Cisco Nexus 3600 NX-OS Quality of Service Configuration Guide, Release 10.2(x)

First Published: 2021-08-23

Last Modified: 2023-09-01

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

CONTENTS

Preface

This preface includes the following sections:

Audience

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

Document Conventions

Command descriptions use the following conventions:

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

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

Examples use the following conventions:

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

Related Documentation for Cisco Nexus 3600 Platform Switches

The entire Cisco Nexus 3600 platform switch documentation set is available at the following URL:

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

Documentation Feedback

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

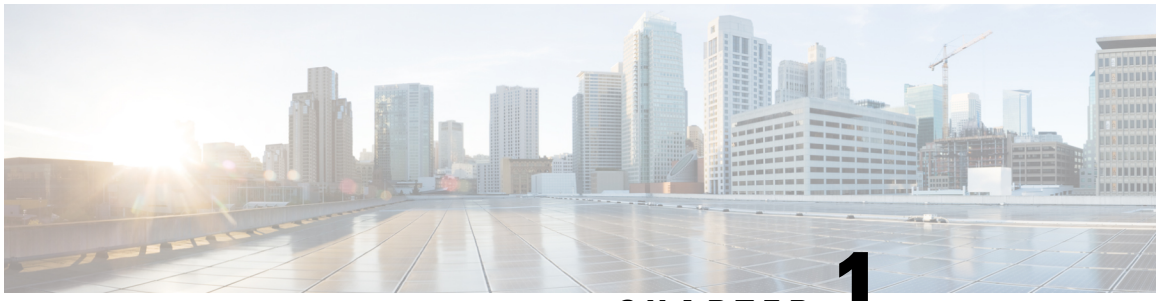
Communications, Services, and Additional Information

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

Cisco Bug Search Tool

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

Preface



CHAPTER 1

New and Changed Information

This chapter provides release-specific information for each new and changed feature in the *Cisco Nexus 3600 NX-OS QoS Configuration Guide*.

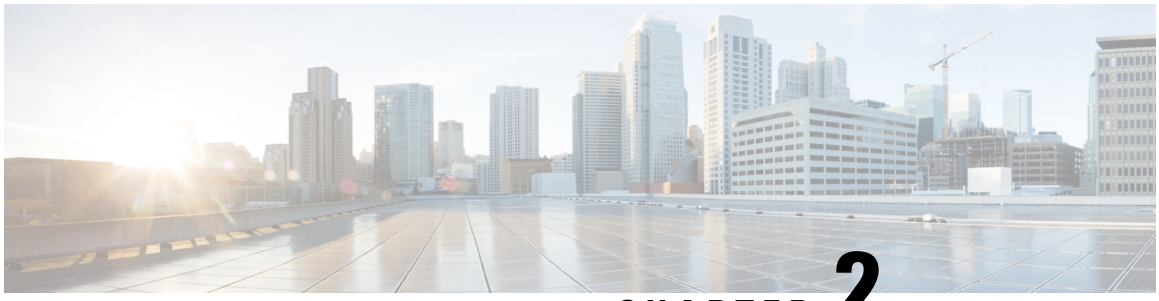
New and Changed Information

The following table provides an overview of the significant changes made to this configuration guide. The table does not provide an exhaustive list of all changes made to this guide or all new features in a particular release.

Table 1: New and Changed Features

Feature	Description	Changed in Release	Where Documented
No feature updates for this release		10.2(1)F	

New and Changed Information



CHAPTER 2

Overview

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* and the *Cisco NX-OS Licensing Options Guide*.

Supported Platforms

Starting with Cisco NX-OS release 7.0(3)I7(1), use the Nexus Switch Platform Support Matrix to know from which Cisco NX-OS releases various Cisco Nexus 9000 and 3000 switches support a selected feature.

About QoS Features

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

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

- QoS policies include classification and marking features.
- QoS policies include policing features.
- Queuing policies use the queuing and scheduling features.

Note The system-defined QoS features and values that are discussed in the "Using Modular QoS CLI" section apply globally to the entire device and can be modified.

Using QoS

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

To configure QoS features, you use the following steps:

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

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

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

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

Classification

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

The values used to classify traffic are called match criteria. When you define a traffic class, you can specify multiple match criteria, you can choose to not match on a particular criterion, or you can determine the traffic class by matching any or all criteria.

Traffic that fails to match any class is assigned to a default class of traffic called class-default.

Marking

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

Policing

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

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

Queuing and Scheduling

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

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

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

Sequencing of QoS Actions

The following are the three types of policies:

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

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

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

Sequencing of Ingress Traffic Actions

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

1. Classification
2. Marking

3. Policing

Sequencing of Egress Traffic Actions

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

1. Queuing and scheduling

High Availability Requirements for QoS Features

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

Note For complete information on high availability, see the *Cisco Nexus 3600 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 following table:

Table 2: MQC Configuration Commands

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

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

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

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

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

QoS Statistics

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

Default QoS Behavior

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

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

Note There is also a default QoS policy that can be applied at the system level. It is inherited by all ports up to the point where the user applies a per-port policy.

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

Virtual Device Contexts

Cisco NX-OS can segment operating system and hardware resources into virtual device contexts (VDCs) that emulate virtual devices. The Cisco Nexus 3600 device currently does not support multiple VDCs. All device resources are managed in the default VDC.

Notes for Enabling VLAN QoS

The VLAN QoS feature enables Layer 2 bridged database lookup for QoS with VLAN as the key instead of the port.

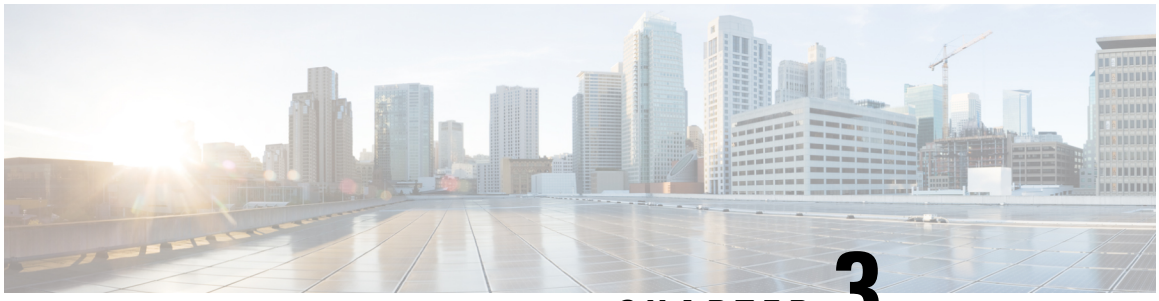
To enable VLAN QoS, you must decrease the TCAM size of another region and increase the TCAM size for the VLAN QoS region.

To configure the size of the VLAN QoS TCAM region:

- Configure the IPv4 vqos to 640 entries.
- Configure the IPv6 ipv6-vqos to 256 entries.
- Decrease the IPv4 qos to 0 entries.
- Decrease the IPv6 ipv6-qos to 0 entries.

```
switch(config)# hardware access-list tcam region vqos 640
switch(config)# hardware access-list tcam region ipv6-vqos 256
switch(config)# hardware access-list tcam region qos 0
switch(config)# hardware access-list tcam region ipv6-qos 0
```

Note After configuring the TCAM size for VLAN QOS, it is necessary to reload the line card.



CHAPTER 3

Configuring Queuing and Scheduling

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 taildrop thresholds. The device drops packets only when the configured thresholds are exceeded.

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

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

Modifying Class Maps

System-defined queuing class maps are provided.

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

Congestion Management

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

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

Traffic Shaping

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

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

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

Prerequisites for Queuing and Scheduling

Queuing and scheduling have the following prerequisites:

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

Guidelines and Limitations for Configuring Queuing and Scheduling

Queuing and scheduling have the following configuration guidelines and limitations:

- Nexus 3600 Switches support only the eight (8) queue configuration in QoS policies. Fewer queues can be configured but are not supported.

- **show** commands with the **internal** keyword are not supported.
- The device supports a system-level queuing policy, so all ports in the system are impacted when you configure the queuing policy.
- A type queuing policy can be attached to the system or to individual interfaces for input or output traffic.
- Changes are disruptive. The traffic passing through ports of the specified port type experience a brief period of traffic loss. All ports of the specified type are affected.
- Performance can be impacted. If one or more ports of the specified type do not have a queuing policy applied that defines the behavior for the new queue, the traffic mapping to that queue might experience performance degradation.
- Traffic shaping might increase the latency of packets due to queuing because it falls back to store-and-forward mode when packets are queued.
- When configuring priorities for one class map queue, you need to configure the priority level for that queue. When configuring priorities for more than one class map queue, you need to configure the priorities for each of the queues.
- The **queue-limit** configuration is applicable only in ingress queuing policy on Cisco Nexus 9500 switches with 9600-R/RX line cards.
- The **bandwidth percent** configuration is applicable only in egress queuing policy on Cisco Nexus 9500 switches with 9600-R/RX line cards.
- If granted buffer is not carved out using a custom input queuing policy for a specified group, only global shared buffers are used.

Order of Resolution

The queue-limit for a priority-group is resolved in the following order:

- Interface ingress queuing policy (if applied and queue-limit configuration specified for that class).
- System ingress queuing policy (if applied and queue-limit configuration specified for that class).

Configuring Queuing and Scheduling

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

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

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

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

Configuring Type Queuing Policies

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

SUMMARY STEPS

1. **configure terminal**
2. **policy-map type queuing** *policy-name*
3. **class type queuing** *class-name*
4. **priority**
5. **no priority**
6. **shape** {**kbps** | **mbps** | **gbps**} *burst size* **min** *minimum bandwidth*
7. **bandwidth percent** *percentage*
8. **no bandwidth percent** *percentage*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**policy-map type queuing** *policy-name*	Creates a named object that represents a set of policies that are to be applied to a set of traffic classes. Policy-map names can contain alphabetic, hyphen, or underscore characters, are case sensitive, and can be up to 40 characters.
Step 3	**class type queuing** *class-name*	Associates a class map with the policy map, and enters configuration mode for the specified system class.
Step 4	**priority**	Specifies that traffic in this class is mapped to a strict priority queue.
Step 5	**no priority**	(Optional) Removes the strict priority queuing from the traffic in this class.
Step 6	**shape** {**kbps** | **mbps** | **gbps**} *burst size* **min** *minimum bandwidth*	Specifies the burst size and minimum guaranteed bandwidth for this queue.
Step 7	**bandwidth percent** *percentage*	Assigns a weight to the class. The class will receive the assigned percentage of interface bandwidth if there are no strict-priority queues. If there are strict-priority queues, however, the strict-priority queues receive their share of the bandwidth first. The remaining bandwidth is shared in a weighted manner among the class configured with a bandwidth percent. For example, if strict-priority queues take 90 percent of the bandwidth, and you configure 75 percent for a class, the class will receive 75 percent of the remaining 10 percent of the bandwidth.

	Command or Action	Purpose
		Note Before you can successfully allocate bandwidth to the class, you must first reduce the default bandwidth configuration on class-default and class-fcoe.
Step 8	**no bandwidth percent** *percentage*	(Optional) Removes the bandwidth specification from this class.

Configuring Queue Limit Using Ingress Queuing Policy

There are situations where each port needs dedicated buffers. An ingress queuing policy can be used for this purpose.

SUMMARY STEPS

1. **configure terminal**
2. **policy-map type queuing** *policy-map-name*
3. **class type queuing** *c-in-q1*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**policy-map type queuing** *policy-map-name*	Enters policy-map queuing class mode and identifies the policy map assigned to the type queuing policy map.
Step 3	**class type queuing** *c-in-q1*	Attaches the class map of type queuing and then enters policy-map class queuing mode. Class queuing names are listed in the System-Defined Type queuing Class Maps table. **Note** The qos-group associated with the class must be defined as a no-drop class in the network-qos policy applied in the system qos. **Note** Up to eight ingress queues are supported for the X9636C-R and X9636Q-R line cards and the C9508-FM-R fabric module (in a Cisco Nexus 9508 switch). The range is from c-in-8q-q-default to c-in-8q-q1 through 7.

Configuring Congestion Management

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

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

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

- Taildrop thresholds based on the queue size and the queue limit usage.

Configuring Tail Drop

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

SUMMARY STEPS

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

DETAILED STEPS

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

	Command or Action	Purpose
Step 3	**class type queuing** *class-name* **Example:** `switch(config-pmap-que)# class type queuing c-out-8q-q7` `switch(config-pmap-c-que)#`	Configures the class map of type queuing and then enters policy-map class queuing mode. Class queuing names are listed in the previous System-Defined Type queuing Class Maps table.
Step 4	**queue-limit** {*queue-size* [**bytes** | **kbytes** | **mbytes**] | **dynamic** *value*} **Example:** `switch(config-pmap-c-que)# queue-limit 1000 mbytes`	Assigns a tail drop threshold based on the queue size in bytes, kilobytes, or megabytes or allows the queue's threshold size to be determined dynamically depending on the number of free cells available. The device drops packets that exceed the specified threshold. The valid values for byte-based queue size are from 1 to 83886080. The valid values for dynamic queue size are from 0 to 10.
Step 5	(Optional) Repeat Steps 2 and 3 to assign tail drop thresholds for other queue classes.	
Step 6	**show policy-map** [**type queuing** [*policy-map-name* | **default-out-policy**]] **Example:** `switch(config-pmap-c-que)# show policy-map type queuing egr-queuing-policy-1`	(Optional) Displays information about all configured policy maps, all policy maps of type queuing, a selected policy map of type queuing, or the default output queuing policy.
Step 7	**copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	(Optional) Saves the running configuration to the startup configuration.

Configuring Bandwidth and Bandwidth Remaining

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

SUMMARY STEPS

1. **configure terminal**
2. **policy-map type queuing** {[**match-first**] *policy-map-name*}
3. **class type queuing***class-name*
4. Assign a minimum rate of the interface bandwidth or assign the percentage of the bandwidth that remains:
   - Bandwidth percent:

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

     bandwidth remaining percent *percent*
5. (Optional) Repeat Steps 3 and 4 to assign tail drop thresholds for other queue classes.

6. exit
7. **show policy-map** [**type queuing** [*policy-map-name* | **default-out-policy**]]
8. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `switch# configure terminal` `switch(config)#`	Enters global configuration mode.
Step 2	**policy-map type queuing** {[**match-first**] *policy-map-name*} **Example:** `switch(config)# policy-map type queuing shape_queues` `switch(config-pmap-que)#`	Configures the policy map of type queuing and then enters policy-map mode for the policy-map name you specify. Policy-map names can contain alphabetic, hyphen, or underscore characters, are case sensitive, and can be up to 40 characters.
Step 3	**class type queuing***class-name* **Example:** `switch(config-pmap-que)# class type queuing c-out-8q-q1` `switch(config-pmap-c-que)#`	Configures the class map of type queuing and then enters policy-map class queuing mode. Class queuing names are listed in the previous System-Defined Type queuing Class Maps table.
Step 4	Assign a minimum rate of the interface bandwidth or assign the percentage of the bandwidth that remains: • Bandwidth percent: **bandwidth** {**percent** *percent*} • Bandwidth remaining percent: **bandwidth remaining percent** *percent* **Example:** • Bandwidth percent: `switch(config-pmap-c-que)# bandwidth percent 25` • Bandwidth remaining percent: `switch(config-pmap-c-que)# bandwidth remaining percent 25`	• Bandwidth percent: Assigns a minimum rate of the interface bandwidth to an output queue as the percentage of the underlying interface link rate. The range is from 0 to 100. The example shows how to set the bandwidth to a minimum of 25 percent of the underlying link rate. • Bandwidth remaining percent: Assigns the percentage of the bandwidth that remains to this queue. The range is from 0 to 100. The example shows how to set the bandwidth for this queue to 25 percent of the remaining bandwidth.
Step 5	(Optional) Repeat Steps 3 and 4 to assign tail drop thresholds for other queue classes.	
Step 6	exit **Example:** `switch(config-cmap-que)# exit` `switch(config)#`	Exits policy-map queue mode and enters global configuration mode.

	Command or Action	Purpose
Step 7	**show policy-map** [**type queuing** [*policy-map-name* | **default-out-policy**]] **Example:** `switch(config-pmap-c-que)# show policy-map type queuing shape_queues`	(Optional) Displays information about all configured policy maps, all policy maps of type queuing, a selected policy map of type queuing, or the default output queuing policy.
Step 8	**copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	(Optional) Saves the running configuration to the startup configuration.

Configuring Priority

If you do not specify the priority, the system-defined egress pq queues behave as normal queues.

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

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

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

SUMMARY STEPS

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

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**policy-map type queuing** {[**match-first**] *policy-map-name*} **Example:** `switch(config)# policy-map type queuing priority_queue1` `switch(config-pmap-que)#`	Configures the policy map of type queuing and then enters policy-map mode for the policy-map name you specify. Policy-map names can contain alphabetic, hyphen, or underscore characters, are case sensitive, and can be up to 40 characters.
Step 3	**class type queuing** *class-name* **Example:** `switch(config-pmap-que)# class type queuing c-out-8q-q1` `switch(config-pmap-c-que)#`	Configures the class map of type queuing and then enters policy-map class queuing mode. Class queuing names are listed in the previous System-Defined Type queuing Class Maps table.
Step 4	**priority** [**level** *value*] **Example:** `switch(config-pmap-c-que)# priority`	Selects this queue as a priority queue. Only one priority level is supported.
Step 5	**class type queuing***class-name* **Example:** `switch(config-pmap-que)# class type queuing c-out-q2` `switch(config-pmap-c-que)#`	(Optional) Configures the class map of type queuing and then enters policy-map class queuing mode. Class queuing names are listed in the previous System-Defined Type queuing Class Maps table. Choose a nonpriority queue where you want to configure the remaining bandwidth. By default, the system evenly distributes the remaining bandwidth among the nonpriority queues.
Step 6	**bandwidth remaining percent** *percent* **Example:** `switch(config-pmap-c-que)# bandwidth remaining percent 25`	(Optional) Assigns the percent of the bandwidth that remains to this queue. The range is from 0 to 100.
Step 7	(Optional) Repeat Steps 5 to 6 to assign the remaining bandwidth for the other nonpriority queues.	
Step 8	exit **Example:** `switch(config-cmap-que)# exit` `switch(config)#`	Exits policy-map queue mode and enters global configuration mode.
Step 9	**show policy-map** [**type queuing** [*policy-map-name* | **default-out-policy**]] **Example:** `switch(config)# show policy-map type queuing priority_queue1`	(Optional) Displays information about all configured policy maps, all policy maps of type queuing, a selected policy map of type queuing, or the default output queuing policy.
Step 10	**copy running-config startup-config** **Example:**	(Optional) Saves the running configuration to the startup configuration.

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

Configuring Traffic Shaping

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

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

Before you begin

Configure random detection minimum and maximum thresholds for packets.

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `switch# configure terminal` `switch(config)#`	Enters global configuration mode.
Step 2	**policy-map type queuing** {[**match-first**] *policy-map-name*} **Example:** `switch(config)# policy-map type queuing shape_queues` `switch(config-pmap-que)#`	Configures the policy map of type queuing and then enters policy-map mode for the policy-map name you specify. Policy-map names can contain alphabetic, hyphen, or underscore characters, are case sensitive, and can be up to 40 characters.
Step 3	**class type queuing** *class-name* **Example:** `switch(config)# class type queuing c-out-q-default` `switch(config-pmap-c-que)#`	Configures the class map of type queuing and then enters policy-map class queuing mode. Class queuing names are listed in the previous System-Defined Type queuing Class Maps table.
Step 4	**shape min** *value* {**bps**	**gbps**	**kbps**	**mbps**	**pps**} **max** *value* {**bps**	**gbps**	**kbps**	**mbps**	**pps**}	Assigns a minimum and maximum bit rate on an output queue. The default bit rate is in bits per second (bps).

	Command or Action	Purpose
	Example: `switch(config-pmap-c-que)# shape min 10 bps max 100 bps`	The example shows how to shape traffic to a minimum rate of 10 bits per second (bps) and a maximum rate of 100 bps.
Step 5	(Optional) Repeat Steps 3 and 4 to assign tail drop thresholds for other queue classes.	
Step 6	**show policy-map** [**type queuing** [*policy-map-name* | **default-out-policy**]] **Example:** `switch(config)# show policy-map type queuing shape_queues`	(Optional) Displays information about all configured policy maps, all policy maps of type queuing, a selected policy map of type queuing, or the default output queuing policy.
Step 7	**copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	(Optional) Saves the running configuration to the startup configuration.

Applying a Queuing Policy on a System

You apply a queuing policy globally on a system.

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `switch# configure terminal` `switch(config)#`	Enters global configuration mode.
Step 2	**system qos** **Example:** `switch (config)# system qos` `switch (config-sys-qos)#`	Enters system qos mode.
Step 3	**service-policy type queuing output** {*policy-map-name* | **default-out-policy**} **Example:** `switch (config-sys-qos)# service-policy type queuing map1`	Adds the policy map to the input or output packets of system. **Note** The **output** keyword specifies that this policy map should be applied to traffic transmitted from an interface.

	Command or Action	Purpose	
		Note	To restore the system to the default queuing service policy, use the **no** form of this command.

Verifying the Queuing and Scheduling Configuration

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

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

Configuration Examples for Queuing and Scheduling

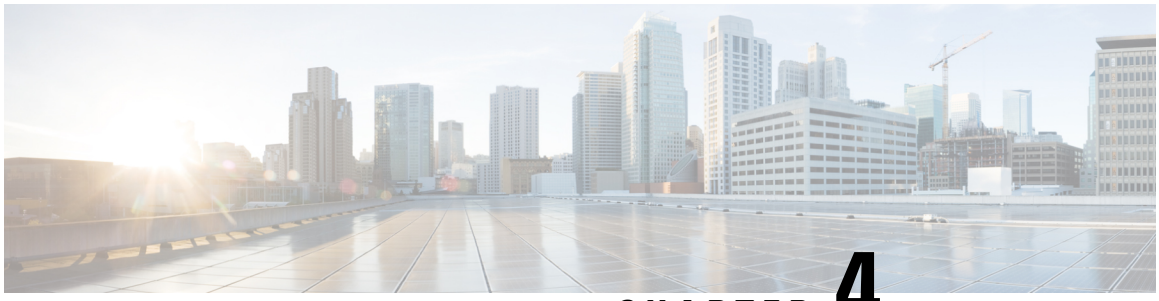
In this section you can find examples of configuring queuing and scheduling.

Example: Configuring Traffic Shaping

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

```
configure terminal
  class-map type queuing match-any c-out-8q-q1
    match qos-group 1
  class-map type queuing match-any c-out-8q-q2
    match qos-group 1
policy-map type queuing pqu
  class type queuing c-out-8q-q3
    bandwidth percent 20
    shape min 100 mbps max 500 mbps
  class type queuing c-out-8q-q2
    bandwidth percent 30
    shape min 200 mbps max 1000 mbps
  class type queuing c-out-8q-q-default
    bandwidth percent 50
  class type queuing c-out-8q-q1
    bandwidth percent 0
  class type queuing c-out-8q-q4
    bandwidth percent 0
  class type queuing c-out-8q-q5
    bandwidth percent 0
```

```
  class type queuing c-out-8q-q6
    bandwidth percent 0
  class type queuing c-out-8q-q7
    bandwidth percent 0
system qos
  service-policy type queuing output pqu
```



CHAPTER 4

Configuring Classification

About Classification

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

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

Table 4: Classification Criteria

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

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

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

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

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

Prerequisites for Classification

Classification has the following prerequisites:

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

Guidelines and Limitations

Classification has the following configuration guidelines and limitations:

- **show** commands with the **internal** keyword are not supported.
- You can specify a maximum of 1024 match criteria in a class map.
- You can configure a maximum of 128 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 the port policy of the incoming packet but not both. If both are present, the device acts on the port policy.
- A QoS policy with a MAC-based ACL as a match in the class map does not work for IPv6 traffic. For QoS, IPv6 traffic needs to be matched based on IPv6 addresses and not on MAC addresses.
- A QoS policy that references an ACL that contains a match for ICMP type or code is not supported.
- A QoS Policy that references an ACL that contains a match for TCP flags is not supported.

Configuring Traffic Classes

Configuring ACL Classification

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, IPv6, or MAC address.

Step 1 Enter global configuration mode.

switch# **configure terminal**

Step 2 Create or access the class map named class-name and enters class-map mode. The class map name can contain alphabetic, hyphen, or underscore characters, and can be up to 40 characters. (**match-any** is the default when no option is selected and multiple match statements are entered.)

switch(config)# **class-map** [**type qos**] [**match-any** | **match-all**] *class-name*

Step 3 Configure the traffic class by matching packets based on the *acl-name*. The **permit** and **deny** ACL keywords are ignored in the matching.

switch(config-cmap-qos)# **match access-group name** *acl-name*

Example: Configuring ACL Classification

The following is a running configuration example. Replace the placeholders with relevant values for your setup.

```
configure terminal
     class-map class_acl
     match access-group name my_acl
```

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

```
show class-map class_acl
```

Configuring DSCP Classification

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

Table 5: Standard DSCP Values

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

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

Step 1 Enter global configuration mode.

switch# **configure terminal**

Step 2 Create or access the class map named class-name and enters class-map mode. The class-map name can contain alphabetic, hyphen, or underscore characters, and can be up to 40 characters.

switch(config)# **class-map** [**type qos**] [**match-any** | **match-all**] *class-name*

Step 3 Configure the traffic class by matching packets based on dscp-values. The standard DSCP values are shown in the following table.

switch(config-cmap-qos)# **match** [**not**] **dscp** *dscp-values*

Step 4 Exit global class-map queuing mode and enters global configuration mode.

switch(config-cmap-qos)# **exit**

Step 5 (Optional) Save the running configuration to the startup configuration.

switch(config)# **copy running-config startup-config**

Example

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

```
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.

Note The DSCP value is trust on the Layer 3 port of a Cisco NX-OS device.

The precedence values are listed in the following:

Table 6: 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)

Step 1 Enter global configuration mode.

configure terminal

Step 2 Create or accesses the class map named class-name and then enters class-map mode. The class-map name can contain alphabetic, hyphen, or underscore characters, and can be up to 40 characters.

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

Step 3 Configure the traffic class by matching packets based on *precedence-values*. Values are shown in the following table. Use the **not** keyword to match on values that do not match the specified range.

match [**not**] **precedence** *precedence-values*

Step 4 Exit global class-map queuing mode and enters global configuration mode.

exit

Step 5 (Optional) Save the running configuration to the startup configuration.

copy running-config startup-config

Example: Configuring IP Precedence Classification

The following is a running configuration example. Replace the placeholders with relevant values for your setup.

```
configure terminal
     class-map class_ip_precedence
     match precedence 1-2, 5-7
     exit
```

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

```
show class-map class_ip_precedence
```

Configuring Protocol Classification

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

Table 7: match Command Protocol Arguments

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

Step 1 Enter global configuration mode.

switch# **configure terminal**

Step 2 Create or access the class map named class-name and then enters class-map mode. The class-map name can contain alphabetic, hyphen, or underscore characters, and can be up to 40 characters.

switch(config)# **class-map** [**type qos**] [**match-any** | **match-all**] *class-name*

Step 3 Configure the traffic class by matching packets based on the specified protocol.

switch(config-cmap-qos)# **match protocol** {**arp** | **bridging** | **cdp** | **dhcp** | **isis**}

Step 4 Exit global class-map queuing mode and enters global configuration mode.

switch(config-cmap-qos)# **exit**

Step 5 (Optional) Save the running configuration to the startup configuration.

switch(config)# **copy running-config startup-config**

Example: Configuring Protocol Classification

The following is a running configuration example. Replace the placeholders with relevant values for your setup.

```
configure terminal
      class-map class_protocol
      match protocol isis
      exit
```

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

```
show class-map class_protocol
```

Configuring CoS Classification

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

Step 1 Enter global configuration mode.

switch# **configure terminal**

Step 2 Create or access the class map named class-name and then enters class-map mode. The class-map name can contain alphabetic, hyphen, or underscore characters, and can be up to 40 characters.

switch(config)# **class-map** [**type qos**] [**match-any** | **match-all**] *class-name*

Step 3 Configure the traffic class by matching packets based on the list of CoS values. Values can range from 0 to 7. Use the **not** keyword to match on values that do not match the specified range.

switch(config-cmap-qos)# **match** [**not**] **cos** *cos-list*

Step 4 Exit global class-map queuing mode and enters global configuration mode.

switch(config-cmap-qos)# **exit**

Step 5 (Optional) Save the running configuration to the startup configuration.

switch(config)# **copy running-config startup-config**

Example: Configuring CoS Classification

The following is a running configuration example. Replace the placeholders with relevant values for your setup.

```
configure terminal
     class-map class_cos
     match cos 4,5-6
     exit
```

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

```
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.

Step 1 Enter global configuration mode.

switch# **configure terminal**

Step 2 Create or access the class map named class-name and then enters class-map mode. The class-map name can contain alphabetic, hyphen, or underscore characters, and can be up to 40 characters.

switch(config)# **class-map** [**type qos**] [**match-any** | **match-all**] *class-name*

Step 3 Configure 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.

switch(config-cmap-qos)# **match ip rtp** *udp-port-value*

Step 4 Exit global class-map queuing mode and enters global configuration mode.

switch(config-cmap-qos)# **exit**

Step 5 (Optional) Save the running configuration to the startup configuration.

switch(config)# **copy running-config startup-config**

Example: Configuring IP RTP Classification

The following is a running configuration example. Replace the placeholders with relevant values for your setup.

```
configure terminal
     class-map class_rtp
     match ip rtp 2000-2100, 4000-4100
     exit
     copy running-config
     startup-config
```

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

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

Configuring MPLS Experimental Classification

Step 1 Enter global configuration mode.

switch# **configure terminal**

Step 2 Access the class-mpls.

switch(config)# **class-map type qos match-any class-mpls**

Step 3 Configure the traffic class by matching mpls experimental.

switch(config-cmap-qos)# **match mpls experimental topmost** *number*

Example: Configuring MPLS Experimental Classification

```
configure terminal
     class-map type qos match-any class-mpls
     match match mpls experimental topmost 2, 5-7
```

Verifying the Classification Configuration

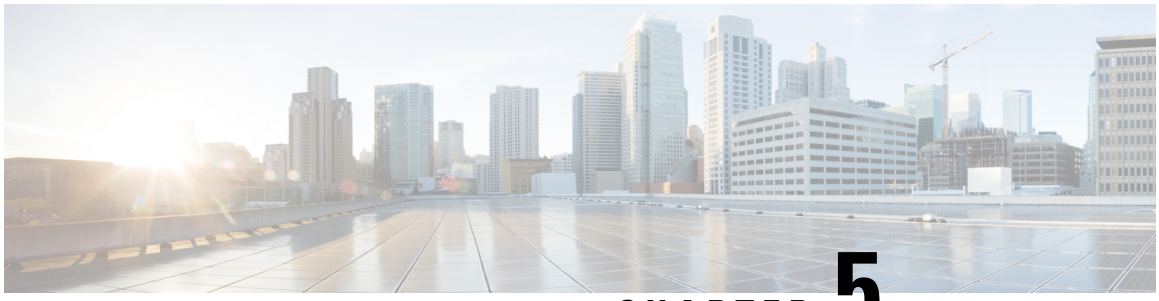
Use the **show class-map** command to verify the class-map configuration. This command displays all class maps.

Configuration Examples for Classification

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

```
class-map class_dscp
match dscp af21, af32
exit
```

```
class-map class_cos
match cos 4, 5-6
exit
```



CHAPTER 5

Configuring Marking

About Marking

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

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

Table 8: Configurable Marking Features

Marking Feature	Description
DSCP	Layer 3 DSCP.
IP precedence	Layer 3 IP precedence. **Note** IP precedence uses only the lower three bits of the type of service (ToS) field. The device overwrites the first three bits of the ToS field to 0.
QoS group	Locally significant QoS values that can be manipulated and matched within the system. The range is from 0 to 7.
Ingress	Status of the marking applies to incoming packets.
CoS	Layer 2 VLAN ID

Prerequisites for Marking

Classification has the following prerequisites:

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

Guidelines and Limitations

Marking has the following configuration guidelines and limitations:

- **show** commands with the **internal** keyword are not supported.
- The **set qos-group** command can only be used in ingress policies.
- Control traffic, such as BPDUs, routing protocol packets, LACP/CDP/BFD, GOLD packets, glean traffic, and management traffic, are automatically classified into a control group based on a criteria. These packets are also given a dedicated buffer pool so that any congestion of data traffic does not affect control traffic. The control qos-group traffic classification cannot be modified.

Configuring Marking

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

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

Configuring DSCP Marking

You can set the DSCP value in the six most significant bits of the DiffServ field of the IP header to a specified value. You can enter numeric values from 0 to 63, in addition to the standard DSCP values shown in the following table.

Table 9: Standard DSCP Values

Value	List of DSCP Values
af11	AF11 dscp (001010)—decimal value 10
af12	AF12 dscp (001100)—decimal value 12
af13	AF13 dscp (001110)—decimal value 14

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

Note For more information about DSCP, see RFC 2475.

Step 1 Enter global configuration mode.

configure terminal

Step 2 Create or access the policy map named *policy-map-name* and then enters policy-map mode. The policy-map name can contain alphabetic, hyphen, or underscore characters, is case sensitive, and can be up to 40 characters.

policy-map [**type qos**] [**match-first**] *policy-map-name*

Step 3 Create a reference to *class-name* and enters policy-map class configuration mode. The class is added to the end of the policy map. Use the **class-default** keyword to select all traffic that is not currently matched by classes in the policy map.

class [**type qos**] {*class-name* | **class-default**}

Step 4 Set the DSCP value to *dscp-value*. Standard values are shown in the previous Standard DSCP Values table.

set dscp *dscp-value*

Example: Configuring DSCP Marking

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

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

The following is a running configuration example. Replace the placeholders with relevant values for your setup.

```
configure terminal
     policy-map policy1
     class class1
     set dscp af31
```

Configuring IP Precedence Marking

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

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

Table 10: 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)

Step 1 Enter global configuration mode.

configure terminal

Step 2 Create or access the policy map named *policy-map-name* and then enters policy-map mode. The policy-map name can contain alphabetic, hyphen, or underscore characters, is case sensitive, and can be up to 40 characters.

policy-map [**type qos**] [**match-first**] *policy-map-name*

Step 3 Create a reference to *class-name* and enters policy-map class configuration mode. The class is added to the end of the policy map.

class [**type qos**] {*class-name* | **class-default**}

Step 4 Set the IP precedence value to *precedence-value*. The value can range from 0 to 7. You can enter one of the values shown in the above Precedence Values table.

set precedence *precedence-value*

Example: Configuring IP Precedence Marking

The following is a running configuration example. Replace the placeholders with relevant values for your setup.

```
configure terminal
     policy-map policy1
     class class1
     set precedence 3
```

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

```
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.

Step 1 Enter global configuration mode.

configure terminal

Step 2 Create or access 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.

policy-map [**type qos**] [**match-first**] [*qos-policy-map-name* | **qos-dynamic**]

Step 3 Create 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.

class [**type qos**] {*class-map-name* | **class-default**} [**insert-before** *before-class-name*]

Step 4 Set the CoS value to *cos-value*. The value can range from 0 to 7.

set cos *cos-value*

Note VLAN QoS supports **set qos-group**. It does not support **set cos**.

Example: Configuring CoS Marking

The following is a running configuration example. Replace the placeholders with relevant values for your setup.

```
configure terminal
     policy-map policy1
     class class1
     set cos 3
```

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

```
show policy-map policy1
```

Configuring Ingress Marking

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

For more information, see 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.

Step 1 Enter global configuration mode.

switch# **configure terminal**

Step 2 Create or accesses the policy map named *policy-map-name* and then enters policy-map mode. The policy-map name can contain alphabetic, hyphen, or underscore characters, is case sensitive, and can be up to 40 characters.

switch(config)# **policy-map** [**type qos**] [**match-first**] [*policy-map-name*]

Step 3 Create a reference to *class-name* and enters policy-map class configuration mode. The class is added to the end of the policy map. Use the **class-default**keyword to select all traffic that is not currently matched by classes in the policy map.

switch(config-pmap-qos)# **class** [**type qos**] {*class-name* | **class-default**}

Step 4 Set the DSCP value to dscp-value. Valid values are listed in the Standard DSCP Values table in the Configuring DSCP Marking section.

switch(config-pmap-c-qos)# **set** *dscp-value*

Step 5 Return to policy-map configuration mode.

switch(config-pmap-c-qos)# **exit**

Step 6 Creates a reference to *class-name* and enters policy-map class configuration mode. The class is added to the end of the policy map. Use the **class-default** keyword to select all traffic that is not currently matched by classes in the policy map.

switch(config-pmap-qos)# **class** [**type qos**] {*class-name* | **class-default**}

Step 7 Sets the DSCP value to dscp-value. Valid values are listed in the Standard DSCP Values table in the Configuring DSCP Marking section.

switch(config-pmap-c-qos)# **set** *dscp-value*

Step 8 Returns to policy-map configuration mode.

switch(config-pmap-c-qos)# **exit**

Step 9 Create a reference to *class-name* and enters policy-map class configuration mode. The class is added to the end of the policy map. Use the **class-default** keyword to select all traffic that is not currently matched by classes in the policy map.

switch(config-pmap-qos)# **class** [**type qos**] {*class-name* | **class-default**}

Step 10 Set the DSCP value to dscp-value. Valid values are listed in the Standard DSCP Values table in the Configuring DSCP Marking section.

switch(config-pmap-c-qos)# **set** *dscp-value*

Step 11 Return to policy-map configuration mode.

switch(config-pmap-c-qos)# **exit**

Step 12 Enter interface mode to configure the Ethernet interface.

switch(config)# **interface ethernet** *slot/port*

Step 13 Add *policy-map-name* to the input packets of the interface. You can attach only one input policy and one output policy to an interface.

switch(config-if)# **service-policy** [**type qos**] {**input** | **output**} {*policy-map-name*} [**no-stats**]

Example: Configuring DSCP Port Marking

The following is a running configuration example. Replace the placeholders with relevant values for your setup.

```
configure terminal
    policy-map policy1
    class class1
    set dscp af31
    exit
```

```
    class class2
    set dscp af1
    exit
    class class-default
    set dscp af22
    exit
    interface ethernet 1/1
    service-policy input policy1
```

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

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

Verifying the Marking Configuration

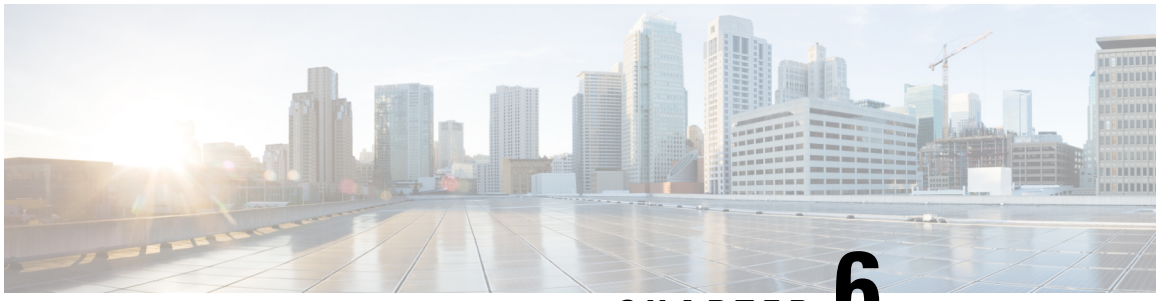
To display the marking configuration information, enter the following command:

show policy-map

Configuration Examples for Marking

The following example shows how to configure marking:

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



CHAPTER 6

Configuring Shared Policers

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.

Guidelines and Limitations

The following are guidelines and limitations for shared policers:

- When the shared policer is applied on interfaces or VLANs with member ports that are across different cores or instances, the rate becomes two times the configured **cir** rate.

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.

To configure shared policer:

1. Create the class map.
2. Create a policy map.
3. Reference the shared policer to the policy map as described in this section.
4. Apply the service policy to the interfaces.

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.

SUMMARY STEPS

1. switch# **configure terminal**
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* [**exceed** {**drop** | **set dscp dscp table** *cir-markdown-map*} [**violate** {**drop** | **set dscp dscp table** *pir-markdown-map*}]]}}
3. switch(config)# **policy-map** [**type qos**] [**match-first**] {*qos-policy-map-name* | **qos-dynamic**}
4. switch(config-pmap-qos)# **class** [**type qos**] {*class-map-name* | **qos-dynamic** | **class-default**} [**insert-before** *before-class-map-name*]
5. switch(config-pmap-c-qos)# **police aggregate shared-policer-name**
6. switch(config-pmap-c-qos)# **exit**
7. switch(config-pmap-qos)# **exit**
8. (Optional) switch(config)# **show policy-map** [**type qos**] [*policy-map-name* | **qos-dynamic**]
9. (Optional) switch(config)# **copy running-config startup-config**

DETAILED STEPS

	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* [**exceed** {**drop** | **set dscp dscp**	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 traffic takes the **violate** action. If **be** or **violate** are specified, the **exceed**

	Command or Action	Purpose
	table *cir-markdown-map*} [**violate** {**drop** | **set dscp dscp table** *pir-markdown-map*}]]}}	action is taken if the data rate ≤ **pir**, and the **violate** action is taken otherwise. **Note** A 64 byte packet size is used for the case of **cir pps**.This results in a 64*8 **pps** to **bps** conversion.
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 policers.

Configuration Example for Shared Policer

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
```