules.
Step 3	(Optional) switch(config)# **show hardware qos dscp-to-queue ingress**	Displays information about the status of dscp-to-queue mapping in ingress direction.
Step 4	(Optional) switch(config)# **copy running-config startup-config**	Saves the running configuration to the startup configuration.

Verifying the Queuing and Scheduling Configuration

To configure queuing and scheduling, perform one of the following tasks:

Command	Purpose
show class-map type queuing[*class-queuing-name*]	Displays information about all configured class maps or a selected class map of type queuing. Class queuing names are listed in Table 6: System-Defined Type queuing Class Maps, on page 15.
show policy-map type queuing [*policy-map-name* | **que-dynamic**]	Displays information about all configured policy maps or a selected policy map of type queuing.
show policy-map system	Displays information about all configured policy maps on the system.
show queuing interface ethernet *slot*/*port*[**.***subinterface* [*module* | **summary**]	Displays queuing information about the specified interface.

For more information about the fields in the output from these commands, see the *Cisco Nexus 7000 Series NX-OS Quality of Service Command Reference*.

Configuration Examples for Queuing and Scheduling

Example: Setting Ingress Port CoS Configuration

Note Setting the ingress port CoS value makes the specified interfaces untrusted.

Note Ensure that you are using the default queue for the port type that you are configuring. For information on the default queue for the port types, see "Using Modular QoS CLI."

The following example shows how to configure ingress port CoS for 1-Gigabit Ethernet ports:

```
configure terminal
 policy-map type queuing untrusted_port_cos
  class type queuing 2q4t-in-q-default
   set cos 5
 interface ethernet 2/1
  service-policy type queuing input untrusted_port_cos
```

The following example shows how to configure ingress port CoS for 10-Gigabit Ethernet ports:

```
configure terminal
 policy-map type queuing untrusted_port_cos
  class type queuing 8q2t-in-q-default
   set cos 5
 interface ethernet 2/1
  service-policy type queuing input untrusted_port_cos
```

Example: Priority and Queue Limit Configuration

The following example shows how to configure the priority and queue limit features:

```
configure terminal
 class-map type queuing match-any 1p3q4t-out-pq1
  match cos 5-7
 class-map type queuing match-any 1p3q4t-out-q2
  match cos 3-4
 class-map type queuing match-any 1p3q4t-out-q3
  match cos 0-2
policy-map type queuing priority_queue1
 class type queue 1p3q4t-out-pq1
  priority
 class type queue 1p3q4t-out-q2
  bandwidth remaining percent 60
  queue-limit 1 mbytes
 class type queue 1p3q4t-out-q3
  bandwidth remaining percent 40
  queue-limit 2 mbytes
```

Example: Shaping and Tail Drop Configuration

The following example shows how to configure the shaping and tail drop features:

```
configure terminal
 class-map type queuing match-any 1p3q4t-out-pq1
  match cos 5-7
 class-map type queuing match-any 1p3q4t-out-q2
  match cos 3-4
policy-map type queuing shape_dt
 class type queue 1p3q4t-out-pq1
  shape percent 50
```

```
  queue-limit cos 5 percent 10
  queue-limit cos 6 percent 10
 class type queue 1p3q4t-out-q2
  shape percent 25
  queue-limit cos 4 percent 15
```

Note If the **priority** keyword is not specified for a **pq1** queue, the queue is considered as a normal queue, not a priority queue.

Example: Bandwidth and WRED Configuration

The following example shows how to configure the bandwidth and WRED features for COS queues:

```
configure terminal
 class-map type queuing match-any 1p3q4t-out-pq1
  match cos 5-7
 class-map type queuing match-any 1p3q4t-out-q2
  match cos 3-4
policy-map type queuing bandwidth_wred
 class type queuing 1p3q4t-out-pq1
  bandwidth percent 50
  random-detect cos-based
  random-detect cos 5 minimum-threshold percent 10 maximum-threshold percent 30
  random-detect cos 6 minimum-threshold percent 40 maximum-threshold percent 60
 class type queuing 1p3q4t-out-q2
  bandwidth percent 25
  random-detect cos-based
  random-detect cos 4 minimum-threshold percent 20 maximum-threshold percent 40
```

The following example shows how to configure the bandwidth and WRED features for DSCP queues:

```
configure terminal
 class-map type queuing match-any 8q2t-in-q1
  match dscp 5-6
 class-map type queuing match-any 8q2t-in-q2
  match dscp 0-4
policy-map type queuing dscp_wred
 class type queuing 8q2t-in-q1
  bandwidth percent 50
  random-detect dscp-based
  random-detect dscp 5 minimum-threshold percent 10 maximum-threshold percent 30
  random-detect dscp 6 minimum-threshold percent 40 maximum-threshold percent 60
 class type queuing 8q2t-in-q2
  bandwidth percent 25
  random-detect dscp-based
  random-detect dscp 4 minimum-threshold percent 20 maximum-threshold percent 40
```

Example: Verifying the Status of DSCP-to-queue Mapping

The following sample output from the **show hardware qos dscp-to-queue ingress** command displays the status of DSCP-to-queue mapping enabled in ingress direction on M-series modules:

```
Switch# show hardware qos dscp-to-queue ingress
```

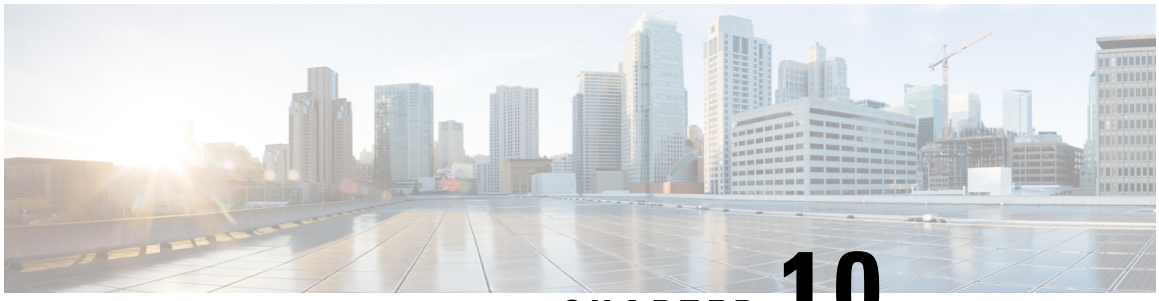
```
status: Enabled
module_type : m-series
```

Feature History for Queuing and Scheduling

The table below summarizes the new and changed features for this document and shows the releases in which each feature is supported. Your software release might not support all the features in this document. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release.

Table 33: Feature History for Queuing and Scheduling

Feature Name	Release	Feature Information
DSCP to Queue Mapping	8.0(1)	Use the **hardware qos dscp-to-queue ingress module type f-series** command to enable dscp-to-queue mapping on M3-Series I/O modules
DSCP to Queue Mapping	6.2(2)	This feature was introduced.
System-defined queue types	6.2(2)	Updated the System-Defined Queue Types table with new system-defined queue types for 4q8q policy templates on the Cisco Nexus 7710 switch and the Cisco Nexus 7718 switch.
No change from Release 4.1(2)	5.1(1)	—



CHAPTER 10

Configuring Queuing and Scheduling on F-Series I/O Modules

This chapter describes how to configure the QoS queuing and scheduling features on the F-Series I/O module of the Cisco NX-OS device.

Finding Feature Information

Your software release might not support all the features documented in this module. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the "New and Changed Information"chapter or the Feature History table in this chapter.

Information About Queuing and Scheduling

On an F-Series module, a queuing policy is closely coupled with the network qos policy. For each network qos policy that is activated, its corresponding default queuing policy is automatically selected for the system target. In the ingress direction, either two or four queues (buffer pools) are formed depending on the policy template. In the egress direction, there are four physical queues for qos policy templates on Cisco Nexus 7000 Series devices, except on the Cisco Nexus 7710 switch and Cisco Nexus 7718 switch, where, beginning with Cisco Release 6.2(2), there is support for eight physical queues.

The system queuing policy applied by default can be overridden on a per-port basis. In general, the user-configured queuing policies are per virtual device context (VDC).

Ingress queuing determines the following attributes:

- Queue-limit—Amount of buffers to be allocated for a class of service (CoS).
- Bandwidth—Priority grouping and its bandwidth allocation advertised using the Data Center Bridging Capability Exchange Protocol (DCBXP).
- Set CoS—Untrusted port default CoS (similar to the M1 modules).

Egress queuing determines the following attributes:

- Bandwidth—Differential Weighted Round Robin (DWRR) bandwidth for a given queue and the group.
- Priority level—The priority level of the queue.
- Shape—The shaper for the queue.

Ingress Queuing

You use the ingress queuing to partition the port ingress buffers that are 1.25 MB and an additional 256 KB (a total of 1.5 MB) to absorb the frames in transit after pause has been sent. This buffer is partitioned among the eight CoS values. The number of partitions is fixed for a given network qos template. The incoming CoS values are mapped to each partition. Each buffer partition is considered as an ingress queue.

There is a high threshold and a low threshold at which the pause or resume frames are generated when a threshold is met. This requirement is applicable to the no-drop CoS only. The frames that are in transit are absorbed by a skid buffer after a pause is generated. If the number of frames exceed the skid buffer threshold, the frames are tail dropped. There are three thresholds for drop eligible (DE), non-DE, and Bridge Protocol Data Unit (BPDU) frames for dropping. For the drop CoS, the high and low thresholds are the same.

The default policy ingress queues are created as follows:

- Different queues per drop class:

  Drop queue =70% buffers; no-drop queue = 30% buffers

- Different queues for priority and nonpriority CoS in a given drop class:

  Nonpriority queue= 90% buffers; priority queue = 10% buffers

Each network qos policy has a corresponding default ingress queuing policy (template) and is automatically activated for the system. They are the default-4q-8e-in-policy, default-4q-7e-in-policy, default-4q-6e-in-policy, default-4q-4e-in-policy, default-8e-4q8q-in-policy, default-7e-4q8q-in-policy, default-6e-4q8q-in-policy, default-4e-4q8q-in-policy, and default-8e-4q4q-in-policy.

The predefined class map names (queue names) for ingress queuing are described in the table below.

Table 34: Predefined Class Maps for Ingress Queuing

Ingress Policy Maps	Ingress Class Map Names
default-4q-8e-in-policy	2q4t-8e-in-q1 and 2q4t-8e-in-q-default
default-4q-7e-in-policy	4q4t-7e-in-q1, 4q4t-7e-in-q-default, 4q4t-7e-in-q3, and 4q4t-7e-in-q4
default-4q-6e-in-policy	4q4t-6e-in-q1, 4q4t-6e-in-q-default, 4q4t-6e-in-q3, and 4q4t-6e-in-q4

Ingress Policy Maps	Ingress Class Map Names
default-4q-4e-in-policy	4q4t-4e-in-q1, 4q4t-4e-in-q-default, 4q4t-4e-in-q3, and 4q4t-4e-in-q4
default-8e-4q4q-in-policy	4q1t-8e-4q4q-in-q1, 4q1t-8e-4q4q-in-q-default, 4q1t-8e-4q4q-in-q3, and 4q1t-8e-4q4q-in-q4
default-8e-4q8q-in-policy (on Cisco Nexus 7710 / 7718 switches only)	8e-4q8q-in-q1, 8e-4q8q-in-q-default, 8e-4q8q-in-q3, and 8e-4q8q-in-q4
default-7e-4q8q-in-policy (Cisco Nexus 7710 / 7718 switches only) • default-7e-4q8q-drop-in-policy • default-7e-4q8q-ndrop-in-policy	c-7e-4q8q-drop-in, c-7e-4q8q-ndrop-in 7e-4q8q-in-q1, 7e-4q8q-in-q-default and 7e-4q8q-in-q3 7e-4q8q-in-q4
default-6e-4q8q-in-policy (Cisco Nexus 7710 / 7718 switches only) • default-6e-4q8q-drop-in-policy • default-6e-4q8q-ndrop-in-policy	c-6e-4q8q-drop-in and c-6e-4q8q-ndrop-in 6e-4q8q-in-q1 and 6e-4q8q-in-q-default 6e-4q8q-in-q3 and 6e-4q8q-in-q4
default-4e-4q8q-in-policy (Cisco Nexus 7710 / 7718 switches only) • default-4e-4q8q-drop-in-policy • default-4e-4q8q-ndrop-in-policy	c-4e-4q8q-drop-in and c-4e-4q8q-ndrop-in 4e-4q8q-in-q1 and 4e-4q8q-in-q-default 4e-4q8q-in-q3 and 4e-4q8q-in-q4

Note

- The naming conventions of the queue are similar to the M1 modules. Also, the process for referring to queuing class maps and changing CoS to queue maps is also similar to M1 modules.
- When a port becomes part of a port channel, the port inherits the policy of the port channel. When the port is moved out of the port channel, the default system queuing policy gets activated on the port.

By default, the queuing policy maps the priority CoS values (CoS 5-7) and nonpriority CoS values (CoS 0-4) into different ingress queues (IVL). CoS to ingress queue mapping is configured from the default VDC and the configuration is applied system wide. A network administrator user role is required to change CoS to IVL.

Starting with the Cisco NX-OS 6.1 release, DSCP to IVL is supported on F2 modules, in the ingress direction, using the match dscp command with the 2q4t-8e-in-q1 class map and the 2q4t-8e-in-q-default class map.

Note Starting with the Cisco NX-OS 6.1(2) release, DSCP to IVL is supported on IPV6 using F2e modules.

Guidelines for the **match dsc**p command are as follows:

- The **match dscp** command is applicable only to queues that have at least one CoS value associated with it. If all DSCP values are not mapped to a nondefault ingress queue, the default queue should have the CoS values associated with it.
- DSCP queuing is automatically disabled when the user removes all **match dscp** commands (using **no match** statements).
- If the **match dscp** command is used in the 2q4t-8e-in-q1 class map to set some DSCP values, all remaining DSCP values are automatically mapped to the default queue.

Bridged Traffic	When the DSCP-to-queue is enabled, the ingress queue selection is based on the DSCP value. When CoS-to-queue is enabled, the ingress queue selection is based on the CoS value, for 802.1Q tagged frames or implied CoS of “0” for untagged frames. Egress queuing selection is based on CoS value, and not affected by DSCP-to-queue mappings. If a CoS value does not exist, then all packets are accepted as CoS 0.
Routed Traffic without Proxy Mode (native F-Series modules)	When the DSCP-to-queue is enabled, the ingress queue selection is based on the DSCP. When CoS -to-queue is enabled, the ingress queue is based on the CoS value, for 802.1Q tagged frames or implied CoS of “0” for untagged frames. When there is a non-IP frame, ingress queue selection is based on CoS irrespective of DSCP-to-ingress queue enabled or not. Egress queuing selection is based on first 3 bits of the DSCP value. If the 802.1q tag is present, the CoS value mutates to match the first 3 bits of the DSCP value on the egress packet. When the CoS-to-ingress queue is enabled for sub-interfaces, the ingress queue selection is based on the CoS. The above stated is valid for any routed traffic ingressing on Layer 3/ Sub-Interface/ SVI and egressing on Layer 3/ Sub-Interface/ SVI. Enabling “hardware QoS dscp-to-queue ingress” does not change behavior for egress queuing classification.

Routed Traffic with Proxy Mode (mixed F-Series and M-Series modules)	When the DSCP-to-ingress queue is enabled, the ingress queue selection is based on the DSCP. When the CoS-to-ingress queue is enabled, the ingress queue selection is based on the CoS. Egress queuing selection is based on first 3 bits of the DSCP value. If 802.1q tag is present, the CoS value mutates to match the first 3 bits of the DSCP value on the egress packet. The above stated is valid for any routed traffic when mixed F-Series and M-Series work in Proxy mode. Enabling "hardware QoS dscp-to-queue ingress" does not change behavior for egress queuing classification.

The following table contains an example of when the match dscp command is used in the 2q4t-8e-in-q1 class map to set specific DSCP values.

Commands	Description
class-map type queuing match-any 2q4t-8e-in-q1 **match cos 5-7** **match dscp 40-45**	The values set by the **match dscp** command are displayed by the **show run** command.
class-map type queuing match-any 2q4t-8e-in-q-default **match dscp 0-39,46-63.**	The remaining DSCP values (0-39, 46-63) are automatically mapped to the default queue. The values associated with the default queue are not displayed by the **show run** command. These values are implicitly programmed in the hardware.
class-map type queuing match-any 2q4t-8e-in-q-default **match dscp 40-45**	When specific DSCP values are mapped to the default queue (2q4t-8e-in-q-default), the remaining DSCP values are automatically mapped to the default queue. There is no restriction when specifying all of the remaining DSCP values in the default queue. The values set by the **match dscp** command are displayed by the **show run** command.
class-map type queuing match-any 2q4t-8e-in-q-default **match dscp 0-39,46-63**	The DSCP values (0-39, 46-63) are automatically mapped to the default queue (2q4t-8e-in-q-default). The values associated with the default queue are not displayed by the **show run** command. These values are implicitly programmed in the hardware.

Note Modifying the default queuing policy maps is a disruptive operation that might cause frame drops.

You can assign a bandwidth percentage to each ingress queue. The CoS values (priority group) of each queue and its bandwidth are relayed to the peer using the DCBXP.

With the Enhanced Transmission Selection (ETS; specifies scheduling of queues based on priority) implementation, when you define both the drop and no-drop classes in a non-8e network qos policy template, the queuing follows a hierarchical pattern. In a hierarchical queuing pattern, queues within a class are configured with respect to the buffer at the first level, and buffers across the queuing groups are configured at the second level.

You use the **queue-limit** command to tune the ingress queue sizes (buffers). You can define the percentage of the total buffer to be allocated to the queue. For more information about the queue-limit command, see the *Cisco Nexus 7000 Series NX-OS Quality of Service Command Reference*.

You use the **bandwidth** command to control the bandwidth allocated to the traffic classes (CoS) in the ingress queue. The bandwidth allocated to a traffic class in the ingress queue does not impact the switch. Instead, it sends the bandwidth information to the peer as an indication of the bandwidth for the traffic classes (CoS) that the peer sends. For more information about the bandwidth command, see the *Cisco Nexus 7000 Series NX-OS Quality of Service Command Reference*.

You use the **set cos** command only on the default queue to make a port that is untrusted on the default queue.

Starting with Cisco NXOS 6.2(2) Release, default dscp values are provided for all the following five templates on F-Series Modules:

- default-nq-4e-policy template 4e
- default-nq-6e-policy template 6e
- default-nq-7e-policy template 7e
- default-nq-8e-policy template 8e
- default-nq-8e-4q4q-policy template 8e-4q4q

The following table lists the default dscp values for 4q mode templates:

Ingress Queue	DSCP Map Value
Template: default-nq-4e-policy template 4e	
4q4t-4e-in-q-default	0-39
4q4t-4e-in-q1	40-63
4q4t-4e-in-q3	—
4q4t-4e-in-q4	—
default-nq-6e-policy template 6e	
4q4t-6e-in-q-default	0-39
4q4t-6e-in-q1	40-63
4q4t-6e-in-q3	—
4q4t-6e-in-q4	—

Ingress Queue	DSCP Map Value
default-nq-7e-policy template 7e	
4q4t-7e-in-q-default	0-15
4q4t-7e-in-q1	40-63
4q4t-7e-in-q3	16-39
4q4t-7e-in-q4	
default-nq-8e-policy template 8e	
2q4t-8e-4q4q-in-q-default	0-39
2q4t-8e-4q4q-in-q1	40-63
default-nq-8e-4q4q-policy template 8e-4q4q	
4q1t-8e-4q4q-in-q-default	0-15
4q1t-8e-4q4q-in-q1	40-63
4q1t-8e-4q4q-in-q3	24-39
4q1t-8e-4q4q-in-q4	16-23

Similarly, the default dscp values are mapped for ingress queues for Cisco 7710/7718 switches.

Egress Queuing

You use egress queuing to determine how to schedule the traffic from the egress queues out of a port. The class map names represent queues and match cos represents the CoS values mapped to them. You can modify the egress class map and match cos to achieve the desired CoS-to-queue mapping.

Note CoS remapping is supported only in strict F-Series VDCs. It is not supported in F-Series/M1 mixed VDCs.

Each egress port has about 0.7 MB of buffers that are distributed equally among the 8 CoS values. A CoS has approximately 0.1 MB of buffers.

The default policy egress queues are created as follows:

- The drop and no-drop CoS must be mapped to different queues.
- The priority CoS is mapped to a strict priority (SP) queue. All the nonpriority CoS values are mapped to a DWRR queue.
- For all the non-8e templates, second level scheduling is used.

Note

- Egress queues have a fixed size and are not user configurable.
- The egress port has four queues, except for the Cisco Nexus 7710 switch and the Cisco Nexus 7718 switch, whereby, beginning with Cisco Release 6.2(2), has support for eight queues (4q8q mode).

Each network qos policy has a corresponding default egress queuing policy (template) and is automatically activated for the system. They are the default-4q-8e-out-policy, default-4q-7e-out-policy, default-4q-6e-out-policy, default-4q-4e-out-policy, default-8e-4q8q-out-policy, default-7e-4q8q-out-policy, default-6e-4q8q-out-policy, default-4e-4q8q-out-policy and the default-8e-4q4q-out-policy. The flexible egress queues configuration is based on these queue types— 1p7qlt-8e, 1p7qlt-7e, 1p3q1t-8e, 1p3q1t-7e, 2p2q1t-4e, 2p6q1t-4e, 3p1q1t-6e, and 3p5qlt-6e.

For the Cisco Nexus 7710 switch and the Cisco Nexus 7718 switch, a hierarchical scheduling pattern is followed on the 7e-4q8q, 6e-4q8q, and 4e-4q8q templates.

The predefined class map names (queue names) for egress queuing are described in the table below.

Table 35: Predefined Class Maps for Egress Queuing

Egress Policy Names	Egress Class Map Names
default-4q-8e-out-policy	1p3q1t-8e-out-pq1, 1p3q1t-8e-out-q2, 1p3q1t-8e-out-q3, and 1p3q1t-8e-out-q-default
default-4q-7e-out-policy	1p3q1t-7e-out-pq1, 1p3q1t-7e-out-q2, 1p3q1t-7e-out-q3, and 1p3q1t-7e-out-q-default
default-4q-6e-out-policy	3p1q1t-6e-out-pq1, 3p1q1t-6e-out-pq2, 3p1q1t-6e-out-pq3, and 3p1q1t-6e-out-q-default
default-4q-4e-out-policy	2p2q1t-4e-out-pq1, 2p2q1t-4e-out-pq2, 2p2q1t-4e-out-q3, and 2p2q1t-4e-out-q-default
default-8e-4q4q-out-policy	1p3q1t-8e-4q4q-out-pq1, 1p3q1t-8e-4q4q-out-q2, 1p3q1t-8e-4q4q-out-q3, and 1p3q1t-8e-4q4q-out-q-default
default-8e-4q8q-out-policy (Cisco Nexus 7710 / 7718 switches only)	8e-4q8q-out-q1(priority queue), 8e-4q8q-out-q2, 8e-4q8q-out-q3, 8e-4q8q-out-q4, 8e-4q8q-out-q5, 8e-4q8q-out-q6, 8e-4q8q-out-q7, and 8e-4q8q-out-q-default
default-7e-4q8q-out-policy (Cisco Nexus 7710 / 7718 switches only) • default-7e-4q8q-drop-out-policy • default-7e-4q8q-ndrop-out-policy	c-7e-4q8q-drop-out and c-7e-4q8q-ndrop-out 7e-4q8q-out-q1 (priority queue), 7e-4q8q-out-q2, 7e-4q8q-out-q3, 7e-4q8q-out-q4, 7e-4q8q-out-q6, 7e-4q8q-out-q7, and 7e-4q8q-out-q-default 7e-4q8q-out-q5

Egress Policy Names	Egress Class Map Names
default-6e-4q8q-out-policy (Cisco Nexus 7710 / 7718 switches only) • default-6e-4q8q-drop-out-policy • default-6e-4q8q-ndrop-out-policy	c-6e-4q8q-drop-out and c-6e-4q8q-ndrop-out 6e-4q8q-out-q1 (priority queue), 6e-4q8q-out-q2, 6e-4q8q-out-q3, 6e-4q8q-out-q6, 6e-4q8q-out-q7, and 6e-4q8q-out-q-default 6e-4q8q-out-q4 (priority queue) and 6e-4q8q-out-q5 (priority queue)
default-4e-4q8q-out-policy (Cisco Nexus 7710 / 7718 switches only) • default-4e-4q8q-drop-out-policy • default-4e-4q8q-ndrop-out-policy	c-4e-4q8q-drop-out and c-4e-4q8q-ndrop-out 4e-4q8q-out-q1 (priority queue), 4e-4q8q-out-q2, 4e-4q8q-out-q3, and 4e-4q8q-out-q-default 4e-4q8q-out-q4 (priority queue), 4e-4q8q-out-q5, and 4e-4q8q-out-q6, 4e-4q8q-out-q7

You can modify an egress CoS to queue map irrespective of the ingress CoS to queue map by using the **match cos** command to configure the desired CoS to queue mapping.

An egress queue follows a hierarchical scheduling pattern when both drop classes are present. For more information, see the “Ingress Queuing” section. For a given network qos template, the egress queuing configuration (the number of DWRR queues, number of priority queues, and the scheduling hierarchy) are fixed. You can modify the bandwidth percentage, priority level, and shaper for a given port.

You use the **bandwidth** command to control the bandwidth allocated to an egress queue (traffic class). For more information about the bandwidth command, see the *Cisco Nexus 7000 Series NX-OS Quality of Service Command Reference*.

Note Bandwidth and priority are mutually exclusive on a class map (queue).

You use the **priority** command to specify that a class of traffic has low latency requirements with respect to other classes. You can configure the priority level to a traffic queue as high or low. Use the priority command to define multiple levels of a strict priority service model. For more information about the **priority** command, see the *Cisco Nexus 7000 Series NX-OS Quality of Service Command Reference*.

The shaper can be configured with a percentage value and it can be enabled on any queue. You use the **shape** command to specify that a class of traffic has a maximum rate imposed on it and the outgoing traffic has a smooth output rate. To achieve a smooth output rate, the excess packets are retained in the queue and then scheduled for transmission later. For more information about the **shape** command, see the *Cisco Nexus 7000 Series NX-OS Quality of Service Command Reference*.

Note A shaper delays excess traffic that does not conform to the profile by queuing it in a buffer to shape the flow.

Shared Buffer Queuing on the F3 Series Module

Note This feature is available only on the F3 Series modules. If you attempt to configure shared buffer queuing on other modules, the switch returns an error.

Beginning with Cisco NX-OS Release 6.2(10) you can split QoS buffers into dedicated and shared buffers. With only dedicated buffers based on the CoS value, one queue may have very high traffic even though memory associated with some of the other queues may be lying idle. The shared buffer pools address this problem. The shared buffer is between ports in a port group.

The default is disabled for shared buffer queuing.

When you enable this feature, you enable it for each specific module. After you have enabled shared buffer queuing, the queue is, by default, divided equally into dedicated and shared buffer pools, 50:50 for the specified module. The dedicated buffer pools continue to function as they always did.

Then, if you want a different ratio, you modify the ratio per port group on the specified module, using the Command Line Interface (CLI). First you specify the port group for the given module and then you can modify the default queue limit ratio for that port group. If you want to change the default queue limit ration for other port groups on that module, you must enter the command for each port group separately.

Finally, you can apply a custom queuing policy to the specified port group.

Note If global level shared buffer queuing is disabled, then shared buffer for all port-groups in that VDC are disabled. If the global level is enabled, all port groups in the VDC are enabled.

Shared buffer queuing is applicable only to port groups of physical interfaces. Shared buffer queuing on port groups is independent of membership in port channels. Thus, members of a port channel may have different shared buffer queuing configurations.

The command is applicable only to the ports in the VDC in which you are working. When you move any of the port groups from this VDC, the shared buffer queuing feature returns to the default disabled state. When you move a port group into the VDC, the port group assumes the global shared buffer configuration of that VDC (for example, if shared buffering is enabled in the VDC, it will also be enabled for the newly moved port group). Finally, if all the port groups are removed from a given VDC with this feature enabled, the shared buffering for that VDC with no ports is returned to the default disabled state.

After you enable shared buffering, the shared buffer pools are configured, using the active template, on the default ingress queuing policy. If you change the template, the setting for shared buffering remains as you last set this feature, either enabled or disabled. Then, the shared buffers are reconfigured based on the ingress queuing policy of the new template. If no user-defined policies are attached to a port group, the same default ingress queuing policy is applied to the shared buffer pool as to the dedicated buffer pool.

Note You cannot change the template if you have any user-defined policies attached to the port group. You must first remove all user-defined queuing policies from the port group, and then you can change the template.

If you enable and configure shared buffer queuing, the shared buffer pools are used before the dedicated buffer queues. Any necessary dropped packets come from the dedicated buffer pools and pause is always honored from the dedicated buffer pools.

Note The cos2q maps and the dscp2 maps are global in scope. The same maps are applied to the shared buffer pools.

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 switch.
- You are in the correct VDC. A VDC is a logical representation of a set of system resources. You can use the **switchto vdc** command with a VDC number.

Guidelines and Limitations

Queuing and scheduling of F-Series modules have the following configuration guidelines and limitations:

- If a no-drop class is paused and the IP traffic is received with the CoS value of the no-drop class, IP traffic is queued in default queue due to the dscp-to-queue mapping behaviour. This is applicable to Cisco Nexus 7700 Series switches by default. Note that the dscp-to-queue mapping can be disabled.
- A queuing policy that is being activated should be consistent with the system network qos policy.
- The default queuing policy is attached to the system target (includes all F Series module ports), which is unlike the M1 series configuration where the default-in-policy is attached exclusively to each port.
- A queuing policy that is attached to a given port, overrides the system queuing policy on that port.
- The DSCP to egress queue selection for DSCP values 2-7 are set to be the same as the values for CoS 2-7. To change this setting, access the type QoS policy and use the set cos command to change the selected egress queue (applicable for all types of interfaces, such as access, trunk, routed, and so on).
- Egress policies on VLAN configurations do not support set match on CoS.
- Egress policies on VLAN configurations do not support set QoS group or discard class.
- The ingress type QoS policy supports **set dscp/cos** and **set qos-group** commands. You can configure either **set dscp/cos** or **set qos-group** command but not both. It is possible to migrate between these configurations at any time.
- F-Series modules do not support the following commands in a QoS policy:
  - **set discard-class** or **match discard-class**
  - **set qos-group** or **match qos-group**

- F Series modules do not support WRED in ingress queuing policies.
- F2 modules do not support CoS-to-queue mapping changes when M1 modules are also installed in the switch.
- F Series modules and M2 modules support shaping in the priority queue. M1 modules do not support shaping in the priority queue.
- F-Series modules and M2 modules support shaping in the priority queue. M1 modules do not support shaping in the priority queue.
- When using an L3 interface on F-series modules (F2/F2e/F3) in Cisco Nexus 7000 series it is mandatory to configure QoS mapping on DSCP instead of CoS.

  Do not configure the QoS mapping on Cos because when the matching happens on CoS the L3 control traffic is placed into the default class and could be dropped due to normal congestion.

  The QoS mapping is configured in the Admin VDC using **hardware qos dscp-to-queue ingress module-type all** command or **hardware qos dscp-to-queue ingress module-type f-series** command.
- See the following information about the default-nq-8e-4q4q-policy template that support four ingress buffers:
  - The default-nq-8e-4q4q-policy template is supported only with F2 modules.
  - When F1 modules are online, the default-nq-8e-4q4q-policy template cannot be attached to the system qos.
  - When the default-nq-8e-4q4q-policy template is attached to system qos, F1 modules are allowed to come online. However, all interfaces of the F1 modules go to the unallocated pool of the corresponding VDC.
  - To make software downgrades nondisruptive, the following is required before the software downgrade:
    - All user defined and cloned 8e-4q4q template queuing policies should be detached manually from all interfaces in each VDC.
    - The default-nq-8e-4q4q-policy or the user defined/cloned 8e-4q4q template network-qos policy should be detached from the system qos.
    - All user defined and cloned 8e-4q4q template network-qos policies should be removed manually from the default VDC.
    - All user defined 8e-4q4q template queuing policies should be removed manually from all VDCs.
    - Use the **clear qos policies 8e-4q4q** command in the default VDC to clear the default 8e-4q4q template policies. This command clears PPF (Policy Propagation Facility) nodes of 8e-4q4q template policies.
    - After executing **clear qos policies 8e-4q4q** command, you must perform an in-service software downgrade (ISSD). If an ISSD is not performed, unexpected results might occur.
  - The **clear qos policies 8e-4q4q** command is only supported in the default VDC. Using this command in the default VDC also clears the 8e-4q4q policy-maps in non-default VDCs.

  - Reloading an F2 module brings up all the cleared default 8e-4q4q template related policy-maps by using the **clear qos policies 8e-4q4q** command.
  - The default 8e-4q4q-policy template is published when a software upgrade is completed.

- See the following information about the Cisco 7710/7718 switches and the four default 4p8q policy templates that support eight egress queues on these switches:
  - The default 4q8q-policy templates are supported and enabled by default on the Cisco Nexus 7710 switch and Cisco Nexus 7718 switch only.
  - The default 4q8q-policy templates are supported on F2e modules only.
  - DSCP queuing is enabled by default on the Cisco Nexus 7710/7718 switches. You must use the **no hardware qos dscp-to-queue** command to disable DSCP queuing on the switch. You can use the **hardware qos dscp-to-queue command module type** command to reenable DSCP queuing.

- See the following information about the **match dscp** command:
  - Supports only the ingress queues for F2 modules for the 8E template. (It does not support egress queues, M1 queues, or fabric-qos queues.)
  - Supports only ingress queues that have at least one CoS value associated with it without any restriction on which CoS value is used.
  - Cannot be used in user-defined class maps.
  - Cannot be used in a user configuration session.
  - Must be disabled for ISSD. (If it is not disabled, the ISSD is disruptive).
  - DSCP to IVL mapping is disabled by default.
  - The **queue-limit** command cannot be specified based on CoS or DSCP values. The configured queue-limit sizes are applicable for both the DSCP and CoS values.
  - No additional statistics are generated to differentiate how many packets are matched on DSCP or CoS.
  - When DSCP to IVL is enabled, an interface uses the DSCP value as trusted for IP packets and the CoS value is trusted for non-IP packets.
  - DSCP to IVL mapping is enabled by default on the Cisco Nexus 7710/7718 switches. You must use the **no hardware qos dscp-to-queue** command to disable DSCP to IVL mapping.
  - DSCP to IVL mapping for FabricPath interfaces is not supported.
  - DSCP to IVL mapping for IPv6 packets is not supported.
  - DSCP to IVL mapping change is a disruptive operation and might cause BFD/routing protocols to flap.

- Shared buffer queuing between ports in a port group is available only on the F3 Series modules.
- Shared buffering is supported only in 8e and 8e-4q4q templates.
- Break-out ports do not support shared buffering.
- The M1, M2, F1, F2 and F2e modules do not support shared buffering.

- Ports in a port channel with a user-defined policy attached should have this same user-defined policy attached to the port groups.
- When a user-defined policy map is attached to a port group, the set cos and bandwidth commands are not applicable to the port group.
- Shared buffer queuing does not apply on the FEX Hif ports.
- When changing egress Class of Service (CoS) to queue mapping, ensure that you specify 2 or 3 seconds as the minimum time limit between changes. Otherwise, continuous traffic drop might occur.
- The M3 modules do not support per-queue counters for egress drops (multicast, unknown unicast, or broadcasts). The egress drops will be per port and per Q-Default counter.
- Only 8e templates are supported on M3 modules.
- The M3 module supports only network-qos template with default-nq-8e-4q8q-policy. It does not support default-nq-4e-4q8q-policy, default-nq-6e-4q8q-policy, default-nq-7e-4q8q-policy, and default-nq-8021qav-4q8q-policy.
- The M3 module supports only the network-qos template. This template contains all the CoS values that match the MTU size.
- All data traffic will be enqueued to the default queue of dot1q-tunnel port because this port is untrusted by default.
- Starting with Cisco NX-OS Release 8.0(1), the dscp-to-queue mapping for M3-Series modules is enabled by using the **hardware qos dscp-to-queue ingress module type f-series** command.

Configuring Queuing and Scheduling

You configure queuing and scheduling by creating policy maps of type queuing that you apply to either traffic direction of an interface. You can configure a queuing policy by following one of these methods:

- Copying predefined policy—You can copy a queuing policy template and modify it as needed.

Note When you copy an ingress or egress queuing policy, you are also copying the internal policies for the hierarchical queuing policy. Copying shortens the default policy name by stripping the *default* and *policy* substrings from it.

- User-defined policy—You can create a queuing policy that conforms to one of the system-defined queuing policy templates.

For information about configuring policy maps and class maps, see “Using Modular QoS CLI.”

Configuring an Ingress Queuing Policy

You must modify the ingress queuing policy only if you want to change the default policy that the port inherited from the system default.

Procedure

	Command or Action	Purpose
Step 1	switch# **qos copy policy type queuing default-4q-8e-in-policy** {**prefix** *prefix* | **suffix** *suffix*}	Copies a system-defined queuing policy and renames it with a prefix or suffix.
Step 2	(Optional) switch# **show policy-map type queuing** [*policy-map-name*]	Displays the queuing policy that you copied and renamed.
Step 3	switch# **configure terminal**	Enters global configuration mode.
Step 4	switch(config)# **policy-map type queuing** [*policy-map-name*]	Configures the policy map of type queuing and enters policy-map mode for the policy map name that you specify. The policy map names can contain alphabetic, hyphen, or underscore characters, are case sensitive, and can be up to 40 characters.
Step 5	switch(config)# **class type queuing** [**2q4t-8e-in-q-default** | **2q4t-8e-in-q1**]	Configures the class map of type queuing and then enters policy-map class queuing mode.
Step 6	switch(config)# **queue-limit percent** [*1-100*]	Sets the queue limit for the queue. The range is from 1 to 100. **Note** The total queue limit for all the queues in the policy cannot exceed 100. In this example, the queue limit is set to 40 percent in the 2q4t-8e-in-q-default and 60 percent in 2q4t-8e-in-q1.
Step 7	switch(config-pmap-c-que)# **bandwidth percent** [*1-100*]	Allocates the bandwidth to the CoS values mapped to the queues for exchanging with the peer. The range is from 1 to 100.
Step 8	switch(config-pmap-c-que)# **exit**	Exits policy-map queue mode and enters configuration mode.
Step 9	switch(config)# **service-policy type queuing input** [*policy-map-name*]	Applies a policy to an interface.
Step 10	(Optional) switch(config)# **show policy-map type queuing** [*policy-map-name*]	Displays information about all configured policy maps or a selected policy map of type queuing.
Step 11	(Optional) switch(config)# **show policy-map interface ethernet** [*slot/port*]	Displays information about the service policy on an Ethernet interface.

Configuring an Egress Queuing Policy

Procedure

	Command or Action	Purpose
Step 1	switch# **qos copy policy type queuing default-4q-8e-in-policy** {**prefix** *prefix* | **suffix** *suffix*}	Copies a system-defined queuing policy and renames it with a prefix or suffix.
Step 2	(Optional) switch# **show policy-map type queuing** [*policy-map-name*]	Displays the queuing policy that you copied and renamed.
Step 3	switch# **configure terminal**	Enters global configuration mode.
Step 4	switch(config)# **policy-map type queuing** [*policy-map-name*]	Configures the policy map of type queuing and enters policy-map mode for the policy map name that you specify. The policy map names can contain alphabetic, hyphen, or underscore characters, are case sensitive, and can be up to 40 characters.
Step 5	switch(config)# **class type queuing** [**1p3q1t-8e-out-pq1** | **1p3q1t-8e-out-q-default** | **1p3q1t-8e-out-q2** | **1p3q1t-8e-out-q3**]	Configures the class map of type queuing and then enters policy-map class queuing mode.
Step 6	switch(config-pmap-c-que)# **bandwidth percent** [*1-100*]	Allocates the bandwidth in all ingress packets to the value specified. The range is from 1 to 100. Alternatively, absolute values in Gbps, Mbps, Kbps can also be specified.
Step 7	switch(config-cmap-que)# **priority level** {**1** | **2**}	Marks the priority level of the traffic queue. 1 stands for the highest priority and 2 stands for the lowest priority.
Step 8	switch(config-cmap-que)# **shape** [**average** | **percent** {**1-100**}]	Shapes the traffic rate from a queue. The range is from 80000 bits per second to 10 Gigabytes per second.
Step 9	switch(config-pmap-que)# **exit**	Exits policy-map queue mode and enters configuration mode.
Step 10	switch(config)# **service-policy type queuing input** [*policy-map-name*]	Applies a policy to an interface.
Step 11	(Optional) switch(config)# **show policy-map type queuing** [*policy-map-name*]	Displays information about all configured policy maps or a selected policy map of type queuing.

Enabling DSCP to Queue Mapping

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **hardware qos dscp-to-queue ingress module type** {**all** | **f-series** | **m-series**}	Enables the dscp-to-queue mapping on the specified module(s). **Note** Starting with Cisco NX-OS Release 8.0(1), use the **f-series** keyword to enable dscp-to-queue mapping on M3-Series I/O modules also.
Step 3	(Optional) switch(config)# **show hardware qos dscp-to-queue ingress**	Displays information about the status of dscp-to-queue mapping in ingress direction.
Step 4	(Optional) switch(config)# **copy running-config startup-config**	Saves the running configuration to the startup configuration.

Configuring Shared Buffer Queuing

You enable or disable shared buffer queuing per module. You then specify the port group to change from the default queue limit ration of 50:50 for dedicated and shared pools.

Currently, the configuring shared buffer queuing functionality is not supported on M3 modules.

The default value is no shared buffer queuing.

Note This command is applicable only on an F3 Series module.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **hardware qos shared-buffer module** *module-number*	Enables the shared buffer queuing for the specified module. This command enables shared buffer queuing in the default ratio of 50:50 for dedicated:shared queues. The default value for shared buffer queuing is disabled. Use the **no** form of this command to disable shared buffer queuing on the specified module.

	Command or Action	Purpose
Step 3	(Optional) switch(config)# **hardware module** *module-number* **port-group** *port-group-number*	Enters the configuration for the specified port group on the module. If you want to change the default queue limit ratio, you do it by port group on the specified module.
Step 4	(Optional) switch(config-port-group)# **qos shared-buffer queue-limit** *percent*	Sets the queue limit for the shared buffer queue for the specified port group. The range is from 10 to 80 percent. **Note** The total queue limit for all the queues in the policy cannot exceed 100.
Step 5	(Optional) switch(config)# **copy running-config startup-config**	Saves the running configuration to the startup configuration.

Verifying the Queuing and Scheduling Configuration

To display the queuing policy configuration, perform one of the following tasks:

Note The **show** commands display only the default policies that correspond to the active template.

Command	Purpose
show queuing interface ethernet	Displays information about whether the queuing policy is applied correctly to the module.
show class-map type queuing	Displays information about all configured class maps or a selected class map of type queuing.
show policy-map type queuing	Displays information about all configured policy maps or a selected policy map of type queuing.
show policy-map system	Displays information about the network qos and queuing policy-maps that are currently in effect on the system.
show hardware qos dscp-to-queue	Shows the status of DSCP queuing.

When you modify a network QoS template, remove queuing policies, if any, that are attached exclusively on an F-Series module and M3 interface because these policies will be inconsistent with the new network QoS template.

For more information about the fields in the output of these commands, see the *Cisco Nexus 7000 Series NX-OS Quality of Service Command Reference* document.

Configuration Examples for Queuing and Scheduling on F-Series Modules

Example: Ingress Queuing Policy Configuration

The following example shows how to configure an ingress queuing policy:

```
policy-map type queuing p-4que-7e-drop-in
 class type queuing 4q4t-7e-in-q1
  queue-limit percent 45
  bandwidth percent 25
 class type queuing 4q4t-7e-in-q2
  queue-limit percent 10
  bandwidth percent 25
 class type queuing 4q4t-7e-in-q3
  queue-limit percent 45
  bandwidth percent 25
policy-map type queuing p-4que-7e-ndrop-in
 class type queuing 4q4t-7e-in-q4
  queue-limit percent 100
  bandwidth percent 25
policy-map type queuing p-4que-7e-in
 class type queuing c-4q-7e-drop-in
  service-policy type queuing p-4que-7e-drop-in
  queue-limit percent 70
 class type queuing c-4q-7e-drop-in
  service-policy type queuing p-4que-7e-ndrop-in
  queue-limit percent 30
```

Example: Egress Queuing Policy Configuration

The following example shows how to configure an egress queuing policy:

```
policy-map type queuing p-4que-6e-drop-out
 class type queuing 1q3p1t-6e-out-pq1
  priority level 1
  shape average percent 50
 class type queuing 1q3p1t-6e-out-q4
  bandwidth remaining percent 100
policy-map type queuing p-4que-6e-ndrop-out
 class type queuing 1q3p1t-6e-out-pq2
  priority level 1
  shape average percent 50
 class type queuing 1q3p1t-6e-out-pq3
  priority level 2
policy-map type queuing p-4que-6e-out
 class type queuing c-4q-6e-drop-out
  service-policy type queuing p-4que-6e-drop-out
  bandwidth percent 70
 class type queuing c-4q-6e-ndrop-out
  service-policy type queuing p-4que-6e-ndrop-out
  bandwidth percent 30
```

Example: Hierarchical Queuing Policy Configuration

The following example shows how to configure a hierarchical queuing policy:

```
policy-map type queuing inner-policy-1
 class type queuing 1p3q1t-out-q1
  bandwidth percent 40
 class type queuing 1p3q1t-out-q2
  bandwidth percent 60
policy-map type queuing inner-policy-2
 class type queuing 1p3q1t-out-q3
  bandwidth percent 40
 class type queuing 1p3q1t-out-q4
  bandwidth percent 60
 class-map type queuing drop-class
  match class-map 1p3q1t-out-q1
  match class-map 1p3q1t-out-q2
 class-map type queuing nodrop-class
  match class-map 1p3q1t-out-q3
  match class-map 1p3q1t-out-q4
policy-map type queuing example-hierarchical-policy
 class type queuing drop-class
  bandwidth percent 40
service-policy type queuing inner-policy-1
  match class nodrop-class
   percent 60
service-policy type queuing inner-policy-2
```

-

Example: Verifying the Status of DSCP-to-queue Mapping

The following sample output from the **show hardware qos dscp-to-queue ingress** command displays the status of DSCP-to-queue mapping enabled in ingress direction on F-series modules:

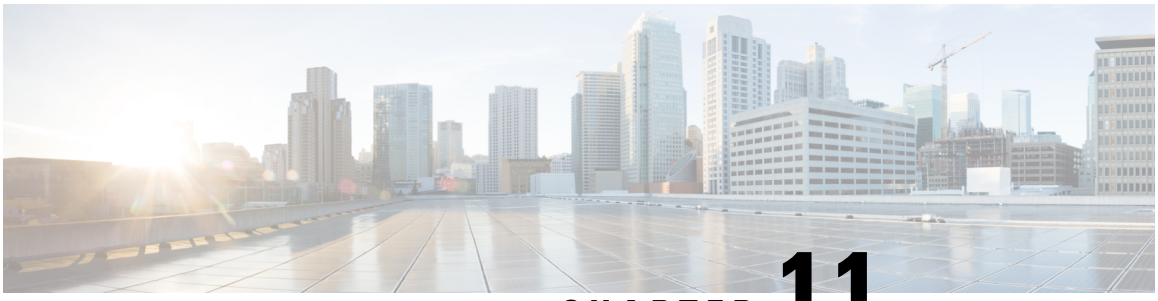
```
Switch# show hardware qos dscp-to-queue ingress

status: Enabled
module_type : f-series
```

Feature History for Queuing and Scheduling for F-Series Modules

The table below summarizes the new and changed features for this document and shows the releases in which each feature is supported. Your software release might not support all the features in this document. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release.

Table 36: Feature History for Queuing and Scheduling for F-Series Modules

Feature Name	Release	Feature Information
DSCP to Queue Mapping	8.0(1)	Use the **hardware qos dscp-to-queue ingress module type f-series** command to enable dscp-to-queue mapping on M3-Series I/O modules also.
Shared buffer queuing on the F3 Series modules	6.2(10)	Support for shared memory buffer queues on the F3 Series modules only.
DSCP to Queue Mapping	6.2(2)	Support for five default templates to enable DSCP to Queue Mapping on F-Series Modules. Support to enable DSCP to Queue mapping using **hardware qos dscp-to-queue ingress module-type** command.
Support for 4q8q policy templates	6.2(2)	Support for four 4q8q policy templates that provide eight egress queues on the Cisco Nexus 7710 switch and Cisco Nexus 7718 switch only.
Support for four ingress buffers	6.1(3)	Support for default-8e-4q4q-policy template that supports four ingress buffers.
DSCP mapping for F2 modules	6.1(1)	Support for DSCP mapping for F2 modules.
Scheduling and Queuing for F1 Series Modules	5.1(1)	This chapter was added. (Chapter title subsequently changed to accommodate other F-Series Modules.)



CHAPTER 11

Configuring Network QoS

This chapter describes how to configure a network qos policy for the Cisco NX-OS device in the Data Center Bridging (DCB) network.

Note This chapter applies to the F-Series I/O modules only.

Finding Feature Information

Your software release might not support all the features documented in this module. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the "New and Changed Information"chapter or the Feature History table in this chapter.

Information About Network QoS

A Data Center Bridging (DCB) network, which is also referred to as a DCB cloud, is a network that provides I/O consolidation. This network consists of switches that support class of service (CoS)-based traffic differentiation. The DCB network carries different types of traffic such as storage area network (SAN), local area network (LAN), and inter-process communication (IPC) traffic. The SAN traffic is sensitive to packet drops and relies on in-order delivery, which means that the traffic is delivered (frames and packets) in the same order in which it was sent. The LAN traffic allows dropping of packets and is delivered on a best-effort

basis. The LAN traffic can have a different level of priority and a chance of being delivered in a timely manner during congestion. The IPC networks require very low latency. Therefore, a DCB network must support traffic differentiation and provide quality of service (QoS).

In a DCB network, virtual links (VLs) are used to differentiate traffic classes. VLs, which are an extension of CoS, enable traffic differentiation and are carried in the priority bits of the 802.1Q or S-Tag.CoS allows forming of a physical link into multiple logical links so that the traffic in the CoS does not affect the traffic on the other CoS.

A DCB network has eight CoS values. All traffic that enters the DCB cloud must be mapped into one of these eight CoS values. Each frame in a DCB network belongs to a CoS. You can define the CoS by a set of parameters that gives a specific behavior to the CoS.

The network qos policy defines the characteristics of each CoS value, which are applicable network wide across virtual device contexts (VDCs) and switches. With a network qos policy, you can configure the following:

- Pause behavior—You can decide whether a CoS requires the lossless behavior (the lossless behavior is provided by using a priority flow control (PFC) mechanism that prevents packet loss during congestion) or not. You can configure drop (frames with this CoS value can be dropped) and no drop (frames with this CoS value cannot be dropped). For the drop and no drop configuration, you also need to enable PFC per port. For more information about PFC, see “Configuring Priority Flow Control.”
- Congestion Control Mechanisms—You can select either tail drop (TD, which drops frames without differentiation based on the per-VL occupancy) or Weighted Random Early Detection (WRED, which drops frames without differentiation based on the per-VL occupancy and the probability factor) only for a drop CoS. By default, TD is enabled for drop CoS in the default policies. Any of the burst-optimized or mesh-optimized thresholds for TD and WRED can be selected for the packet-drop algorithm based on the traffic pattern expected for the CoS. If no congestion control algorithm is selected, and congestion occurs, a hard tail-drop that is based on a single threshold occurs for the drop CoS.
- MTU—You can set the maximum transmission unit (MTU) or maximum payload length for CoS. The MTU range is from 1500 to 9216. The MTU must be smaller than the system jumbo MTU in all VDCs. The MTU must be the same for the CoS that is mapped to the same ingress queue. For more information about the ingress queue, see “Configuring Queuing and Scheduling on F-Series I/O Modules.”
- Protocols—You can select Fibre Channel over Ethernet (FCoE), iSCSI, or TCP as the protocol for a CoS value. The protocol value is used in the DCB Exchanges.

Differences in Drop CoS and No-Drop CoS Values

The table below shows the drop and no-drop CoS values for the different policy templates.

Table 37: Differences in Drop CoS and No-Drop CoS Values

Templates		
default-4q-8e-policy	0–7	—
default-4q-7e-policy	0–2, 4–7	3
default-4q-6e-policy	0–2, 5–7	3, 4
default-4q-4e-policy	0, 5, 6, 7	1– 4

Templates		
default-8e-4q4q-policy	0–7	—
default-8e-4q8q-policy (on Cisco Nexus 7706/7710/7718 switches only)	0–7	—
default-7e-4q8q-policy (on Cisco Nexus 7706/7710/7718 switches only)	0–2 , 4–7	3
default-6e-4q8q-policy (on Cisco Nexus 7706/7710/7718 switches only)	0–2, 5–7	3, 4
default-4e-4q8q-policy (on Cisco Nexus 7706/7710/7718 switches only)	0, 5, 6, 7	1–4

Queue Names and Default Mappings of CoS Values to Egress/Ingress Queues

The table below shows the queue names and default mappings of CoS values to egress and ingress queues

Table 38: Queue Names and Default Mappings of CoS Values to Egress/Ingress Queues

Templates	Queue Names for Ingress Queues	Ingress CoS Values	Queue Names for Egress Queues	Egress Cos Values	Priority CoS Value
default-4q-8e-policy	2q4t-8e-in-q1	5–7	1p3q1t-8e-out-pq1	5–7	5–7
	2q4t-8e-in-q-default	0–4	1p3q1t-8e-out-q2	3–4	
			1p3q1t-8e-out-q3	2	
			1p3q1t-8e-out-q-default	0-1	
default-4q-7e-policy	4q4t-7e-in-q1	5–7	1p3q1t-7e-out-pq1	5–7	5–7
	4q4t-7e-in-q-default	0–1	1p3q1t-7e-out-q2	3	
	4q4t-7e-in-q3	2,4	1p3q1t-7e-out-q3	2,4	
	4q4t-7e-in-q4	3	1p3q1t-7e-out-q-default	0,1	
default-4q-6e-policy	4q4t-6e-in-q1	5–7	3p1q1t-6e-out-pq1	5–7	5–7
	4q4t-6e-in-q-default	0-2	3p1q1t-6e-out-pq2	4	4
	4q4t-6e-in-q3	4	3p1q1t-6e-out-pq3	3	3
	4q4t-6e-in-q4	3	3p1q1t-6e-out-q-default	0–2	

Templates	Queue Names for Ingress Queues	Ingress CoS Values	Queue Names for Egress Queues	Egress Cos Values	Priority CoS Value
default-4q-4e-policy	4q4t-4e-in-q1 4q4t-4e-in-q-default 4q4t-4e-in-q3 4q4t-4e-in-q4	5–7 0 4 1-3	2p2q1t-4e-out-pq1 2p2q1t-4e-out-pq2 2p2q1t-4e-out-q3 2p2q1t-4e-out-q-default	5–7 4 1–3 0	5–7 4
default-8e-4q4q-policy	4q1t-8e-4q4q-in-q1 4q1t-8e-4q4q-in-qdefault 4q1t-8e-4q4q-in-q3 4q1t-8e-4q4q-in-q4	5–7 0,1 3,4 2	1p3q1t-8e-4q4q-out-pq1 1p3q1t-8e-4q4q-out-q2 1p3q1t-8e-4q4q-out-q3 1p3q1t-8e-4q4qout-q-default	5–7 0,1 3,4 2	5–7
default-8e-4q8q-policy (Cisco Nexus 7710/ 7718 switches only)	8e-4q8q-in-q1 8e-4q8q-in-q-default 8e-4q8q-in-q3 8e-4q8q-in-q4	5–7 0–4 — —	8e-4q8q-out-q1 (priority queue) 8e-4q8q-out-q2 8e-4q8q-out-q3 8e-4q8q-out-q4 8e-4q8q-out-q5 8e-4q8q-out-q6 8e-4q8q-out-q7 8e-4q8q-out-q-default	5 7 6 4 3 2 1 0	5 (Drop category)

Templates	Queue Names for Ingress Queues	Ingress CoS Values	Queue Names for Egress Queues	Egress Cos Values	Priority CoS Value
default-7e-4q8q-policy (Cisco Nexus 7710/ 7718 switches only)	default-7e-4q8qdrop-in-policy: 7e-4q8q-in-q1 7e-4q8q-in-q-default 7e-4q8q-in-q3	5–7 0–1 2–4	default-7e-4q8qdrop-out-policy: 7e-4q8q-out-q1 (priority queue) 7e-4q8q-out-q2 7e-4q8q-out-q3 7e-4q8q-out-q4 7e-4q8q-out-q6 7e-4q8q-out-q7 7e-4q8q-out-q-default	5 7 6 4 2 1 0	5 (Drop category)
	default-7e-4q8qndrop-in-policy: 7e-4q8q-in-q4	3	default-7e-4q8qndrop-out-policy: 7e-4q8q-out-q5	3	
default-6e-4q8q-policy (Cisco Nexus 7710 /7718 switches only)	default-6e-4q8qdrop-in-policy: 6e-4q8q-in-q1 6e-4q8q-in-q-default	5–7 0-2	default-6e-4q8qdrop-out-policy: 6e-4q8q-out-q1 (priority queue) 6e-4q8q-out-q2 6e-4q8q-out-q3 6e-4q8q-out-q6 6e-4q8q-out-q7 6e-4q8q-out-q-default	5 7 6 2 1 0	5 (Drop category)
	default-6e-4q8qndrop-in-policy: 6e-4q8q-in-q3 6e-4q8q-in-q4	4 3	default-6e-4q8qndrop-out-policy: 6e-4q8q-out-q4 (priority queue) 6e-4q8q-out-q5 (priority queue)	4 3	4 (no drop category, highest priority) 3 (2nd highest priority)

Templates	Queue Names for Ingress Queues	Ingress CoS Values	Queue Names for Egress Queues	Egress Cos Values	Priority CoS Value
default-4e-4q8q-policy (Cisco Nexus 7710/ 7718 switches only)	default-4e-4q8qdrop-in-policy: 4e-4q8q-in-q1 4e-4q8q-in-q-default	5–7 0	default-4e-4q8qdrop-out-policy:		5 (Drop category)
			4e-4q8q-out-q1 (priority queue) 4e-4q8q-out-q2 4e-4q8q-out-q3 4e-4q8q-out-q-default	5 7 6 0	
	default-4e-4q8qndropout-policy: 4e-4q8q-in-q3 4e-4q8q-in-q4	4 1–3	default-4e-4q8q-ndropout-policy:		4 (no drop category)
			4e-4q8q-out-q4 (priority queue) 4e-4q8q-out-q5 4e-4q8q-out-q6 4e-4q8q-out-q7	4 3 2 1	

Default DSCP Mappings

The table below shows the default DSCP values to Ingress queues for the Cisco Nexus 7710/7718 switches.

Table 39: Default DSCP Mappings on Cisco Nexus 7710/7718 Switches

Template	Ingress Queue	Default DSCP Mappings
default-8e-4q8q-policy	8e-4q8q-in-q-default	0-39
	8e-4q8q-in-q1	40-63
	8e-4q8q-in-q4	0-39
	8e-4q8q-in-q3	0-39
default-7e-4q8q-policy	7e-4q8q-in-q-default	0-15
	7e-4q8q-in-q1	40-63
	7e-4q8q-in-q4	—
	7e-4q8q-in-q3	16-39

Template	Ingress Queue	Default DSCP Mappings
default-6e-4q8q-policy	6e-4q8q-in-q-default	0-39
	6e-4q8q-in-q1	40-63
	6e-4q8q-in-q4	—
	6e-4q8q-in-q3	—
default-4e-4q8q-policy	4e-4q8q-in-q-default	0-39
	4e-4q8q-in-q1	40-63
	4e-4q8q-in-q4	—
	4e-4q8q-in-q3	—

In a default network policy template name, the numbers 4, 6, 7, and 8 denote the number of the drop CoS that is defined in the policy and e denotes Ethernet.

Note The 4q8q policy templates are supported and enabled by default on the Cisco Nexus 7710 switch and the Cisco Nexus 7718 switch only.

Note For the default-8e-4q8q-in-policy, as the ingress buffers are limited to two queues (8e-4q8q-in-q1 and 8e-4q8q-in-q-default), you must change the queue limit by using the queue limit command, before any CoS2q / dscp-to-queue mapping changes are made to 8e-4q8q-in-q3 and 8e-4q8q-in-q4.

The network qos policy templates are created when the first F-Series module becomes operational or the templates are saved in the start-up configuration.

Note A policy that does not conform to a system-defined policy template is currently not supported.

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 switch.
- You are in the default VDC. A VDC is a logical representation of a set of system resources. You can use the **switchto vdc** command with a VDC number.

Guidelines and Limitations

The network QoS policy has the following configuration guidelines and limitations:

Note These guidelines and limitations are applicable to all F-Series edge, M3, and FabricPath mode ports.

- You must configure and apply a network qos policy only to the default VDC.
- Selecting a template with a no-drop CoS value does not automatically give no-drop behavior to it. The no-drop behavior is enabled for those CoS values only on ports where priority flow control (PFC) is successfully negotiated or turned on.
- When the port MTU is configured on an interface, it overrides the network qos MTU.
- In releases earlier than Cisco NX-OS Release 6.2(1), the Fabric Extender (FEX) interfaces do not support the MTU changes made to a QoS policy template.
- The FEX port channel requires a minimum MTU setting of 1058 for traffic with CoS 5–CoS 7. The FEX fails when the MTU is less than 1058 and does not register with the switch.
- Changing the network qos policy is a disruptive operation and it can cause traffic drops on any or all ports across VDCs.
- DCB network qos policies pertain to F-Series modules. DCE network qos policies are created only when DCE network enabled line cards are inserted into a chassis.

PFC and F1 Series Module Ports

- When PFC is enabled on a port, precision time protocol (PTP) is not supported on the port.
- The pong utility is not supported on a VDC when PFC is enabled on any of the ports in the same VDC.
- PFC is not supported when PTP is enabled on the same port or when the pong utility is enabled in the same VDC.

Configuring iSCSI

- As a best practice, both iSCSI and FCoE should be configured on the same CoS (vl) in the network-qos policy for the default-nq-7e-policy and default-nq-6e-policy templates.
  - Avoid using CoS 4 for iSCSI in the default-nq-6e-policy template.

    (CoS 4 is reserved for no-drop control traffic.)
  - Avoid using CoS 4 for iSCSI in the default-nq-4e-policy template.

    (CoS 4 is reserved for no-drop control traffic.)
  - Configure the network-qos policy with MTU = 2112 if iSCSI shares the CoS (vl) with FCoE.

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 template that fits your requirement. For more information about the predefined policies, see Table 39: Default DSCP Mappings on Cisco Nexus 7710/7718 Switches, on page 140. By default, default-nq-8e-policy is configured. The numbers denote the number of drop (Ethernet) CoS values. The template CoS values are chosen based on standard conventions and usage patterns.
- Copying the predefined templates—You can copy a network qos policy template and modify it as needed. Copying a network qos policy trims the default policy name by stripping the default and policy substrings from it.
- User-defined policy—You can create a network qos policy that conforms to one of the system-defined policy templates.
-

Note Ports that are in the nondefault virtual device contexts (VDCs) inherit the network qos policy from the default VDC.

You can copy and modify a network qos policy template and use the network qos policy commands only from the default-vdc.

Copy a predefined network qos policy template:

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **qos copy policy-map type network-qos default-nq-7e-policy** {**prefix** *prefix* | **suffix** *suffix*}	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 3	switch(config)# **show policy-map type network-qos**	Displays the type network qos policy map.

Configure a User-Defined Network

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.

	Command or Action	Purpose
Step 2	switch(config)# **class-map type network-qos match-any** {*class-map-name*}	Configures the class map of the type network-qos, specifies the class map name as eth, and enters class-map mode.
Step 3	switch(config-cmap-nqos)# **match cos** [*0-7*]	Specifies the CoS value to match. The range is from 0 to 7.
Step 4	switch(config-cmap-nqos)# **class-map type network-qos match-any** {*class-map-name*}	Specifies the type network qos class name.
Step 5	switch(config-cmap-nqos)# **match protocol** [**fcoe** | **iscsi** | **tcp**]	Specifies the CoS value to match and specifies which protocol has to be mapped to a given CoS value.
Step 6	switch(config-cmap-nqos)# **match cos** [*0-7*]	Specifies the CoS value to match. The range is from 0 to 7.
Step 7	switch(config-cmap-nqos)# **class-map type network-qos match-any** {*class-map-name*}	Specifies the type network qos class name.
Step 8	switch(config-cmap-nqos)# **match cos** [*0-7*]	Specifies the CoS value to match. The range is from 0 to 7.
Step 9	switch(config-cmap-nqos)# **policy-map type network-qos** [*my_template*]	Creates or accesses the policy map. The policy-map name can contain alphabetic, hyphen, or underscore characters, is case sensitive, and can be up to 40 characters.
Step 10	switch(config-pmap-nqos-c)# **class type network-qos eth**	Refers to the class map of type network qos as configured in Step 2.
Step 11	switch(config-pmap-nqos-c)# **no pause**	Specifies drop for the CoS.
Step 12	switch(config-pmap-nqos-c)# **mtu** [*mtu_size*]	Specifies the MTU or the payload length. The range is from 1500 to 9216. The MTU size in this example is set to 1600.
Step 13	switch(config-pmap-nqos-c)# **congestion-control** [**random-detect** {**threshold** [**burst-optimized** | **mesh-optimized**]} | **tail-drop**{**threshold** [**burst-optimized** | **mesh-optimized**]}]	Specifies either the WRED or TD congestion control protocol and the thresholds optimized for bursty or mesh traffic.
Step 14	switch(config-pmap-nqos-c)# **class type network-qos**	Configures the class map of type network-qos and specifies the class map name.
Step 15	switch(config-pmap-nqos-c)# **pause**	Specifies no-drop. The default is **no pause**.
Step 16	switch(config-pmap-nqos-c)# **class type network-qos**	Configures the class map of type network-qos and specifies the class map name.
Step 17	switch(config-pmap-nqos-c)# **pause**	Specifies no-drop. The default is **no pause**.

	Command or Action	Purpose
Step 18	switch(config-pmap-nqos-c)# **mtu** [*mtu_size*]	Specifies the MTU value. The range is from 1500 to 9216.
Step 19	switch(config-pmap-nqos-c)# **exit**	Exits policy-map network-qos mode and enters global configuration mode.

Applying a Network QoS Policy on a Target

You apply a network qos policy only globally on a system across VDCs. Applying a network qos policy also automatically applies the corresponding queuing policies.

To apply a network qos policy to a target, use the **service-policy** command.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **system qos**	Enters system qos mode.
Step 3	switch(config-sys-qos)# **service-policy type network-qos** {*my_template*}	Adds the policy map to the input or output packets of system.
Step 4	switch(config-sys-qos)#**exit**	Exits config-sys-qos mode and enters configuration mode.

Verifying the Network QoS

To display the network qos policy configuration, 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.

For detailed information about the fields in the output from these commands, see the *Cisco Nexus 7000 Series NX-OS Quality of Service Command Reference*.

Configuration Examples for Network QoS

The following example shows how to configure a network QoS policy:

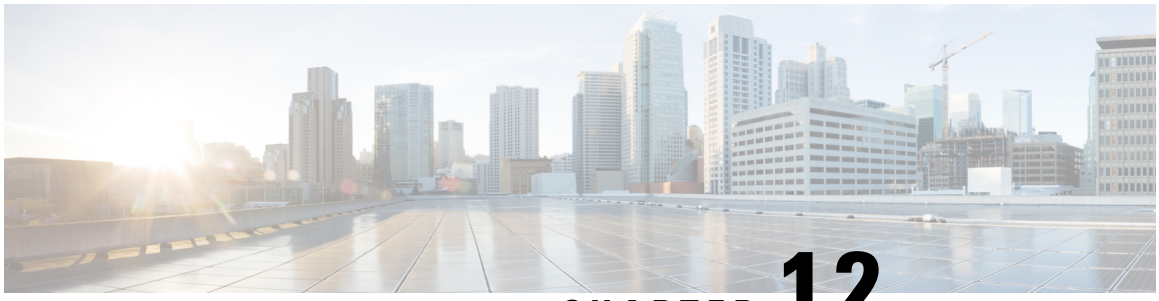
```
policy-map type network-qos default-nq-6e-policy
  class type network-qos c-nq-6e-drop
   match cos 0-2,5-7
   congestion-control tail-drop
   mtu 1500
  class type network-qos c-nq-6e-ndrop-fcoe
   match cos 3
   match protocol fcoe
   pause
   mtu 2112
  class type network-qos c-nq-6e-ndrop
   match cos 4
   pause
   mtu 1500
```

Feature History for Network QoS

The table below summarizes the new and changed features for this document and shows the releases in which each feature is supported. Your software release might not support all the features in this document. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release.

Table 40: Feature History for Network QoS

Feature Name	Release	Feature Information
Support for 4q8q policy templates	6.2(2)	Support for four 4q8q templates that provide eight egress queues for the Cisco Nexus 7710 switch and Cisco Nexus 7718 switch only.
Support for four ingress buffers	6.1(3)	Support for the default-8e-4q4q-policy template that supports four ingress buffers.
network-qos policy	5.1(1)	This feature was introduced.



CHAPTER 12

Configuring Priority Flow Control

This chapter describes how to configure priority flow control (PFC) on the Cisco NX-OS device.

Finding Feature Information

Your software release might not support all the features documented in this module. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the "New and Changed Information"chapter or the Feature History table in this chapter.

Information About Priority Flow Control

Priority flow control (PFC; IEEE 802.1bb), 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) or link-level flow control (LFC). However, PFC functions on a per class-of-service (CoS) basis.

When a buffer threshold is exceeded due to congestion, LFC sends a pause frame to its peer to pause all data transmission on the link for a specified period of time. When the congestion is mitigated (traffic comes under the configured threshold), a resume frame is generated to restart data transmission on the link.

In contrast, 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.

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 switch.
- You are in the VDC. A VDC is a logical representation of a set of system resources. You can use the **switchto vdc** command with a VDC number.

Guidelines and Limitations

PFC has the following configuration guidelines and limitations:

- If PFC is enabled on a port or a port channel, it does not cause a port flap.
- A flap occurs when both the PFC and LFC are enabled and PFC is disabled before LFC is configured.
- PFC configuration enables PFC in both the send (Tx) and receive (Rx) direction.
- PFC on mode is used to support the hosts that support PFC but do not support the Data Center Bridging Capability Exchange Protocol (DCBXP).
- Only an exact match of the no-drop CoS is considered as a successful negotiation of PFC by the DCBXP.
- M3 modules do not support Priority Flow Control.

PFC and F1 Series Module Ports

- When PFC is enabled on a port, precision time protocol (PTP) is not supported on the port.
- The pong utility is not supported on a VDC when PFC is enabled on any of the ports in the same VDC.
- PFC is not supported when PTP is enabled on the same port or when the pong utility is enabled in the same VDC.

Default Settings for Priority Flow Control

Table 41: Default PFC Settings

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 three 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 also enable Link-level Flow Control (LFC) on the same port in which PFC is enabled. However, PFC, if enabled, always gets the priority.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **interface ethernet** [*slot/port-number*]	Enters interface mode on the interface specified.
Step 3	switch(config-if)# **priority-flow-control mode** {**auto** | **off** | **on**}	Sets the PFC to the auto, off, or on mode. By default, PFC mode is set to auto on all ports.
Step 4	(Optional) switch(config-if)# **show interface priority-flow-control**	Displays the status of PFC on all interfaces.

Verifying the Priority Flow Control Configuration

Command	Purpose
show interface priority-flow-control	Displays the status of PFC on all interfaces.

For detailed information about the fields in the output from these commands, see the *Cisco Nexus 7000 Series NX-OS Quality of Service Command Reference*.

Configuration Examples for Priority Flow Control

The following example shows how to configure PFC:

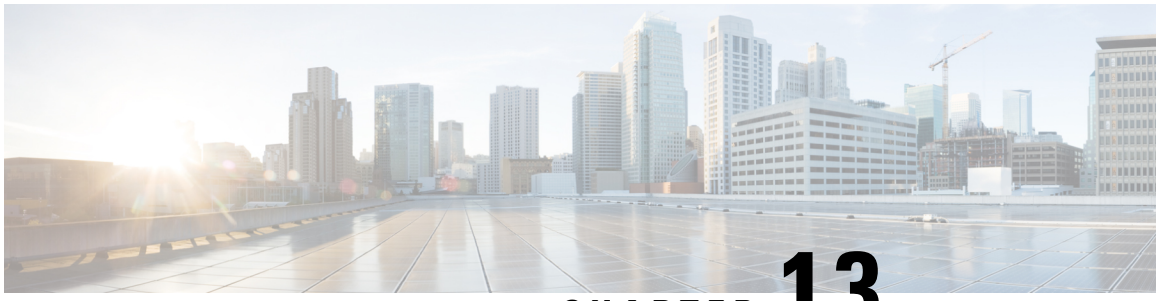
```
configure terminal
 interface ethernet 5/5
 priority-flow-control mode on
```

Feature History for Priority Flow Control

The table below summarizes the new and changed features for this document and shows the releases in which each feature is supported. Your software release might not support all the features in this document. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release.

Table 42: Feature History for PFC

Feature Name	Release	Feature Information
PFC	5.1(1)	This feature was introduced.



CHAPTER 13

Configuring Local Policy-Based Routing

This chapter describes how to configure local policy-based routing (PBR) on the Cisco NX-OS device.

Finding Feature Information

Your software release might not support all the features documented in this module. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the "New and Changed Information"chapter or the Feature History table in this chapter.

Information About Local Policy-Based Routing

Local policy-based routing allows you to configure a defined policy for IPv6 traffic flows, lessening reliance on routes derived from routing protocols. All packets received on an interface with local policy-based routing are configured in route maps. The route maps dictate the policy, determining where to forward packets.

Route maps are composed of match and set statements that you can mark as permit or deny. You can interpret the statements as follows:

- If the packets match any route map statements, all the set statements are applied. One of these actions involves choosing the next hop.
- If a statement is marked as deny, the packets that meet the match criteria are sent back through the normal forwarding channels and destination-based routing is performed.

If the statement is marked as permit and the packets do not match any route-map statements, the packets are sent back through the normal forwarding channels and destination-based routing is performed.

Route Maps

You can use route maps for route redistribution or policy-based routing. Route map entries consist of a list of match and set criteria. The match criteria specify match conditions for incoming routes or packets, and the set criteria specify the action taken if the match criteria are met.

You can configure multiple entries in the same route map. These entries contain the same route map name and are differentiated by a sequence number.

You create a route map with one or more route map entries arranged by the sequence number under a unique route map name. The route map entry has the following parameters:

- Sequence number
- Permission—permit or deny
- Match criteria
- Set changes

By default, a route map processes routes or IP packets in a linear fashion, that is, starting from the lowest sequence number. You can configure the route map to process in a different order using the continue statement, which allows you to determine which route map entry to process next.

Match Criteria

You can use a variety of criteria to match a route or IP packet in a route map. When Cisco NX-OS processes a route or packet through a route map, it compares the route or packet to each of the match statements configured. If the route or packet matches the configured criteria, Cisco NX-OS processes it based on the permit or deny configuration for that match entry in the route map and any set criteria configured.

The match categories and parameters are as follows:

- IP access lists—(For policy-based routing only). Match based on source or destination IP address, protocol, or QoS parameters.

Set Changes

Once a route or packet matches an entry in a route map, the route or packet can be changed based on one or more configured set statements.

The set changes are as follows:

- Policy-based routing only—Change the interface or the default next-hop address.

Prerequisites for Local Policy-Based Routing

Local policy-based routing has the following prerequisites:

- Install the correct license.
- You must enable local policy-based routing (see the "Enabling the Policy-Based Routing Feature" section).
- Assign an IP address on the interface and bring the interface up before you apply a route map on the interface for policy-based routing.
- If you configure VDCs, install the appropriate license and enter the desired VDC (see the *Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide* for configuration information and the *Cisco NX-OS Licensing Guide* for licensing information).

Guidelines and Limitations

Local policy-based routing has the following configuration guidelines and limitations:

- A local policy-based routing route map can have only one match or set statement per route-map statement.
- A **match** command cannot refer to more than one ACL in a route map used for local policy-based routing.
- An ACL used in a local policy-based routing route map cannot include a deny statement.
- The same route map can be shared among different interfaces for local policy-based routing as long as the interfaces belong to the same virtual routing and forwarding (VRF) instance.
- Setting a tunnel interface or an IP address via a tunnel interface as a next hop in a local policy-based routing policy is not supported.

Default Settings for Local Policy-Based Routing

Table 43: Default Local Policy-based Routing Setting

Parameter	Default
Local policy-based routing	Disabled

Configuring Local Policy-Based Routing

Configuring Route Maps

You can use route maps for route redistribution or route filtering. Route maps can contain multiple match criteria and multiple set criteria.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters configuration mode.

	Command or Action	Purpose
Step 2	switch(config)# **route-map** *map-name* [**permit** | **deny**] [*seq*]	Creates a route map or enters route-map configuration mode for an existing route map. Use seq to order the entries in a route map.
Step 3	(Optional) switch(config-route-map)# **continue** *seq*	Determines what sequence statement to process next in the route map. Used only for filtering and redistribution.
Step 4	(Optional) switch(config-route-map)#**exit**	Exits route-map configuration mode.
Step 5	(Optional) switch(config)# **copy running-config startup-config**	Saves this configuration change.

You can configure the following optional match parameters for route maps in route-map configuration mode:

Procedure

	Command or Action	Purpose
Step 1	switch(config-route-map)# **match ipv6 address ip access list** *number*	Matches against one or more IP access lists.

You can configure the following optional set precedence parameter for route maps in route-map configuration mode:

Procedure

	Command or Action	Purpose
Step 1	[**no**] **set precedence** {**number** | **name**}	Sets the IPv6 precedence for policy-based routing. The options are as follows: • 0—routine • 1—priority • 2—immediate • 3—flash • 4—flash-override • 5—critical • 6—internet • 7—network Use the **no** form of this command to disable the feature.

Enabling the Policy-Based Routing Feature

You must enable the policy-based routing feature before you can configure a route policy.

Before you begin

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters configuration mode.
Step 2	switch(config)# [**no**] **feature pbr**	Enables the policy-based routing feature. Use the **no** form of this command to disable the feature.
Step 3	(Optional) switch(config)# **show feature**	Displays enabled and disabled features.
Step 4	(Optional) switch(config)# **copy running-config startup-config**	Saves this configuration change.

Configuring a Local Route Policy

You use route maps in local policy-based routing to assign routing policies.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters configuration mode.
Step 2	switch(config)# **feature pbr**	Enables the policy-based routing feature.
Step 3	switch(config)# [**no**] **ipv6 local policy route-map** *map-name*	Assigns a route map for local policy-based routing to the interface. Use the **no** form of this command to disable the feature.
Step 4	(Optional) switch(config)# **show ipv6 local policy**	Displays information about the policy.
Step 5	(Optional) switch(config)# **copy running-config startup-config**	Saves this configuration change.

Verifying the Local Policy-Based Routing Configuration

To display the local policy-based routing configuration, perform the following task:

Command	Purpose
show ipv6 local policy	Displays information about the local IPv6 policy.
show route-map *name*	Displays information about a route map.

For detailed information about the fields in the output from these commands, see the *Cisco Nexus 7000 Series NX-OS Quality of Service Command Reference*.

Configuration Example for Local Policy-Based Routing

This example shows how to configure a simple local route policy on an interface:

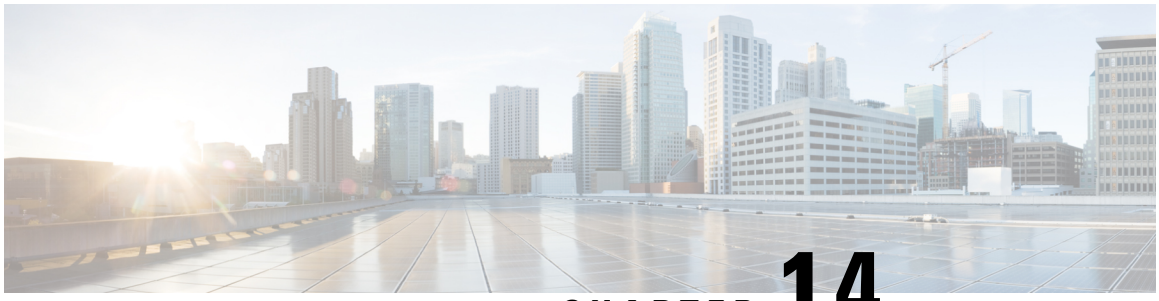
```
feature pbr
route-map Testmap, permit, sequence 10
  ip address 10
  ip next-hop
  ip precedence: internet
```

Feature History for Local Policy-Based Routing

The table below summarizes the new and changed features for this document and shows the releases in which each feature is supported. Your software release might not support all the features in this document. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release.

Table 44: Feature History for Local Policy-Based Routing

Feature Name	Release	Feature Information
Local Policy-Based Routing	6.2(2)	This feature was introduced.



CHAPTER 14

Monitoring QoS Statistics

This chapter describes how to enable, display, and clear QoS statistics on the Cisco NX-OS device.

Finding Feature Information

Your software release might not support all the features documented in this module. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the "New and Changed Information"chapter or the Feature History table in this chapter.

Information 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.

Prerequisites for Monitoring QoS Statistics

Monitoring QoS statistics has the following prerequisites:

- You must be familiar with the concepts in “Using Modular QoS CLI.”
- You must log in to the switch.
- You are in the correct VDC. A VDC is a logical representation of a set of system resources. You can use the **switchto vdc** command with a VDC number.

Enabling Statistics

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

Note On M1 modules, when QoS statistics are disabled, the output from the show policy-map interface num type queuing command might be delayed by as much as 90 seconds.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# [**no**] **qos statistics**	Enables QoS statistics on all interfaces. The **no** option disables QoS statistic
Step 3	(Optional) switch(config)# **show policy-map interface**	Displays the statistics status and the configured policy maps on all interfaces.
Step 4	(Optional) switch(config)# **show policy-map vlan**	Displays the statistics status and the configured policy maps on all VLANs.
Step 5	(Optional) switch(config)# **copy running-config startup-config**	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.

Procedure

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

Clearing Statistics

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

Procedure

	Command or Action	Purpose
Step 1	switch# **clear qos statistics** [**interface**] [**vlan**] [**input** | **output**] [**type** {**qos** | **queuing**}]	Displays statistics and the configured policy maps on all interfaces or the specified interface, all VLANs or the specified VLANs, data direction, or QoS type.

Configuration Examples For Monitoring QoS Statistics

The following example shows how to display the QoS statistics:

```
switch(config)# show policy-map interface ethernet 8/1

Global statistics status: enabled
Ethernet8/1
Service-policy (qos) input: pmap
policy statistics status: enabled
Class-map (qos): map (match-all)
0 packets, 0 bytes
5 minute offered rate 0 bps, drop rate 0 bps
Match: cos 0
police cir 10 mbps bc 200 ms
conformed 0 bytes, 0 bps action: transmit
violated 0 bytes, 0 bps action: drop
Class-map (qos): map1 (match-all)
0 packets, 0 bytes
5 minute offered rate 0 bps, drop rate 0 bps
Match: dscp 0
police cir 10 mbps bc 200 ms
conformed 0 bytes, 0 bps action: transmit
violated 0 bytes, 0 bps action: drop
Class-map (qos): map2 (match-all)
0 packets, 0 bytes
5 minute offered rate 0 bps, drop rate 0 bps
Match: precedence 5
police cir 20 mbps bc 200 ms
conformed 0 bytes, 0 bps action: transmit
violated 0 bytes, 0 bps action: drop
Class-map (qos): map3 (match-all)
0 packets, 0 bytes
5 minute offered rate 0 bps, drop rate 0 bps
Match: cos 3
police cir 30 mbps bc 200 ms
conformed 0 bytes, 0 bps action: transmit
violated 0 bytes, 0 bps action: drop
Class-map (qos): map4 (match-all)
0 packets, 0 bytes
5 minute offered rate 0 bps, drop rate 0 bps
Match: packet length 100
police cir 40 mbps bc 200 ms
conformed 0 bytes, 0 bps action: transmit
violated 0 bytes, 0 bps action: drop
Class-map (qos): map5 (match-all)
0 packets, 0 bytes
5 minute offered rate 0 bps, drop rate 0 bps
Match: access-group foo
police cir 50 mbps bc 200 ms
```

```
conformed 0 bytes, 0 bps action: transmit
violated 0 bytes, 0 bps action: drop
Class-map (qos): class-default (match-any)
0 packets, 0 bytes
5 minute offered rate 0 bps, drop rate 0 bps
police cir 60 mbps bc 200 ms
conformed 0 bytes, 0 bps action: transmit
violated 0 bytes, 0 bps action: drop
```

The following example shows how to display the QoS statistics in the specified port channel:

```
switch(config)# show policy-map interface port-channel 6

Global statistics status: enabled

port-channel6

  Service-policy (queuing) input: default-8e-4q8q-in-policy
    SNMP Policy Index:  301993627

    Class-map (queuing): 8e-4q8q-in-q1 (match-any)
      queue-limit percent 10
      bandwidth percent 49
      queue dropped pkts: 0
      queue dropped bytes: 0
      queue transmit pkts: 2175032764  queue transmit bytes: 1051188564890

    Class-map (queuing): 8e-4q8q-in-q-default (match-any)
     queue-limit percent 88
      bandwidth percent 49
      queue dropped pkts: 0
      queue dropped bytes: 0  current depth bytes: 99
      queue transmit pkts: 518903560636  queue transmit bytes: 457520859584290
```

In this example, the **current depth bytes** field appears because of an active congestion.

The **current depth bytes** field appears for any physical interface when there is an active congestion and the software reads the counter. The value of the counter must be non zero. The current depth indicates that there are packets waiting in the buffer to be forwarded. The value of the current depth is in bytes.

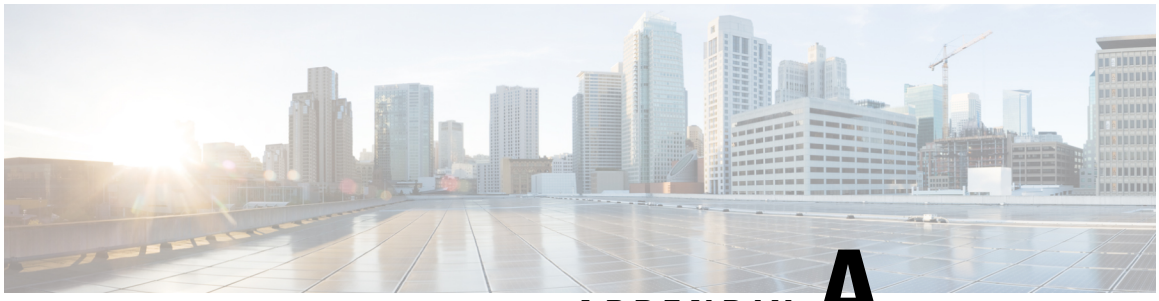
For complete information on the show policy-map command, see the *Cisco Nexus 7000 Series NX-OS Quality of Service Command Reference*.

Feature History for Statistics

The table below summarizes the new and changed features for this document and shows the releases in which each feature is supported. Your software release might not support all the features in this document. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release.

Table 45: Feature History for Statistics

Feature Name	Release	Feature Information
No changes from Release 4.1(2)	5.1(1)	—



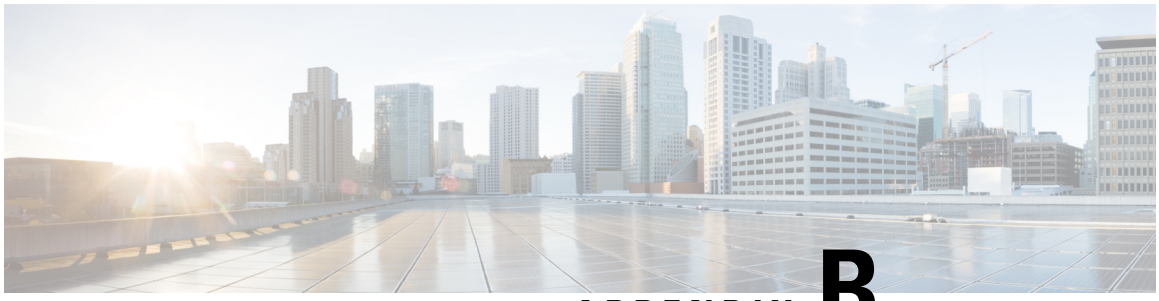
APPENDIX A

Configuration Limits for Quality of Service Configuration Features

Configuration Limits for QoS

The configuration limits are documented in the *Cisco Nexus 7000 Series NX-OS Verified Scalability Guide*.

Configuration Limits for Quality of Service Configuration Features



APPENDIX B

Additional References Appendix

This appendix contains additional information related to implementing QoS on the Cisco NX-OS device. This appendix includes the following sections:

Related Documents

Related Topic	Document Title
VDCs	Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide
CLI commands	Cisco Nexus 7000 Series NX-OS Quality of Service Command Reference
Release Notes	Cisco Nexus 7000 Series NX-OS Release Notes

RFCs

RFCs	Title
RFC 2597	Assured Forwarding PHB Group
RFC 2697	A Single Rate Three Color Marker
RFC 2698	A Two Rate Three Color Marker
RFC 3289	Management Information Base for the Differentiated Services Architecture
RFC 3550	RTP: A Transport Protocol for Real-time Applications