Cisco Nexus 3548 Switch NX-OS Quality of Service Configuration Guide, Release 6.x

First Published: 2013-05-21

Last Modified: 2017-08-30

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

Text Part Number: OL-29551-01

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.

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.

CHAPTER 1

New and Changed Information in this Release

This chapter contains the following sections:

New and Changed Information for this Release

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

Table 1: New and Changed Quality of Service Features

Feature	Description	Added or Changed in Release	Where Documented
Active Latency Monitoring	Support for active latency monitoring.	6.0(2)A7(1)	Active Latency Monitoring Overview, on page 41
Link Level Flow Control	This feature was introduced.	6.0(2)A1(1)	Configuring Link Level Flow Control, on page 47

CHAPTER 2

Overview

This chapter contains the following sections:

Quality of Service Overview

This document describes the configurable Cisco NX-OS Quality of Service (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, 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, as follows:

- QoS policies include classification and marking features.
- Queuing policies use the queuing and scheduling features.
- Network QoS policies include configuring maximum transmission unit (MTU).

CHAPTER 3

Configuring QoS

This chapter contains the following sections:

Information About Quality of Service

The configurable Cisco NX-OS quality of service (QoS) features allow you to classify the network traffic, prioritize the traffic flow, and provide congestion avoidance.

The default QoS configuration on the device provides best-effort service for Ethernet traffic. QoS can be configured to provide additional classes of service for Ethernet traffic. Cisco NX-OS QoS features are configured using Cisco Modular QoS CLI (MQC).

In the event of congestion or collisions, Ethernet will drop packets. The higher level protocols detect the missing data and retransmit the dropped packets.

Modular QoS CLI

The Cisco Modular QoS CLI (MQC) provides a standard set of commands for configuring QoS.

You can use MQC to define additional traffic classes and to configure QoS policies for the whole system and for individual interfaces. Configuring a QoS policy with MQC consists of the following steps:

1. Define traffic classes.
2. Associate policies and actions with each traffic class.
3. Attach policies to logical or physical interfaces as well as at the global system level.

MQC provides two 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.

The class map classifies incoming packets based on matching criteria, such as the IEEE 802.1p class of service (CoS) value. Unicast and multicast packets are classified.

policy-map

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

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

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

network-qos

Defines MQC objects that you can use for system level related actions.

qos

Defines MQC objects that you can use for classification.

queuing

Defines MQC objects that you can use for queuing and scheduling.

Note The qos type is the default for the **class-map** and **policy-map** commands, but not for the **service-policy** which requires that you specify an explicit type.

You can attach policies to interfaces or EtherChannels as well as at the global system level by using the **service-policy** command.

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

An MQC target is an entity (such as an Ethernet interface) that represents a flow of packets. A service policy associates a policy map with an MQC target and specifies whether to apply the policy on incoming or outgoing packets. This mapping enables the configuration of QoS policies such as marking, bandwidth allocation, buffer allocation, and so on.

System Classes

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

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

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

Default System Classes

The device provides the drop system class.

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

This class is created automatically when the system starts up (the class is named **class-default** in the CLI). You cannot delete this class and you cannot change the match criteria associated with the default class.

Information About Policy Types

The device supports a number of policy types. You create class maps in the policy types.

There are three policy types

- Network-qos
- Queuing
- QoS

The following QoS parameters can be specified for each type of class:

- Type network-qos—A network-qos policy is used to instantiate system classes and associate parameters with those classes that are of system-wide scope.
  - Classification—The traffic that matches this class are as follows:
    - QoS Group—A class map of type network-qos identifies a system class and is matched by its associated qos-group.
  - Policy—The actions that are performed on the matching traffic are as follows:

    Note A network-qos policy can only be attached to the system QoS target.

    - MTU—The MTU that needs to be enforced for the traffic that is mapped to a system class.

      Note The Cisco Nexus device supports one MTU for all classes for all ports.

    - Set CoS value—This configuration is used to mark 802.1p values for all traffic mapped to this system class.
    - Congestion Control ECN—Data Center TCP (DCTCP) is an enhancement to the TCP congestion control algorithm for data center networks. It leverages Explicit Congestion Notification (ECN) feature, to mark all the packets when the queue length exceeds a configured

ECN threshold value. The routers and end hosts use this marking as a signal that the network is congested to slow down sending packets. To enable an ECN, use the **congestion-control dctcp ecn** command in the network-qos policy map mode.

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

- Type queuing—A type queuing policy is used to define the scheduling characteristics of the queues associated with system classes.

  The Cisco Nexus device supports type queuing in the egress direction.

  Note Some configuration parameters when applied to an EtherChannel are not reflected on the configuration of the member ports.

  - Classification—The traffic that matches this class are as follows:
    - QoS Group—A class map of type queuing identifies a system class and is matched by its associated QoS group.
  - Policy—The actions that are performed on the matching traffic are as follows:

    Note These policies can be attached to the system qos target or to any interface. The output queuing policy is used to configure output queues on the device associated with system classes.

    - Bandwidth—Sets the guaranteed scheduling deficit weighted round robin (DWRR) percentage for the system class.
    - Priority—Sets a system class for strict-priority scheduling. Only one system class can be configured for priority in a given queuing policy.

- Type qos—A type QoS policy is used to classify traffic that is based on various Layer 2, Layer 3, and Layer 4 fields in the frame and to map it to system classes.

  Note Some configuration parameters when applied to an EtherChannel are not reflected on the configuration of the member ports.

  - Classification—The traffic that matches this class are as follows:
    - Access Control Lists—Classifies traffic based on the criteria in existing ACLs.
    - Class of Service—Matches traffic based on the CoS field in the frame header.

- DSCP—Classifies traffic based on the Differentiated Services Code Point (DSCP) value in the DiffServ field of the IP header.
- IP Real Time Protocol—Classifies traffic on the port numbers used by real-time applications.
- Precedence—Classifies traffic based on the precedence value in the type of service (ToS) field of the IP header.

- Policy—The actions that are performed on the matching traffic are as follows:

Note This policy can be attached to the system or to any interface. It applies to input traffic only.

- QoS Group—Sets the QoS group that corresponds to the system class this traffic flow is mapped to.
  - Cisco Nexus device supports the following:
    - Five QoS groups
    - Five queues for unicast
    - Five queues for multicast

Network QoS Policy Type

A network-qos policy is used to instantiate system classes and associate parameters with those classes that are of system-wide scope.

- Classification—The traffic that matches this class are as follows:
  - QoS Group—A class map of type network-qos identifies a system class and is matched by its associated qos-group.
- Policy—The actions that are performed on the matching traffic are as follows:

Note A network-qos policy can only be attached to the system QoS target.

  - MTU—The MTU that needs to be enforced for the traffic that is mapped to a system class.

Note The Cisco Nexus device supports one MTU for all classes for all ports.

  - Set CoS value—This configuration is used to mark 802.1p values for all traffic mapped to this system class.

- Congestion Control DCTCP and ECN—Data Center TCP (DCTCP) is an enhancement to the TCP congestion control algorithm for data center networks. It leverages Explicit Congestion Notification (ECN) feature, to mark all the packets when the queue length exceeds a configured DCTCP threshold value. The routers and end hosts use this marking as a signal that the network is congested to slow down sending packets. To enable an DCTCP/ECN, use the "congestion-control dctcp ecn" command in the network-qos policy map mode.

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

The following example shows how to enable DCTCP and ECN and verify the configuration on the network QoS policy maps:

```
switch# configuration terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# policy-map type network-qos system_network_policy
switch(config-pmap-nq)# class type network-qos nc1
switch(config-pmap-nq-c)# set cos 2
switch(config-pmap-nq-c)# class type network-qos nc2
switch(config-pmap-nq-c)# congestion-control dctcp ecn-threshold 30000 bytes
switch(config-pmap-nq-c)#
switch(config-pmap-nq-c)# system qos
switch(config-sys-qos)# service-policy type network-qos system_network_policy
switch(config-sys-qos)# end
switch#
switch# show policy-map system


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

policy-map type network-qos system_network_policy
class type network-qos nc1
match qos-group 1

mtu 1500
set cos 2
class type network-qos nc2
match qos-group 2

mtu 1500
congestion-control dctcp ecn-threshold 30000 bytes
class type network-qos class-default
match qos-group 0

mtu 1500
```

Queuing Policy Type

A queuing policy type is used to define the scheduling characteristics of the queues associated with system classes.

The Cisco Nexus device supports type queuing in the egress direction.

Note Some configuration parameters when applied to a Port Channel are not reflected on the configuration of the member ports.

- Classification—The traffic that matches this class are as follows:
  - QoS Group—A class map of type queuing identifies a system class and is matched by its associated QoS group.
- Policy—The actions that are performed on the matching traffic are as follows:

Note These policies can be attached to the system qos target or to any interface. The output queuing policy is used to configure output queues on the device associated with system classes.

  - Bandwidth—Sets the guaranteed scheduling deficit weighted round robin (DWRR) percentage for the system class.
  - Priority—Sets a system class for strict-priority scheduling. Only one system class can be configured for priority in a given queuing policy.

QoS Policy Type

A QoS policy type is used to classify traffic that is based on various Layer 2, Layer 3, and Layer 4 fields in the frame and to map it to system classes.

Note Some configuration parameters when applied to a Port Channel are not reflected on the configuration of the member ports.

- Classification—The traffic that matches this class are as follows:
  - Access Control Lists—Classifies traffic based on the criteria in existing ACLs.
  - Class of Service—Matches traffic based on the CoS field in the frame header.
  - DSCP—Classifies traffic based on the Differentiated Services Code Point (DSCP) value in the DiffServ field of the IP header.
  - IP Real Time Protocol—Classifies traffic on the port numbers used by real-time applications.
  - Precedence—Classifies traffic based on the precedence value in the type of service (ToS) field of the IP header.
- Policy—The actions that are performed on the matching traffic are as follows:

Note This policy can be attached to the system or to any interface. It applies to input traffic only.

  - QoS Group—Sets the QoS group that corresponds to the system class this traffic flow is mapped to.

- Cisco Nexus device supports the following:
  - Five QoS groups
  - Five queues for unicast
  - Five queues for multicast

MTU

The Cisco Nexus device supports one MTU for all classes for all ports.

When configuring MTU, follow these guidelines:

- For the Cisco Nexus device, the MTU is controlled by the value configured on the class default.
- Enter the **system jumbomtu** command to define the upper bound of any MTU in the system. The system jumbo MTU has a default value of 9216 bytes. The minimum MTU is 1500 bytes and the maximum MTU is 9216 bytes.
- The system class MTU sets the MTU for all packets in the class. The system class MTU cannot be configured larger than the global jumbo MTU.
- The default system class has a default MTU of 1500 bytes. You can configure this value.
- You can specify the MTU value for either a single Layer 3 interface or a range of Layer 3 interfaces. When you change the Layer 3 interface MTU value to the jumbo MTU value (1500 bytes or greater), you must also change the network QoS MTU value to 1500 bytes or greater. The device generates a syslog message to inform you of this requirement.

Trust Boundaries

The trust boundary is enforced by the incoming interface as follows:

- By default, all Ethernet interfaces are trusted interfaces.The 802.1p CoS and DSCP are preserved unless the marking is configured. There is no default CoS to queue and DSCP to queue mapping. You can define and apply a policy to create these mappings. By default, without a user defined policy, all traffic is assigned to the default queue.
- Any packet that is not tagged with an 802.1p CoS value is classified into the default drop system class. If the untagged packet is sent over a trunk, it is tagged with the default untagged CoS value, which is zero.
- You can override the default untagged CoS value for an Ethernet interface or port channel.
- You can override the default untagged CoS value for an Ethernet interface or a port channel interface using the **untagged cos** *cos-value* command.
- You can override the default untagged Cos value for an Ethernet or a Layer 3 interface or a port channel interface using the **untagged cos** *cos-value* command.

After the system applies the untagged CoS value, QoS functions the same as for a packet that entered the system tagged with the CoS value.

Ingress Classification Policies

You use classification to partition traffic into classes. You classify the traffic based on the packet property (CoS field) or the packet header fields that include IP precedence, Differentiated Services Code Point (DSCP), and Layer 2 to Layer 4 parameters. The values used to classify traffic are called match criteria.

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

Egress Queuing Policies

You can associate an egress policy map with an Ethernet interface to guarantee the bandwidth for the specified traffic class or to configure the egress queues.

Each Ethernet interface supports up to five queues, one for each system class. The queues have the following default configuration:

- In addition to these queues, control traffic that is destined for the CPU uses strict priority queues. These queues are not accessible for user configuration.
- Standard Ethernet traffic in the default drop system class is assigned a queue. This queue uses WRR scheduling with 100 percent of the bandwidth.

If you add a system class, a queue is assigned to the class. You must reconfigure the bandwidth allocation on all affected interfaces. Bandwidth is not dedicated automatically to user-defined system classes.

You can configure one strict priority queue. This queue is serviced before all other queues except the control traffic queue (which carries control rather than data traffic).

QoS for Traffic Directed to the CPU

The device automatically applies QoS policies to traffic that is directed to the CPU to ensure that the CPU is not flooded with packets. Control traffic, such as bridge protocol data units (BPDU) frames, is given higher priority to ensure delivery.

QoS Configuration Guidelines and Limitations

To maintain optimal switch performance, follow these guidelines when configuring system classes and policies:

- Switch resources (such as buffers, virtual output queues, and egress queues) are partitioned based on the default and user-defined system classes. Cisco NX-OS automatically adjusts the resource allocation to accommodate the configured system classes.
- When configuring Port Channels, the service policy configured on an Port Channel applies to all member interfaces.
- By default, queues 6 and 7 are reserved for control plane traffic and queue 5 for SPAN traffic. So you can configure four classes along with the default class.
- On Cisco Nexus N3548 Series switches, the bandwidth percentage that is configured under the queuing policy is not honored under the following conditions:

- When there is an egress port that is experiencing congestion due to an input/output rate mismatch.
- When there are multiple traffic classes using different UC/MC queues.
- If all streams are competing for the buffers because the input rate of all streams is more than the output rate.

Some streams experience buffer crunch as the competing streams use up all the system buffers. There is no fair distribution of the shared buffers on Cisco Nexus N3548 Series switches, due to which the streams that can not be buffered are dropped aggressively. This results in the output rates that are less than the configured bandwidth for that stream and the other streams that exceed the configured bandwidth.

To work around this issue, you have to configure the CLI command **hardware profile buffer qos-group** *X* **threshold** *Y* where X is the qos-group number of the traffic that is exceeding the configured bandwidth and Y is the percentage of the shared buffers that can be used by the stream. The threshold value Y should be a small value, for example, 10 or 20. It can be fine tuned based on the burst absorption rate that is required at the same time honoring the bandwidth. The default threshold is 95%.

Configuring System Classes

Configuring Class Maps

You can create or modify a class map with the **class-map** command. The class map is a named object that represents a class of traffic. In the class map, you specify a set of match criteria for classifying the packets. You can then reference class maps in policy maps.

Note The class map type default is type qos and its match criteria default is match-all.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **class-map** [**type** {**network-qos** | **qos** | **queuing**}] *class-map name*	Creates or accesses a named object that represents the specified class of traffic. Class-map names can contain alphabetic, hyphen, or underscore characters, are case sensitive, and can be up to 40 characters. The three class-map configuration modes are as follows: • **network-qos—**Network-wide (global) mode. CLI prompt: switch(config-cmap-nq)# • **qos—**Classification mode; this is the default mode. CLI prompt: switch(config-cmap-qos)# • **queuing—**Queuing mode. CLI prompt: switch(config-cmap-que)#

	Command or Action	Purpose
Step 3	switch(config)# **class-map** [**type qos**] [**match-all** | **match-any**] *class-map name*	(Optional) Specifies that packets must match any or all criteria that is defined for a class map. • **match-all—**Classifies traffic if packets match all criteria that is defined for a specified class map (for example, if both the defined CoS and the ACL criteria match). • **match-any—**Classifies traffic if packets match any criteria that is defined for a specified class map (for example, if either the CoS or the ACL criteria matches). Class-map names can contain alphabetic, hyphen, or underscore characters, are case sensitive, and can be up to 40 characters.
Step 4	switch(config)# **no class-map** [**type** {**network-qos** | **qos** | **queuing**}] *class-name*	(Optional) Deletes the specified class map. **Note** You cannot delete the system-defined class map: class-default. Class-map names can contain alphabetic, hyphen, or underscore characters, are case sensitive, and can be up to 40 characters.

Configuring ACL Classification

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

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **class-map type qos** *class-name*	Creates a named object that represents a class of traffic. Class-map names can contain alphabetic, hyphen, or underscore characters, are case sensitive, and can be up to 40 characters.
Step 3	switch(config-cmap-qos)# **match access-group name** *acl-name*	Configures a traffic class by matching packets based on the *acl-name*. The **permit** and **deny** ACL keywords are ignored in the matching. **Note** You can only define a single ACL in a class map. You cannot add any other match criteria to a class with a **match access-group** defined.

	Command or Action	Purpose
Step 4	switch(config-cmap-qos)# **no match access-group name** *acl-name*	(Optional) Removes the match from the traffic class.

This example shows how to classify traffic by matching packets based on existing ACLs:

```
switch# configure terminal
switch(config)# class-map type qos class_acl
switch(config-cmap-qos)# match access-group name acl-01
```

Use the **show class-map** command to display the ACL class-map configuration:

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

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*.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **class-map type qos** *class-name*	Creates a named object that represents a class of traffic. Class-map names can contain alphabetic, hyphen, or underscore characters, are case sensitive, and can be up to 40 characters.
Step 3	switch(config-cmap-qos)# **match cos** *cos-value*	Specifies the CoS value to match for classifying packets into this class. You can configure a CoS value in the range of 0 to 7.
Step 4	switch(config-cmap-qos)# **no match cos** *cos-value*	(Optional) Removes the match from the traffic class.

This example shows how to classify traffic by matching packets based on a defined CoS value:

```
switch# configure terminal
switch(config)# class-map type qos match-any class_cos
switch(config-cmap-qos)# match cos 4, 5-6
```

Use the **show class-map** command to display the CoS value class-map configuration:

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

Configuring DSCP Classification

You can classify traffic based on the Differentiated Services Code Point (DSCP) value in the DiffServ field of the IP header.

Table 2: Standard DSCP Values

Value	List of DSCP Values
af11	AF11 dscp (001010)—decimal value 10
af12	AF12 dscp (001100)—decimal value 12
af13	AF13 dscp (001110)—decimal value 14
af21	AF21 dscp (010010)—decimal value 18
af22	AF22 dscp (010100)—decimal value 20
af23	AF23 dscp (010110)—decimal value 22
af31	AF31 dscp (011010)—decimal value 26
af32	AF32 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)# **class-map type qos** *class-name*	Creates a named object that represents a class of traffic. Class-map names can contain alphabetic, hyphen, or underscore characters, are case sensitive, and can be up to 40 characters.
Step 3	switch(config-cmap-qos)# **match dscp** *dscp-list*	Configures the traffic class by matching packets based on the values in the *dscp-list* variable. For a list of DSCP values, see the Standard DSCP Values table.
Step 4	switch(config-cmap-qos)# **no match dscp** *dscp-list*	(Optional) Removes the match from the traffic class. For a list of DSCP values, see the Standard DSCP Values table.

This example shows how to classify traffic by matching packets based on the DSCP value in the DiffServ field of the IP header:

```
switch# configure terminal
switch(config)# class-map type qos match-any class_dscp
switch(config-cmap-qos)# match  dscp af21, af32
```

Use the **show class-map** command to display the DSCP class-map configuration:

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

Configuring IP RTP Classification

The IP Real-time Transport Protocol (RTP) is a transport protocol for real-time applications that transmits 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 use an even port and the next higher odd port is used for RTP Control Protocol (RTCP) communications.

You can classify 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** *class-name*	Creates a named object that represents a class of traffic. Class-map names can contain alphabetic, hyphen, or underscore characters, are case sensitive, and can be up to 40 characters.
Step 3	switch(config-cmap-qos)# **match ip rtp** *port-number*	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.
Step 4	switch(config-cmap-qos)# **no match ip rtp** *port-number*	(Optional) Removes the match from the traffic class.

The following example shows how to classify traffic by matching packets based on UDP port ranges that are typically used by RTP applications:

```
switch# configure terminal
switch(config)# class-map type qos match-any class_rtp
switch(config-cmap-qos)# match  ip rtp 2000-2100, 4000-4100
```

Use the **show class-map** command to display the RTP class-map configuration:

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

Configuring Precedence Classification

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

Table 3: 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)

Value	List of Precedence Values
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)# **class-map type qos match-any** *class-name*	Creates a named object that represents a class of traffic. Class-map names can contain alphabetic, hyphen, or underscore characters, are case sensitive, and can be up to 40 characters.
Step 3	switch(config-cmap-qos)#**match precedence** *precedence-values*	Configures the traffic class by matching packets based on precedence values. For a list of precedence values, see the Precedence Values table.
Step 4	switch((config-cmap-qos)# **no match precedence** *precedence-values*	(Optional) Removes the match from the traffic class. For a list of precedence values, see the Precedence Values table.

This example shows how to classify traffic by matching packets based on the precedence value in the ToS byte field of the IP header:

```
switch# configure terminal
switch(config)# class-map type qos match-any class_precedence
switch(config-cmap-qos)# match precedence 1-2, critical
```

Use the **show class-map** command to display the IP precedence value class-map configuration:

```
switch# show class-map class_precedence
```

Creating Policy Maps

The **policy-map** command is used to create a named object that represents a set of policies that are to be applied to a set of traffic classes.

The device provides one default system class: a drop class for best-effort service (class-default). You can define up to four additional system classes for Ethernet traffic.

The following predefined policy maps are used as default service policies:

- network-qos: default-nq-policy
- Input qos: default-in-policy
- Output queuing: default-out-policy

You need to create a policy map to specify the policies for any user-defined class. In the policy map, you can configure the QoS parameters for each class. You can use the same policy map to modify the configuration of the default classes.

The device distributes all the policy-map configuration values to the attached network adapters.

Before You Begin

Before creating the policy map, define a class map for each new system class.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **policy-map** [**type** {**network-qos** | **qos** | **queuing**}] *policy-name*	Creates a named object representing 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. The three policy-map configuration modes are as follows: • network-qos—Network-wide (global) mode. CLI prompt: switch(config-pmap-nq)# • qos—Classification mode; this is the default mode. CLI prompt: switch(config-pmap-qos)# • queuing—Queuing mode. CLI prompt: switch(config-pmap-que)#
Step 3	switch(config)# **no policy-map** [**type** {**network-qos** | **qos** | **queuing**}] *policy-name*	(Optional) Deletes the specified policy map.
Step 4	switch(config-pmap)# **class** [**type** {**network-qos** | **qos** | **queuing**}] *class-name*	Associates a class map with the policy map, and enters configuration mode for the specified system class. The three class-map configuration modes are as follows: • network-qos—Network-wide (global) mode. CLI prompt: switch(config-pmap-c-nq)# • qos—Classification mode; this is the default mode. CLI prompt: switch(config-pmap-c-qos)# • queuing—Queuing mode. CLI prompt: switch(config-pmap-c-que)# **Note** The associated class map must be the same type as the policy-map type.
Step 5	switch(config-pmap)# **no class** [**type** {**network-qos** | **qos** | **queuing**}] *class-name*	(Optional) Deletes the class map association.

Configuring Type QoS Policies

Type qos policies are used for classifying the traffic of a specific system class identified by a unique qos-group value. A type qos policy can be attached to the system or to individual interfaces for ingress traffic only.

You can set a maximum of five QoS groups for ingress traffic.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **policy-map type qos** *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	switch(config-pmap-qos)# [**class** | **class-default**] **type qos** *class-name*	Associates a class map with the policy map, and enters configuration mode for the specified system class. **Note** The associated class map must be the same type as the policy map type.
Step 4	switch(config-pmap-c-qos)# **set qos-group** *qos-group-value*	Configures one or more **qos-group** values to match on for classification of traffic into this class map. The list below identifies the ranges of the *qos-group-value* . There is no default value. **Note** The switch can only support a maximum of five QoS groups within this range.
Step 5	switch(config-pmap-c-qos)# **no set qos-group** *qos-group-value*	(Optional) Removes the **qos-group** values from this class.

This example shows how to define a type qos policy map:

```
switch# configure terminal
switch(config)# policy-map type qos policy-s1
switch(config-pmap-qos)# class type qos class-s1
switch(config-pmap-c-qos)# set qos-group 2
```

Configuring Type Network QoS Policies

Type network qos policies can only be configured on the system qos attachment point. They are applied to the entire switch for a particular class.

Procedure

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

	Command or Action	Purpose
Step 2	switch(config)# **policy-map type network-qos** *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	switch(config-pmap-nq)# **class type network-qos** *class-name*	Associates a class map with the policy map, and enters configuration mode for the specified system class. **Note** The associated class map must be the same type as the policy map type.
Step 4	switch(config-pmap-c-nq)# **mtu** *mtu-value*	Specifies the MTU value in bytes. **Note** The *mtu-value* that you configure must be less than the value set by the **system jumbomtu** command.
Step 5	switch(config-pmap-c-nq)# **no mtu**	(Optional) Resets the MTU value in this class.
Step 6	switch(config-pmap-c-nq)# **set cos** *cos-value*	Specifies a 802.1Q CoS value which is used to mark packets on this interface. The value range is from 0 to 7.
Step 7	switch(config-pmap-c-nq)# **no set cos** *cos-value*	(Optional) Disables the marking operation in this class.

This example shows how to define a type network-qos policy map:

```
switch# configure terminal
switch(config)# policy-map type network-qos policy-que1
switch(config-pmap-nq)# class type network-qos class-que1
switch(config-pmap-c-nq)# mtu 5000
switch(config-pmap-c-nq)# set cos 4
```

Configuring Type Queuing Policies

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

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **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.

	Command or Action	Purpose
Step 3	switch(config-pmap-que)# **class type queuing** *class-name*	Associates a class map with the policy map, and enters configuration mode for the specified system class.
Step 4	switch(config-pmap-c-que)# **priority**	Specifies that traffic in this class is mapped to a strict priority queue. **Note**
Step 5	switch(config-pmap-c-que)# **no priority**	(Optional) Removes the strict priority queuing from the traffic in this class.
Step 6	switch(config-pmap-c-que)# **bandwidth percent** *percentage*	**Note** Before you can successfully allocate bandwidth to the class, you must first reduce the default bandwidth configuration on class-default.
Step 7	switch(config-pmap-c-que)# **no bandwidth percent** *percentage*	(Optional) Removes the bandwidth specification from this class.

```
(config-pmap-c-que)# queue-limit 0 bytes
class type queuing cos-dscp-6
queue-limit 0 bytes
class type queuing cos-dscp-7
```

Information About Marking

Marking is a method that you use to modify the QoS fields of the incoming and outgoing packets.

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

- DSCP
- IP precedence
- CoS

Configuring CoS Marking

The value of the CoS field is recorded 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.

	Command or Action	Purpose
Step 2	switch(config) # **policy-map** [**type network-qos**] *policy-map name*	Creates or accesses the policy map named *policy-map-name* and 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-nq) # **class** [**type network-qos**] {*class-map name* |**class-default**}	Creates a reference to the *class-map-name* and enters policy-map class configuration mode. 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-nq) # **set cos** *cos-value*	Specifies the CoS value to cos-value. The *cos-value* can range from 0 to 7. **Note** This command is supported only for egress policies.

Configuring DSCP Marking

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

Note You can set DSCP or IP precedence but you cannot set both values because they modify the same field in the IP packet.

Table 4: Standard DSCP Values

Value	List of DSCP Values
af11	AF11 dscp (001010)—decimal value 10
af12	AF12 dscp (001100)—decimal value 12
af13	AF13 dscp (001110)—decimal value 14
af21	AF21 dscp (010010)—decimal value 18
af22	AF22 dscp (010100)—decimal value 20
af23	AF23 dscp (010110)—decimal value 22
af31	AF31 dscp (011010)—decimal value 26

Value	List of DSCP Values
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

Procedure

	Command or Action	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**policy-map type qos** *qos-policy-map-name*	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	**class** [**type qos**] {*class-map-name* | **class-default**}	Creates a reference to class-map-name, and enters policy-map class configuration mode. Use the **class-default** keyword to select all traffic that is not currently matched by classes in the policy map.
Step 4	**set dscp** *dscp-value*	Sets the DSCP value to dscp-value. See the Standards DSCP Values table.

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

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

Configuring IP Precedence Marking

You can set the value of the IP precedence field in bits 0 to 2 of the IPv4 type of service (ToS) field. The following table shows the precedence values:

Note You can set IP precedence or DSCP but you cannot set both values because they modify the same field in the IP packet.

Table 5: 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# **config terminal**	Enters global configuration mode.
Step 2	switch(config) # **policy-map** [**type qos**] *qos-policy-map-name*	Creates or accesses the policy map named *policy-map-name*, and then enters policy-map mode. The policy-map name can contain alphabetic, hyphen, or underscore characters, is case sensitive, and can be up to 40 characters.
Step 3	switch(config-pmap-nq) # **class** [**type qos**] {*class-map-name* | **class-default**}	Creates a reference to class-map-name, and enters policy-map class configuration mode. 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-nq) # **set precedence** *precedence-value*	Sets the IP precedence value to precedence-value. You can enter one of the values shown in the Precedence Values table.

This example shows how to set the precedence marking to 5:

```
switch(config)# policy-map type qos my_policy
switch(config-pmap-qos)# class type qos my_class
switch(config-pmap-c-qos)# set precedence 5
switch(config-pmap-c-qos)#
```

Attaching the System Service Policy

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

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **system qos**	Enters system class configuration mode.
Step 3	switch(config-sys-qos)# **service-policy type** {**network-qos** | **qos input** |**queuing** [**input** | **output**]} *policy-name*	Specifies the policy map to use as the service policy for the system. There are three policy-map configuration modes: • network-qos—Network-wide (system qos) mode. • qos—Classification mode (system qos input or interface input only). • queuing—Queuing mode (output at system qos and interface).

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

Restoring the Default System Service Policies

If you have created and attached new policies to the system QoS configuration, enter the **no** form of the command to reapply the default policies.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **system qos**	Enters system class configuration mode.
Step 3	switch(config-sys-qos)# **no service-policy type qos input** *policy-map name*	Resets the classification mode policy map. This policy-map configuration is for system QoS input or interface input only:
Step 4	switch(config-sys-qos)# **no service-policy type network-qos** *policy-map name*	Resets the network-wide policy map.
Step 5	switch(config-sys-qos)# **no service-policy type queuing [input | output]***policy-map name*	Resets the output queuing mode policy map.

Enabling the Jumbo MTU

You can enable the jumbo Maximum Transmission Unit (MTU) for the whole switch by setting the MTU to its maximum size (9216 bytes) in the policy map for the default Ethernet system class (class-default).

When you configure jumbo MTU on a port-channel subinterface you must first enable MTU 9216 on the base interface and then configure it again on the subinterface. If you enable the jumbo MTU on the subinterface before you enable it on the base interface then the following error will be displayed on the console:

```
switch(config)# int po 502.4
switch(config-subif)# mtu 9216
ERROR: Incompatible MTU values
```

Note The Cisco Nexus device supports 1 MTU for all classes for all ports.

To use FCoE on switch, add class-fcoe in the custom network-qos policy. If already using FCoE, make sure to add the below lines in the config so that the FCoE does not go down on the switch after enabling the jumbo qos policy.

```
switch# conf t
switch(config)# policy-map type network-qos jumbo
switch(config-pmap-nq)# class type network-qos class-fcoe
switch(config-pmap-nq-c)# end
```

This example shows how to change qos to enable the jumbo MTU:

```
switch# conf t
switch(config)# policy-map type network-qos jumbo
switch(config-pmap-nq)# class type network-qos class-default
switch(config-pmap-c-nq)# mtu 9216
```

Note The **system jumbomtu** command defines the maximum MTU size for the switch. However, jumbo MTU is supported only for system classes that have MTU configured.

Verifying the Jumbo MTU

On the Cisco Nexus device, traffic is classified into one of eight QoS groups. The MTU is configured at the QoS group level. By default, all Ethernet traffic is in QoS group 0. To verify the jumbo MTU for Ethernet traffic, use the **show queueing interface ethernet** *slot/chassis_number* command and find "HW MTU" in the command output to check the MTU for QoS group 0. The value should be 9216.

The **show interface** command always displays 1500 as the MTU. Because the Cisco Nexus device supports different MTUs for different QoS groups, it is not possible to represent the MTU as one value on a per interface level.

This example shows how to display jumbo MTU information for Ethernet 1/19:

```
switch(config)# show queuing interface ethernet 1/19
Ethernet1/19 queuing information:
  TX Queuing
    qos-group  sched-type  oper-bandwidth
        0       WRR            100

  RX Queuing
    Multicast statistics:
        Mcast pkts dropped                      : 0
    Unicast statistics:
    qos-group 0
    HW MTU: 9216 (9216 configured)
    drop-type: drop, xon: 0, xoff: 0
    Statistics:
        Ucast pkts dropped                      : 0
```

Configuring QoS on Interfaces

Configuring Untagged CoS

Any incoming packet not tagged with an 802.1p CoS value is assigned the default untagged CoS value of zero (which maps to the default Ethernet drop system class). You can override the default untagged CoS value for an Ethernet or EtherChannel interface.

You can configure flow control on a Layer 2 or Layer 3 interface. Use the **no switchport** command to configure a Layer 3 interface

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **interface** {**ethernet** [*chassis*/]*slot*/*port* | **port-channel** *channel-number*}	Enters the configuration mode for the specified interface or port channel.
Step 3	switch(config-if)# **no switchport**	(Optional) Selects a Layer 3 interface.
Step 4	switch(config-if)# **untagged cos** *cos-value*	Configures the untagged CoS value. Values can be from 1 to 7.

The following example shows how to set the CoS value to 4 for untagged frames received on an interface:

```
switch# configure terminal
switch(config)# interface ethernet 1/2
switch(config-if)# untagged cos 4
```

The following example shows how to set the CoS value to 3 for untagged frames received on a Layer 3 interface:

```
switch# configure terminal
switch(config)# interface ethernet 1/5
switch(config-if) no switchport
switch(config-if)# untagged cos 3
switch(config-if)#
```

Configuring Buffers and Queues

Configuring a Multicast Slow Receiver Port

When you have a combination of 10-gigabyte and 1-gigabyte ports, you can use this command on the 1-gigabyte port to reduce the effects of the 1-gigabyte port blocking the 10-gigabyte port. Use this command on the 1-gigabyte port only when there is Head-of-Line Blocking (HOLB) on the 10-gigabyte port due to a slow receiver on the 1-gigabyte port.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **hardware profile multicast slow-receiver port port** *port-number*}	Configures a specific 1-Gigabyte port as a slow-receiver port so that it does not block the 10-Gigabyte port. **Note** You can use this configuration on only one of the four ports of a port-group.
Step 3	switch(config)# **copy running-config startup-config**	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

The following example shows how to configure port 46 as the multicast slow-receiver port:

```
switch# configure terminal
switch(config)# hardware profile multicast slow-receiver port 46
switch(config)# copy running-config startup-config
```

Configuring the Percentage of Buffer Used for a Specific QoS Group or Virtual Lane

You can configure the percentage of shared buffer used for a specific QoS group or virtual lane (VL)

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch# **hardware profile buffer qosgroup** *number* **threshold** *percentage*	Configures the buffer for the specified QoS group. The *number* argument specifies the QoS group number. The range is from 0 to 4. The *percentage* argument specified the percentage of maximum usages. The range is from 1 to 100.
Step 3	switch(config)# **copy running-config startup-config**	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

The following example shows how to configure the shared buffer for QoS group 1 to a maximum of 40 percent usage:

```
switch# configure terminal
```

```
switch(config)# hardware profile buffer qosgroup 1 threshold 40
switch(config)# copy running-config startup-config
```

Configuring the Percentage of Buffer Used for SPAN Traffic

You can configure the percentage of shared buffer used for SPAN traffic.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch# **hardware buffer span-threshold** *percentage*	Configures the percentage of maximum usage of the hardware buffer for SPAN traffic. The *percentage* range is from 0 to 100.
Step 3	switch(config)# **copy running-config startup-config**	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

The following example shows how to configure 30 percent of the hardware buffer for SPAN traffic:

```
switch# configure terminal
switch(config)# hardware buffer span-threshold 30
switch(config)# copy running-config startup-config
```

Verifying the Qos Configuration

To verify the QoS configurations, perform one of these tasks:

Command	Purpose
switch# **show class-map**	Displays the class maps defined on the device.
switch# **show policy-map** [*name*]	Displays the policy maps defined on the device. Optionally, you can display the named policy only.
switch# **show policy-map interface** [*interface number*]	Displays the policy map settings for an interface or all interfaces.
switch# **show policy-map system**	Displays the policy map settings attached to the system qos.
switch# **show policy-map type** {**network-qos** | **qos** | **queuing**} [*name*]	Displays the policy map settings for a specific policy type. Optionally, you can display the named policy only.

Command	Purpose
switch# **show interface untagged-cos** [**module** *number*]	Displays the untagged CoS values for all interfaces.
switch# **show wrr-queue cos-map** [*var*]	Displays the mapped CoS values to egress queues.
switch# **running-config ipqos**	Displays information about the running configuration for QoS.
switch# **startup-config ipqos**	Displays information about the startup configuration for QoS.
switch# **show queuing interface ethernet** *slot-no/port-no*	Displays the queuing information on interfaces.

This example shows how to configure a network QoS policy:

```
switch(config)# class-map type network-qos cnq1
switch(config-cmap-nq)# match qos-group 1
switch(config-cmap-nq)# exit
switch(config)# class-map type network-qos cnq6
switch(config-cmap-nq)# match qos-group 6
switch(config-cmap-nq)#
switch(config-cmap-nq)# exit
switch(config)# policy-map type network-qos pnqos
switch(config-pmap-nq)# class type network-qos cnq1
switch(config-pmap-nq-c)# set cos 4
switch(config-pmap-nq-c)# exit
switch(config-pmap-nq)# class type network-qos cnq6
switch(config-pmap-nq-c)# set cos 5
switch(config-pmap-nq-c)# congestion-control random-detect ecn
switch(config-pmap-nq-c)# exit
switch(config-pmap-nq)# class type network-qos class-default
switch(config-pmap-nq-c)# mtu 9216
switch(config-pmap-nq-c)# exit
switch(config-pmap-nq)# exit
switch(config)# system qos
switch(config-sys-qos)# service-policy type network-qos pnqos
switch(config-sys-qos)#
```

This example shows how to configure a queuing policy:

```
switch(config)# class-map type queuing cqu1
switch(config-cmap-que)# match qos-group 1
switch(config-cmap-que)# exit
switch(config)# class-map type queuing cqu6
switch(config-cmap-que)# match qos-group 6
switch(config-cmap-que)# exit
switch(config)# policy-map type queuing pqu
switch(config-pmap-que)# class type queuing class-default
switch(config-pmap-c-que)# bandwidth percent 70
switch(config-pmap-c-que)# exit
switch(config-pmap-que)# class type queuing cqu1
switch(config-pmap-c-que)# bandwidth percent 10
switch(config-pmap-c-que)# exit
switch(config-pmap-que)# class type queuing cqu6
switch(config-pmap-c-que)# bandwidth percent 20
switch(config-pmap-c-que)# exit
switch(config-pmap-que)# exit
switch(config)# system qos
switch(config-sys-qos)# service-policy type queuing output pqu
switch(config-sys-qos)#
```

This example shows how to configure a QoS policy:

```
switch(config)# class-map type qos cqos1
switch(config-cmap-qos)# match cos 1
switch(config-cmap-qos)# exit
switch(config)# class-map type qos cqos6
switch(config-cmap-qos)# match cos 6
switch(config-cmap-qos)# exit
switch(config)# policy-map type qos pqos
switch(config-pmap-qos)# class type qos cqos1
switch(config-pmap-c-qos)# set qos-group 1
switch(config-pmap-c-qos)# exit
switch(config-pmap-qos)# class type qos cqos6
switch(config-pmap-c-qos)# set qos-group 6
switch(config-pmap-c-qos)# exit
switch(config-pmap-qos)# exit
switch(config)# system qos
switch(config-sys-qos)# service-policy type qos input pqos
switch(config-sys-qos)#
```

This example shows how to verify the untagged-cos configuration on interfaces:

```
switch(config-if)# show interface untagged-cos
================================

Interface      Untagged-CoS
=================================

Ethernet1/1  4
Ethernet1/2
Ethernet1/3  5
Ethernet1/4
Ethernet1/5
Ethernet1/6
Ethernet1/7
Ethernet1/8
Ethernet1/9
Ethernet1/10
Ethernet1/11
Ethernet1/12
Ethernet1/13
Ethernet1/14
Ethernet1/15
Ethernet1/16
Ethernet1/17
```

This example shows how to display the QoS running configuration:

```
switch(config)# show running-config ipqos

!Command: show running-config ipqos
!Time: Mon Mar 15 08:24:12 2010

version 5.0(3)U1(1)
class-map type qos match-all cqos1
  match cos 1
class-map type qos match-all cqos6
  match cos 6
class-map type queuing cqu1
  match qos-group 1
class-map type queuing cqu6
  match qos-group 6
policy-map type qos pqos
  class cqos1
    set qos-group 1
  class cqos6
    set qos-group 6
policy-map type queuing pqu
  class type queuing cqu1
    bandwidth percent 10
  class type queuing cqu6
    bandwidth percent 20
  class type queuing class-default
    bandwidth percent 70
```

```
class-map type network-qos cnq1
  match qos-group 1
class-map type network-qos cnq6
  match qos-group 6
policy-map type network-qos pnqos
  class type network-qos cnq1
    set cos 4
  class type network-qos cnq6
    set cos 5
    congestion-control random-detect ecn
  class type network-qos class-default
    mtu 9216
system qos
  service-policy type qos input pqos
  service-policy type network-qos pnqos
  service-policy type queuing output pqu


interface Ethernet1/1
  untagged cos 4

interface Ethernet1/3
  untagged cos 5

switch(config)#
```

This example shows how to display the class map configuration:

```
switch(config)# show class-map


  Type qos class-maps
  ===================

    class-map type qos match-all cqos1
      match cos 1

    class-map type qos match-all cqos6
      match cos 6

    class-map type qos match-any class-default
      match any


  Type queuing class-maps
  =======================

    class-map type queuing cqu1
      match qos-group 1

    class-map type queuing cqu6
      match qos-group 6

    class-map type queuing class-default
      match qos-group 0



  Type network-qos class-maps
  ===============================

    class-map type network-qos cnq1
      match qos-group 1

    class-map type network-qos cnq6
      match qos-group 6

    class-map type network-qos class-default
      match qos-group 0

switch(config)#
```

This example shows how to display the policy map configuration:

```
switch(config)# show policy-map


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

  policy-map type qos pqos
    class type qos cqos1
      set qos-group 1
    class type qos cqos6
      set qos-group 6
    class type qos class-default
      set qos-group 0
  policy-map type qos default-in-policy
    class type qos class-default
      set qos-group 0

  Type queuing policy-maps
  ========================

  policy-map type queuing pqu
    class type queuing cqu1
      bandwidth percent 10
    class type queuing cqu6
      bandwidth percent 20
    class type queuing class-default
      bandwidth percent 70
  policy-map type queuing default-out-policy
    class type queuing class-default
      bandwidth percent 100


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

  policy-map type network-qos pnqos
    class type network-qos cnq1
      mtu 1500
      set cos 4
    class type network-qos cnq6
      mtu 1500
      set cos 5
      congestion-control random-detect ecn
    class type network-qos class-default
      mtu 9216
  policy-map type network-qos default-nq-policy
    class type network-qos class-default
      mtu 1500
switch(config)#
```

This example shows how to display all active policy maps in the system:

```
switch(config)# show policy-map system


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

  policy-map type network-qos pnqos
    class type network-qos cnq1      match qos-group 1

      mtu 1500
      set cos 4
    class type network-qos cnq6      match qos-group 6

      mtu 1500
      set cos 5
      congestion-control random-detect ecn
    class type network-qos class-default      match qos-group 0

      mtu 9216
```

```
  Service-policy (qos) input:   pqos
    policy statistics status:   disabled

    Class-map (qos):   cqos1 (match-all)
      Match: cos 1
      set qos-group 1

    Class-map (qos):   cqos6 (match-all)
      Match: cos 6
      set qos-group 6

    Class-map (qos):   class-default (match-any)
      Match: any
      set qos-group 0

  Service-policy (queuing) output:   pqu
    policy statistics status:   disabled

    Class-map (queuing):   cqu1 (match-any)
      Match: qos-group 1
      bandwidth percent 10

    Class-map (queuing):   cqu6 (match-any)
      Match: qos-group 6
      bandwidth percent 20

    Class-map (queuing):   class-default (match-any)
      Match: qos-group 0
      bandwidth percent 70

switch(config)#
```

This example shows how to display the service policy maps configured on the interfaces:

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


Global statistics status :   disabled

Ethernet1/1

  Service-policy (qos) input:   pqos
    policy statistics status:   disabled

    Class-map (qos):   cqos1 (match-all)
      Match: cos 1
      set qos-group 1

    Class-map (qos):   cqos6 (match-all)
      Match: cos 6
      set qos-group 6

    Class-map (qos):   class-default (match-any)
      Match: any
      set qos-group 0

  Service-policy (queuing) output:   pqu
    policy statistics status:   disabled

    Class-map (queuing):   cqu1 (match-any)
      Match: qos-group 1
      bandwidth percent 10

    Class-map (queuing):   cqu6 (match-any)
      Match: qos-group 6
      bandwidth percent 20

    Class-map (queuing):   class-default (match-any)
      Match: qos-group 0
      bandwidth percent 70

switch(config)#
```

This example shows how to display the queuing information for a specific interface:

```
switch(config)# show queuing interface ethernet 1/1
Ethernet1/1 queuing information:
  TX Queuing
    qos-group  sched-type  oper-bandwidth
        0       WRR             20
        1       WRR             10
        2       WRR             10
        3       WRR             10
        4       WRR             10

  RX Queuing
    Multicast statistics:
        Mcast pkts dropped                      : 0
    Unicast statistics:
    qos-group 0
    HW MTU: 1500 (1500 configured)
    drop-type: drop, xon: 0, xoff: 0
    Statistics:
        Ucast pkts dropped                      : 0
    qos-group 1
    HW MTU: 1500 (1500 configured)
    drop-type: drop, xon: 0, xoff: 0
    Statistics:
        Ucast pkts dropped                      : 0
    qos-group 2
    HW MTU: 1500 (1500 configured)
    drop-type: drop, xon: 0, xoff: 0
    Statistics:
        Ucast pkts dropped                      : 0
    qos-group 3
    HW MTU: 1500 (1500 configured)
    drop-type: drop, xon: 0, xoff: 0
    Statistics:
        Ucast pkts dropped                      : 0
    qos-group 4
    HW MTU: 1500 (1500 configured)
    drop-type: drop, xon: 0, xoff: 0
    Statistics:
        Ucast pkts dropped                      : 0
```

CHAPTER 4

Configuring Active Latency Monitoring

This chapter contains the following sections:

Active Latency Monitoring Overview

Active Latency Monitoring provides a real-time view of the latency that is incurred by the packets while traveling through the switch on a per port basis. The latency measurement is FIFO measurement. Functionally, as soon as the packet enters the switch, the ASIC adds a timestamp to it. When it is scheduled to go out of the egress port, the egress port calculates the latency for each packet that is going out of that port based on current time and the ingress timestamp on the packet.

Note Active latency monitoring is currently not available for Cisco Nexus N3548 Series switches. This feature is only supported for Cisco Nexus N3548-X Series switches.

Each egress port maintains the information in the frame count and the latency register, along with the minimum and maximum latency on that port. The software periodically reads the frame count (default 3 seconds) and the total latency to calculate the average latency per port. Based on per port latency information, the software calculates the average switch latency.

Active Latency Monitoring Guidelines and Limitations

Active Latency Monitoring has the following limitations and guidelines:

- Disabling the latency monitor does not clear the existing latency monitor data.
- Clear the latency monitor data before enabling the latency monitor.
- The latency monitor data is lost when the sampling interval is modified.

- The latency monitor data is not maintained across a switch reload.

Configuring Active Latency Monitoring

To configure active latency monitoring, complete the following steps:

Note The average or maximum latency threshold is in nanoseconds. The software sampling interval value is between 1 to 30 seconds. The default values for the parameters are:

- Sampling = 3 seconds
- Threshold-avg = 1000000 nanoseconds
- Threshold-max = 2000000 nanoseconds

Procedure

	Command or Action	Purpose
Step 1	**clear hardware profile latency monitor**	Clears the latency monitor data.
Step 2	**[no] hardware profile latency monitor**	Enables or disables latency monitoring.
Step 3	**hardware profile latency monitor threshold-avg <value>**	(Optional) Sets the average threshold for syslog generation.
Step 4	**hardware profile latency monitor threshold-max <value>**	(Optional) Sets the maximum threshold for syslog generation.
Step 5	**hardware profile latency monitor sampling <value>**	(Optional) Sets the sampling interval in seconds.
Step 6	**exit**	Updates the configuration and exits the configuration mode.
Step 7	**show hardware profile latency monitor summary**	(Optional) Displays the latency values on the packets.

Show Examples for Active Latency Monitoring

See the following examples that provide a real-time view of the latency incurred by the packets:

```
switch# show hardware profile latency monitor summary

10/13/2015 06:55:58
Device instance 0

Total Switch
```

```
============
                    3s              30s             1hr             All Time

Min Latency (ns)    390             375             n/a             369

Max Latency (ns)    775             1844            n/a             1950

Avg Latency (ns)    612             721             n/a             754

Std Deviation       205.24          117.23          n/a             69.17


Ethernet1/1
===========
                    3s              30s             1hr             All Time

Min Latency (ns)    775             762             n/a             762

Max Latency (ns)    775             1757            n/a             1950

Avg Latency (ns)    775             838             n/a             870

Std Deviation       n/a             83.87           n/a             100.93

<snip>

Ethernet1/13
============
                    3s              30s             1hr             All Time

Min Latency (ns)    671             646             n/a             644

Max Latency (ns)    671             1844            n/a             1844

Avg Latency (ns)    671             736             n/a             740

Std Deviation       n/a             100.16          n/a             93.76
```

```
switch# show hardware profile latency monitor summary detail

10/13/2015 06:57:00
Device instance 0
Format:
        timestamp
        ifindex
        fcnt
        min_latency
        max_latency
        avg_latency
10/13/2015 06:56:58
Ethernet1/1
fcnt          2
min_latency   565
max_latency   571
avg_latency   568
10/13/2015 06:56:55
Ethernet1/1
fcnt          1
min_latency   576
max_latency   576
avg_latency   576
10/13/2015 06:56:52

<snip>

Ethernet1/2
fcnt          0
min_latency   4294967295
max_latency   0
avg_latency   0
10/13/2015 06:56:55
Ethernet1/2
```

```
fcnt          0
min_latency   4294967295
max_latency   0
avg_latency   0
10/13/2015 06:56:52


switch# # show hardware profile latency monitor summary clear-timestamp

10/13/2015 06:56:31
Device instance 0

Egress Port             Last Clear Timestamp
==========================================

Total Switch            10/13/2015 06:54:35

Ethernet1/1             10/13/2015 06:54:35

Ethernet1/2             10/13/2015 06:54:35

<snip>

Ethernet1/47            10/13/2015 06:54:35

Ethernet1/48            10/13/2015 06:54:35


switch# show hardware profile latency monitor summary brief

10/13/2015 06:57:27
Device instance 0

Egress Port             Avg Latency (ns)
=======================================

Total Switch            769

Ethernet1/1             874

Ethernet1/2             1682

<snip>

Ethernet1/47            n/a

Ethernet1/48            n/a


switch# show hardware profile latency monitor summary sort
10/13/2015 06:57:34
Device instance 0

Egress Port             Avg Latency (ns)
=======================================

Ethernet1/2             1682

Ethernet1/5             1664

Ethernet1/1             871

Ethernet1/13            765

Ethernet1/6             507

Ethernet1/3             n/a


switch# show hardware profile latency monitor summary top

10/13/2015 06:57:44
```

```
Device instance 0

Egress Port             Avg Latency (ns)
========================================

Ethernet1/2             1682

Ethernet1/5             1664

<snip>

Ethernet1/6             500

Ethernet1/3             n/a
```

CHAPTER 5

Configuring Link Level Flow Control

This chapter contains the following sections:

Link Level Flow Control

Link-level flow control is a congestion management technique that pauses data transmission until the congestion in the system is resolved. When a receiving device becomes congested, it communicates with the transmitter by sending a PAUSE frame. When the transmitting device receives a Pause frame it stops the transmission of any further data frames for a short period of time. The link-level flow control feature applies to all the traffic on the link. The transmit and receive directions are separately configurable. By default, link-level flow control is disabled for both directions.

Guidelines and Restrictions for Link Level Flow Control

- Ethernet interfaces do not auto-detect the link-level flow control capability. You must configure the capability explicitly.
- Only link-level flow control is supported. Priority flow control (PFC) is not supported.
- Enabling link level flow control requires a part of the buffer to be reserved. This reduces the available shared buffer space.
- Flow control is not supported on 40G ports.
- Data Center Bridging Exchange Protocol (DCBX) is not supported.
- Configuration time quanta of the pause frames is not supported.
- Only pure CoS-based classification of traffic classes is supported.

- Setting of pause threshold values is restricted.
- Configuring Link Level Flow Control on the interfaces will flap the interfaces which results in a momentary traffic loss.
- When a no-drop QoS group is configured, you must ensure that packets received on ports that do not have flow control send-on configured are not classified to a no-drop QoS group.
- Only a no-drop QoS group is capable of generating link level pause frames.
- Weighted Random Early Detection (WRED) should not be enabled on a no-drop class because it can cause egress queue drops.
- It is recommended to use default buffer sizes for no-drop classes because if the buffer size is specified through CLI, it will allocate the same buffer size for all ports irrespective of the link speed, and MTU size.
- It is recommended to change the LLFC configuration when there is no traffic, otherwise packets already in the MMU of the system may not get the expected treatment.
- When configuring a no-drop class for QoS you must use QoS-Group 1 and map the QoS Group 1 to the no-drop class.

Information About Link Level Flow Control

Link Level Flow Control on Interfaces

When link level flow control is configured the system changes the interface state to Down if the specified interface is in UP state and then applies the flow control configuration. After the configuration is successfully applied to the interface, the system restores the interface to the UP state.

Link Level Flow Control on Ports

During a port shutdown event, the flow-control settings on an interface are retained, however no traffic is received or transmitted on the link. During a port startup event the flow-control settings are reinstated on to the hardware.

Mismatched Link Level Flow Control Configurations

The transmit and receive directions can be configured separately, and each device on the network can have a different Link Level Flow Control (LLFC) configuration. The following table describes how devices with mis-matched configurations interact.

Switch A	Switch B	Description
LLFC configured to receive and transmit PAUSE frames.	LLFC configured to receive PAUSE frames.	Switch A can transmit 802.3x PAUSE frames and honor 802.3x PAUSE frames. Switch B can only receive 802.3x PAUSE frames.

Switch A	Switch B	Description
LLFC configured to receive and transmit PAUSE frames.	LLFC configured to transmit PAUSE frames.	Switch A can transmit 802.3x PAUSE frames and honor 802.3x PAUSE frames. Switch B can transmit 802.3x PAUSE frames but will drop all received PAUSE frames.

How to Configure Link Level Flow Control

Configuring Link Level Flow Control Receive

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface ethernet 1/1** **Example:** `Device(config)# interface ethernet 1/1`	Configures an interface type and enters interface configuration mode.
Step 4	**flowcontrol receive on** **Example:** `Device(config-if)# flowcontrol receive on`	Enables the interface to receive and process pause frames.
Step 5	**exit** **Example:** `Device(config-if)# exit`	Exits interface configuration mode.

Configuring Link Level Flow Control Transmit

To configure link-level flow control transmit on an interface, you enable flow control on the interface, configure a network-qos type QoS policy to enable a no-drop QoS group, and apply a qos type QoS policy to classify the traffic that requires no-drop behavior to the no-drop class.

You must ensure that bandwidth is allocated for the No-Drop QoS class using a queuing policy when you define a no-drop class. For more information, see the "Configuring Type Queuing Policies" section.

Note When a no-drop QoS Group is configured you must ensure that packets received on ports that do not have flow-control send-on configured, are not classified to a no-drop QoS group. This is required as any ingress port that does not have flow-control send-on configured, can not generate a link level pause frame and there is no way to request the transmitting device to stop the transmission. Therefore, if flow-control send-on is not configured on all the interfaces you should not use a system policy to classify the packets to the no-drop QoS group. Instead, you should apply an interface QoS policy to the interfaces that having flow-control send-on enabled.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface ethernet 1/1** **Example:** `Device(config)# interface ethernet 1/1`	Configures an interface type and enters interface configuration mode.
Step 4	**flowcontrol send on** **Example:** `Device(config-if)# flowcontrol send on`	Enables the interface to send pause frames to remote devices.
Step 5	**exit** **Example:** `Device(config-if)# exit`	Exits interface configuration mode and returns to global configuration mode.

	Command or Action	Purpose
Step 6	**class-map type** *network-qos class-name* **Example:** `Device(config)# class-map type network-qos class1`	Creates a network-qos class, and places the device in network-qos class-map configuration mode.
Step 7	**match qos-group** *group-number* **Example:** `Device(config-cmap-nq)# match qos-group 1`	Specifies an interface type and number, and places the device in interface configuration mode.
Step 8	**policy-map type** *network-qos policy-map-name* **Example:** `Device(config-cmap-nq)# policy-map type network-qos my_network_policy`	Creates a network-qos policy map, and places the device in network-qos policy-map configuration mode.
Step 9	**class type** *network-qos class-name* **Example:** `Device(config-pmap-nq)# class type network-qos class1`	Specifies the network-qos class map to use for matching, for this policy, and and places the device in network-qos policy-map-class configuration mode.
Step 10	**pause no-drop** **Example:** `Device(config-pmap-nq-c)# pause no-drop`	Specifies the pause characteristics for this class.
Step 11	**system qos** **Example:** `Device(config-pmap-nq-c)# system qos`	Enters QoS system configuration mode.
Step 12	**service-policy type network-qos** *policy-name* **Example:** `Device(config-sys-qos)# service-policy type network-qos my_network_policy`	Applies a QoS policy map to the network.
Step 13	**exit** **Example:** `Device(config-sys-qos)# exit`	Exits QoS system configuration mode and returns to global configuration mode.

	Command or Action	Purpose
Step 14	**class-map type qos** *class-map-name* **Example:** `Device(config)# class-map type qos class1`	Creates a class map and enters the class-map configuration mode.
Step 15	**match cos** *cos-value* **Example:** `Device(config-cmap-qos)#  match cos 2`	Defines the class of traffic using the class of service (CoS) value in a type qos class map .
Step 16	**policy-map type qos** *policy-name* **Example:** `Device(config-cmap-qos)#  policy-map type qos my_qos_policy`	Creates a policy map and enters the policy map type qos configuration mode.
Step 17	**class type qos** *class-name* **Example:** `Device(config-pmap-qos)# class type qos class1`	Adds a reference to an existing qos class map in a policy map and enters the class mode.
Step 18	**set qos-group** *group-number* **Example:** `Device(config-pmap-c-qos)# set qos-group 1`	Assigns the QoS group identifier for a class of traffic in a type qos policy map.
Step 19	**system qos** **Example:** `Device(config-pmap-c-qos)# system qos`	Configures a QoS system policy and enters system QoS configuration mode.
Step 20	**service-policy type qos input** *policy-map-name* **Example:** `Device(config-sys-qos)# service-policy type qos input my_qos_policy`	Attaches a policy map to a system policy.
Step 21	**exit** **Example:** `Device(config-sys-qos)# exit`	Exits QoS system configuration mode and returns to global configuration mode.

	Command or Action	Purpose
Step 22	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode.
Step 23	**show running ipqos** **Example:** `Device# show running ipqos`	Shows the running configuration for the IP QoS Manager.

Configuration Examples for Link Level Flow Control

Example: Configuring Link Level Flow Control Receive

Configuring Link Level Flow Control Receive

The following example shows how to configure Link Level Flow Control receive on the device:

```
Device# configure terminal
Device(config)# interface ethernet 1/1
Device(config-if)# flowcontrol receive on
Device(config-if)# exit
```

INDEX

Q

R

S

T

V