



Quality of Service Configuration Guide, Cisco IOS Release 15.2(7)Ex (Catalyst 2960-L Switches)

First Published: 2019-03-27

Last Modified: 2019-12-10

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2019 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1

Configuring AutoQoS 1

- Prerequisites for Auto-QoS 1
- Restrictions for Auto-QoS 1
- Information about Configuring Auto-QoS 2
 - Auto-QoS Overview 2
 - Generated Auto-QoS Configuration 3
 - VoIP Device Specifics 3
 - Enhanced Auto-QoS for Video, Trust, and Classification 4
 - Auto-QoS Configuration Migration 4
- Auto-QoS Configuration Guidelines 4
 - Auto-QoS VoIP Considerations 5
 - Auto-QoS Enhanced Considerations 5
- Effects of Auto-QoS on Running Configuration 5
- How to Configure Auto-QoS 5
 - Enabling Auto-QoS 6
 - Troubleshooting Auto-QoS 7
- Monitoring Auto-QoS 8
- Configuration Example for Auto-QoS 8
 - Examples: Global Auto-QoS Configuration 9
 - Examples: Auto-QoS Generated Configuration For Enhanced Video, Trust, and Classify Devices 10
- Additional References for Auto-QoS 12
- Feature History and Information for Auto-QoS 12

CHAPTER 2

Configuring QoS 13

- Prerequisites for QoS 13

QoS ACL Guidelines	13
Policing Guidelines	13
General QoS Guidelines	14
Restrictions for QoS	14
Information About QoS	15
QoS Implementation	15
Layer 2 Frame Prioritization Bits	16
Layer 3 Packet Prioritization Bits	16
End-to-End QoS Solution Using Classification	16
QoS Basic Model	17
Actions at Ingress Port	17
Actions at Egress Port	18
Classification Overview	18
Policing and Marking Overview	22
Queueing and Scheduling Overview	23
Queueing and Scheduling on Egress Queues	25
Packet Modification	27
Standard QoS Default Configuration	28
Default Egress Queue Configuration	28
Default Mapping Table Configuration	29
How to Configure QoS	29
Enabling QoS Globally	29
Configuring Classification Using Port Trust States	30
Configuring the Trust State on Ports Within the QoS Domain	30
Configuring the CoS Value for an Interface	32
Configuring a Trusted Boundary to Ensure Port Security	34
Enabling DSCP Transparency Mode	35
Configuring the DSCP Trust State on a Port Bordering Another QoS Domain	37
Configuring a QoS Policy	38
Classifying Traffic by Using ACLs	38
Classifying Traffic by Using Class Maps	45
Classifying, Policing, and Marking Traffic on Physical Ports by Using Policy Maps	47
Configuring Egress Queue Characteristics	50
Configuration Guidelines	50

Mapping DSCP or CoS Values to an Egress Queue and to a Threshold ID	51
Configuring SRR Shaped Weights on Egress Queues	53
Configuring SRR Shared Weights on Egress Queues	54
Configuring the Egress Expedite Queue	55
Limiting the Bandwidth on an Egress Interface	56
Monitoring Standard QoS	57
Configuration Examples for QoS	58
Example: Configuring Port to the DSCP-Trusted State and Modifying the DSCP-to-DSCP-Mutation Map	58
Examples: Classifying Traffic by Using ACLs	58
Examples: Classifying Traffic by Using Class Maps	59
Examples: Classifying, Policing, and Marking Traffic on Physical Ports Using Policy Maps	60
Examples: Configuring DSCP-to-DSCP Mutation Maps	62
Examples: Configuring Egress Queue Characteristics	62
Feature Information for QoS	63



CHAPTER 1

Configuring AutoQoS

- [Prerequisites for Auto-QoS, on page 1](#)
- [Restrictions for Auto-QoS, on page 1](#)
- [Information about Configuring Auto-QoS, on page 2](#)
- [How to Configure Auto-QoS, on page 5](#)
- [Monitoring Auto-QoS, on page 8](#)
- [Configuration Example for Auto-QoS, on page 8](#)
- [Additional References for Auto-QoS, on page 12](#)
- [Feature History and Information for Auto-QoS, on page 12](#)

Prerequisites for Auto-QoS

Before configuring standard QoS or auto-QoS, you must have a thorough understanding of these items:

- The types of applications used and the traffic patterns on your network.
- Traffic characteristics and needs of your network. Is the traffic bursty? Do you need to reserve bandwidth for voice and video streams?
- Bandwidth requirements and speed of the network.
- Location of congestion points in the network.

Restrictions for Auto-QoS

The following are restrictions for automatic QoS (auto-QoS):

- Ternary content-addressable memory (TCAM) sharing of policy-map (policer/markings) across ports is not supported. Because of this, the number of interfaces on which auto-QoS/QoS policy-map can be applied is limited.
- The same TCAM region must be used for both security Access control lists (ACLs) and ACLs used via policy map.
- Policy-maps with the **match ip dscp** command matches both IPv4 and IPv6 addresses, which limits the scale number to 16 class-maps. One TCAM entry is created for IPv4 and one TCAM entry for IPv6.

- Per ASIC, 8 TCP port comparators and 8 UDP port comparators are supported, and each gt (greater than)/lt (less than)/neq (not equal) operator uses 1 port comparator, and each range operator uses 2 port comparators. A policy-map with this combination affects the TCAM scale and number of interfaces to which the policy-map can be attached.
- The following restrictions apply to IPv4 ACL network interfaces:
 - When controlling access to an interface, you can use a named or numbered ACL.
 - If you apply an ACL to a Layer 3 interface, and routing is not enabled on the switch, the ACL only filters packets that are intended for the CPU, such as SNMP, Telnet, or web traffic.
 - You do not have to enable routing to apply ACLs on Layer 2 interfaces.
- Deny ACLs are not supported on QoS policy-maps.

Information about Configuring Auto-QoS

This section provides information about configuring Auto-QoS.

Auto-QoS Overview

You can use the auto-QoS feature to simplify the deployment of QoS features. Auto-QoS determines the network design and enables QoS configurations so that the switch can prioritize different traffic flows. It uses the egress queues instead of using the default (disabled) QoS behavior. The switch offers best-effort service to each packet, regardless of the packet contents or size, and sends it from a single queue.

When you enable auto-QoS, it automatically classifies traffic based on the traffic type and ingress packet label. The switch uses the classification results to choose the appropriate egress queue.

You can use auto-QoS commands to identify ports connected to the following Cisco devices:

- Cisco IP Phones
- Devices running the Cisco SoftPhone application
- Cisco TelePresence
- Cisco IP Camera
- Cisco digital media player

You also use the auto-QoS commands to identify ports that receive trusted traffic through an uplink. Auto-QoS then performs these functions:

- Detects the presence or absence of auto-QoS devices through conditional trusted interfaces.
- Configures QoS classification
- Configures egress queues

Generated Auto-QoS Configuration

By default, auto-QoS is disabled on all ports. Packets are not modified--the CoS, DSCP and IP precedence values in the packet are not changed.

When you enable the auto-QoS feature on the first port of the interface:

- Ingress packet label is used to categorize traffic, to assign packet labels, and to configure the ingress and egress queues.
- QoS is globally enabled (**mls qos** global configuration command), and other global configuration commands are automatically generated. (See [Examples: Global Auto-QoS Configuration, on page 9](#)).
- Switch enables the trusted boundary feature and uses the Cisco Discovery Protocol to detect the presence of a supported device.
- Policing is used to determine whether a packet is in or out of profile and specifies the action on the packet.

VoIP Device Specifics

The following activities occur when you issue these auto-QoS commands on a port:

- When you enter the **auto qos voip cisco-phone** command on a port at the network edge connected to a Cisco IP Phone, the switch enables the trusted boundary feature. If the packet does not have a DSCP value of 24, 26, or 46 or is out of profile, the switch changes the DSCP value to 0. When there is no Cisco IP Phone, the ingress classification is set to not trust the QoS label in the packet. The policing is applied to the traffic matching the policy-map classification before the switch enables the trust boundary feature.
- When you enter the **auto qos voip cisco-softphone** interface configuration command on a port at the network edge that is connected to a device running the Cisco SoftPhone, the switch uses policing to determine whether a packet is in or out of profile and to specify the action on the packet. If the packet does not have a DSCP value of 24, 26, or 46 or is out of profile, the switch changes the DSCP value to 0.
- When you enter the **auto qos voip trust** interface configuration command on a port connected to the network interior, the switch trusts the CoS value for nonrouted ports or the DSCP value for routed ports in ingress packets (the assumption is that traffic has already been classified by other edge devices).

Table 1: Traffic Types, Packet Labels, and Queues

	VoIP Data Traffic	VoIP Control Traffic	Routing Protocol Traffic	STP BPDU Traffic	Real-Time Video Traffic	All Other Traffic	
DSCP value	46	24, 26	48	56	34	—	
CoS value	5	3	6	7	3	—	
CoS-to-Egress queue map	4, 5 (queue 1)	2, 3, 6, 7 (queue 2)			0 (queue 2)	2 (queue 3)	0, 1 (queue 4)

- When you enable auto-QoS by using the **auto qos voip cisco-phone**, the **auto qos voip cisco-softphone**, or the **auto qos voip trust** interface configuration command, the switch automatically generates a QoS

configuration based on the traffic type and ingress packet label and applies the commands listed in [Examples: Global Auto-QoS Configuration, on page 9](#) to the port.

Enhanced Auto-QoS for Video, Trust, and Classification

Auto-QoS is enhanced to support video. Automatic configurations are generated that classify and trust traffic from Cisco TelePresence systems and Cisco IP cameras.

Auto-QoS Configuration Migration

Auto-QoS configuration migration from legacy auto-QoS to enhanced auto-QoS occurs when:

- A switch is booted with a 12.2(55)SE image and QoS is not enabled.
Any video or voice trust configuration on the interface automatically generates enhanced auto-QoS commands.
- A switch is enabled with QoS, these guidelines take effect:
 - If you configure the interface for conditional trust on a voice device, only the legacy auto-QoS VoIP configuration is generated.
 - If you configure the interface for conditional trust on a video device, the enhanced auto-QoS configuration is generated.
 - If you configure the interface with classification or conditional trust based on the new interface auto-QoS commands, enhanced auto-QoS configuration is generated.
- Auto-QoS migration happens after a new device is connected when the **auto qos srnd4** global configuration command is enabled.



Note

If an interface previously configured with legacy auto-QoS migrates to enhanced auto-QoS, voice commands and configuration are updated to match the new global QoS commands.

Auto-QoS configuration migration from enhanced auto-QoS to legacy auto-QoS can occur only when you disable all existing auto-QoS configurations from the interface.

Auto-QoS Configuration Guidelines

Before configuring auto-QoS, you should be aware of this information:

- After auto-QoS is enabled, do not modify a policy map that includes *AutoQoS* in its name. If you need to modify the policy map, make a copy of it, and change the copied policy map. To use this new policy map instead of the generated one, remove the generated policy map from the interface, and apply the new policy map to the interface.
- To take advantage of the auto-QoS defaults, you should enable auto-QoS before you configure other QoS commands. If necessary, you can fine-tune the QoS configuration, but we recommend that you do so only after the auto-QoS configuration is completed.
- You can enable auto-QoS on static, dynamic-access, voice VLAN access, and trunk ports.

- By default, the CDP is enabled on all ports. For auto-QoS to function properly, do not disable CDP.

Auto-QoS VoIP Considerations

Before configuring auto-QoS for VoIP, you should be aware of this information:

- Auto-QoS configures the switch for VoIP with Cisco IP Phones on nonrouted and routed ports. Auto-QoS also configures the switch for VoIP with devices running the Cisco SoftPhone application.



Note When a device running Cisco SoftPhone is connected to a nonrouted or routed port, the switch supports only one Cisco SoftPhone application per port.

- When enabling auto-QoS with a Cisco IP Phone on a routed port, you must assign a static IP address to the IP phone.
- This release supports only Cisco IP SoftPhone Version 1.3(3) or later.
- Connected devices must use Cisco Call Manager Version 4 or later.

Auto-QoS Enhanced Considerations

Auto-QoS is enhanced to support video. Automatic configurations are generated that classify and trust traffic from Cisco TelePresence systems and Cisco IP cameras.

Before configuring auto-QoS enhanced, you should be aware of this information:

- The **auto qos srnd4** global configuration command is generated as a result of enhanced auto-QoS configuration.

Effects of Auto-QoS on Running Configuration

When auto-QoS is enabled, the **auto qos** interface configuration commands and the generated global configuration are added to the running configuration.

The switch applies the auto-QoS-generated commands as if the commands were entered from the CLI. An existing user configuration can cause the application of the generated commands to fail or to be overridden by the generated commands. These actions may occur without warning. If all the generated commands are successfully applied, any user-entered configuration that was not overridden remains in the running configuration. Any user-entered configuration that was overridden can be retrieved by reloading the switch without saving the current configuration to memory. If the generated commands are not applied, the previous running configuration is restored.

How to Configure Auto-QoS

This section provides information about how to configure Auto-QoS.

Enabling Auto-QoS

For optimum QoS performance, enable auto-QoS on all the devices in your network.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 2	interface interface-id Example: Device(config)# interface gigabitethernet 0/1	Specifies the port that is connected to a video device or the uplink port that is connected to another trusted switch or router in the network interior, and enters interface configuration mode.
Step 3	Use one of the following: <ul style="list-style-type: none"> • auto qos voip {cisco-phone cisco-softphone trust} • auto qos video {cts ip-camera media-player} • auto qos classify [police] • auto qos trust {cos dscp} Example: Device(config-if)# auto qos trust dscp	Enables auto-QoS for VoIP. <ul style="list-style-type: none"> • cisco-phone: If the port is connected to a Cisco IP Phone, the QoS labels of incoming packets are trusted only when the telephone is detected. • cisco-softphone: The port is connected to device running the Cisco SoftPhone feature. • trust: The uplink port is connected to a trusted switch or router, and the VoIP traffic classification in the ingress packet is trusted. Enables auto-QoS for a video device. <ul style="list-style-type: none"> • cts: A port connected to a Cisco Telepresence system. • ip-camera: A port connected to a Cisco video surveillance camera. • media-player: A port connected to a CDP-capable Cisco digital media player. QoS labels of incoming packets are trusted only when the system is detected. Enables auto-QoS for classification. <ul style="list-style-type: none"> • police: Policing is set up by defining the QoS policy maps and applying them to ports (port-based QoS).

	Command or Action	Purpose
		Enables auto-QoS for trusted interfaces. <ul style="list-style-type: none"> • cos: Class of service. • dscp: Differentiated Services Code Point. • <cr>—Trust interface.
Step 4	exit Example: Device(config-if) # exit	Returns to global configuration mode.
Step 5	interface interface-id Example: Device(config) # interface gigabitethernet 0/1	Specifies the switch port identified as connected to a trusted switch or router, and enters interface configuration mode.
Step 6	auto qos trust Example: Device(config-if) # auto qos trust	Enables auto-QoS on the port, and specifies that the port is connected to a trusted router or switch.
Step 7	end Example: Device(config-if) # end	Returns to privileged EXEC mode.
Step 8	show auto qos interface interface-id Example: Device(config) # show auto qos interface gigabitethernet 0/1	Verifies your entries. This command displays the auto-QoS command on the interface on which auto-QoS was enabled. You can use the show running-config privileged EXEC command to display the auto-QoS configuration and the user modifications.

Troubleshooting Auto-QoS

To troubleshoot auto-QoS, use the **debug auto qos** privileged EXEC command. For more information, see the **debug auto qos** command in the command reference for this release.

To disable auto-QoS on a port, use the **no** form of the **auto qos** command interface configuration command, such as **no auto qos voip**. Only the auto-QoS-generated interface configuration commands for this port are removed. If this is the last port on which auto-QoS is enabled and you enter the **no auto qos voip** command, auto-QoS is considered disabled even though the auto-QoS-generated global configuration commands remain (to avoid disrupting traffic on other ports affected by the global configuration).

Monitoring Auto-QoS

Table 2: Commands for Monitoring Auto-QoS

Command	Description
show auto qos [interface [interface-type]]	Displays the initial auto-QoS configuration. You can compare the show auto qos and the show running-config command output to identify the user-defined QoS settings.
show mls qos [interface maps]	Displays information about the QoS configuration that might be affected by auto-QoS.
show mls qos interface [interface-type queueing statistics]	Displays information about the QoS interface configuration that might be affected by auto-QoS.
show mls qos maps [cos-output-q dscp-mutation dscp-output-q]	Displays information about the QoS maps configuration that might be affected by auto-QoS.
show running-config	Displays information about the QoS configuration that might be affected by auto-QoS. You can compare the show auto qos and the show running-config command output to identify the user-defined QoS settings.

Configuration Example for Auto-QoS

The following sections provide configuration examples for Auto-QoS.

Examples: Global Auto-QoS Configuration

The following table describes the automatically generated commands for auto-QoS and enhanced auto-QoS by the switch.

Table 3: Generated Auto-QoS Configuration

Description	Automatically Generated Command {voip}
The switch automatically maps CoS values to an egress queue and to a threshold ID.	<pre> Device(config)# no mls qos srr-queue output cos-map Device(config)# mls qos srr-queue output cos-map queue 1 threshold 1 4 Device(config)# mls qos srr-queue output cos-map queue 2 threshold 1 2 6 7 6 7 Device(config)# mls qos srr-queue output cos-map queue 2 threshold 2 3 4 Device(config)# mls qos srr-queue output cos-map queue 3 threshold 2 0 Device(config)# mls qos srr-queue output cos-map queue 4 threshold 2 1 </pre>
The switch automatically maps DSCP values to an egress queue and to a threshold ID.	<pre> Device(config)# no mls qos srr-queue output dscp-map Device(config)# mls qos srr-queue output dscp-map queue 1 threshold 2 32 33 40 41 42 43 44 45 Device(config)# mls qos srr-queue output dscp-map queue 1 threshold 2 46 47 Device(config)# mls qos srr-queue output dscp-map queue 2 threshold 1 16 17 18 19 20 21 22 23 Device(config)# mls qos srr-queue output dscp-map queue 2 threshold 1 26 27 28 29 30 31 34 35 Device(config)# mls qos srr-queue output dscp-map queue 2 threshold 1 36 37 38 39 Device(config)# mls qos srr-queue output dscp-map queue 2 threshold 2 24 48 49 50 51 52 53 54 Device(config)# mls qos srr-queue output dscp-map queue 2 threshold 2 55 56 57 58 59 60 61 62 Device(config)# mls qos srr-queue output dscp-map queue 2 threshold 2 63 Device(config)# mls qos srr-queue output dscp-map queue 3 threshold 1 0 1 2 3 4 5 6 7 Device(config)# mls qos srr-queue output dscp-map queue 4 threshold 1 8 9 10 11 12 13 14 15 </pre>

Examples: Auto-QoS Generated Configuration For Enhanced Video, Trust, and Classify Devices

If you entered the following enhanced auto-QoS commands, the switch configures a CoS-to-DSCP map (maps CoS values in incoming packets to a DSCP value):

- **auto qos video cts**
- **auto qos video ip-camera**
- **auto qos video media-player**
- **auto qos trust**
- **auto qos trust cos**
- **auto qos trust dscp**

If you entered the **auto qos classify** command, the switch automatically creates class maps and policy maps (as shown below).

```
Device(config)# policy-map AUTOQOS-SRND4-CLASSIFY-POLICY
Device(config-pmap)# class AUTOQOS_MULTITIENHANCED_CONF_CLASS
Device(config-pmap-c)# set dscp af41
Device(config-pmap)# class AUTOQOS_BULK_DATA_CLASS
Device(config-pmap-c)# set dscp af11
Device(config-pmap)# class AUTOQOS_TRANSACTION_CLASS
Device(config-pmap-c)# set dscp af21
Device(config-pmap)# class AUTOQOS_SCAVANGER_CLASS
Device(config-pmap-c)# set dscp cs1
Device(config-pmap)# class AUTOQOS_SIGNALING_CLASS
Device(config-pmap-c)# set dscp cs3
Device(config-pmap)# class AUTOQOS_DEFAULT_CLASS
Device(config-pmap-c)# set dscp default
;
Device(config-if)# service-policy input AUTOQOS-SRND4-CLASSIFY-POLICY
```

If you entered the **auto qos classify police** command, the switch automatically creates class maps and policy maps (as shown below).

```
Device(config)# class-map match-all AUTOQOS_MULTITIENHANCED_CONF_CLASS
Device(config-cmap)# match access-group name AUTOQOS-ACL-MULTITIENHANCED-CONF
Device(config)# class-map match-all AUTOQOS_DEFAULT_CLASS
Device(config-cmap)# match access-group name AUTOQOS-ACL-DEFAULT
Device(config)# class-map match-all AUTOQOS_TRANSACTION_CLASS
Device(config-cmap)# match access-group name AUTOQOS-ACL-TRANSACTIONAL-DATA
Device(config)# class-map match-all AUTOQOS_SIGNALING_CLASS
Device(config-cmap)# match access-group name AUTOQOS-ACL-SIGNALING
Device(config)# class-map match-all AUTOQOS_BULK_DATA_CLASS
Device(config-cmap)# match access-group name AUTOQOS-ACL-BULK-DATA
Device(config)# class-map match-all AUTOQOS_SCAVANGER_CLASS
Device(config-cmap)# match access-group name AUTOQOS-ACL-SCAVANGER
Device(config)# policy-map AUTOQOS-SRND4-CLASSIFY-POLICE-POLICY
Device(config-pmap)# class AUTOQOS_MULTITIENHANCED_CONF_CLASS
Device(config-pmap-c)# set dscp af41
Device(config-pmap)# police 5000000 8000 exceed-action drop
Device(config-pmap)# class AUTOQOS_BULK_DATA_CLASS
Device(config-pmap-c)# set dscp af11
Device(config-pmap)# class AUTOQOS_TRANSACTION_CLASS
```



```

Device(config-pmap-c) # set dscp af21
Device(config-pmap) # class AUTOQOS_SCAVANGER_CLASS
Device(config-pmap-c) # set dscp cs1
Device(config-pmap) # police 10000000 8000 exceed-action drop
Device(config-pmap) # class AUTOQOS_SIGNALING_CLASS
Device(config-pmap-c) # set dscp cs3
Device(config-pmap) # police 32000 8000 exceed-action drop
Device(config-pmap) # class AUTOQOS_DEFAULT_CLASS
Device(config-pmap-c) # set dscp default

```

This is the enhanced configuration for the **auto qos voip cisco-phone** command:

```

Device(config) # class-map match-all AUTOQOS_VOIP_DATA_CLASS
Device(config-cmap) # match ip dscp ef
Device(config) # class-map match-all AUTOQOS_VOIP_VIDEO_CLASS
Device(config-cmap) # match ip dscp af41
Device(config) # class-map match-all AUTOQOS_VOIP_SIGNAL_CLASS
Device(config-cmap) # match ip dscp cs3
Device(config) # class-map match-all AUTOQOS_DEFAULT_CLASS
Device(config-cmap) # match access-group name AUTOQOS-ACL-DEFAULT
Device(config) # policy-map AUTOQOS-SRND4-CISCOPHONE-POLICY
Device(config-pmap) # class AUTOQOS_VOIP_DATA_CLASS
Device(config-pmap-c) # set dscp ef
Device(config-pmap) # class AUTOQOS_VOIP_VIDEO_CLASS
Device(config-pmap-c) # set dscp af41
Device(config-pmap) # class AUTOQOS_VOIP_SIGNAL_CLASS
Device(config-pmap-c) # set dscp cs3
Device(config-pmap) # class AUTOQOS_DEFAULT_CLASS
Device(config-pmap-c) # set dscp default
Device(config-if) # service-policy input AUTOQOS-SRND4-CISCOPHONE-POLICY

```

This is the enhanced configuration for the **auto qos voip cisco-softphone** command:

```

Device(config) # class-map match-all AUTOQOS_VOIP_DATA_CLASS
Device(config-cmap) # match ip dscp ef
Device(config) # class-map match-all AUTOQOS_MULTIHANCED_CONF_CLASS
Device(config-cmap) # match access-group name AUTOQOS-ACL-MULTIHANCED-CONF
Device(config) # class-map match-all AUTOQOS_BULK_DATA_CLASS
Device(config-cmap) # match access-group name AUTOQOS-ACL-BULK-DATA
Device(config) # class-map match-all AUTOQOS_TRANSACTION_CLASS
Device(config-cmap) # match access-group name AUTOQOS-ACL-TRANSACTIONAL-DATA
Device(config) # class-map match-all AUTOQOS_SCAVANGER_CLASS
Device(config-cmap) # match access-group name AUTOQOS-ACL-SCAVANGER
Device(config) # class-map match-all AUTOQOS_SIGNALING_CLASS
Device(config-cmap) # match access-group name AUTOQOS-ACL-SIGNALING

Device(config) # policy-map AUTOQOS-SRND4-SOFTPHONE-POLICY
Device(config-pmap) # class AUTOQOS_VOIP_DATA_CLASS
Device(config-pmap-c) # set dscp ef
Device(config-pmap) # class AUTOQOS_MULTIHANCED_CONF_CLASS
Device(config-pmap-c) # set dscp af41
Device(config-pmap) # police 5000000 8000 exceed-action drop
Device(config-pmap) # class AUTOQOS_BULK_DATA_CLASS
Device(config-pmap-c) # set dscp af11
Device(config-pmap) # class AUTOQOS_TRANSACTION_CLASS
Device(config-pmap-c) # set dscp af21
Device(config-pmap) # class AUTOQOS_SCAVANGER_CLASS
Device(config-pmap-c) # set dscp cs1
Device(config-pmap) # police 10000000 8000 exceed-action drop
Device(config-pmap) # class AUTOQOS_SIGNALING_CLASS
Device(config-pmap-c) # set dscp cs3

```

```
Device(config-pmap)# police 32000 8000 exceed-action drop
Device(config-pmap)# class AUTOQOS_DEFAULT_CLASS
Device(config-pmap-c)# set dscp default
;
Device(config-if)# service-policy input AUTOQOS-SRND4-SOFTPHONE-POLICY
```

Additional References for Auto-QoS

Related Documents

Related Topic	Document Title
For complete syntax and usage information for the commands used in this chapter.	<i>Cisco IOS Quality of Service Solutions Command Reference</i>

Feature History and Information for Auto-QoS

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use the Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 4: Feature Information for Configuring Auto-QoS

Feature Name	Releases	Feature Information
Auto-QoS	Cisco IOS Release 15.2(5)E	This feature was introduced.



CHAPTER 2

Configuring QoS

- [Prerequisites for QoS, on page 13](#)
- [Restrictions for QoS, on page 14](#)
- [Information About QoS, on page 15](#)
- [How to Configure QoS, on page 29](#)
- [Configuration Examples for QoS, on page 58](#)
- [Feature Information for QoS, on page 63](#)

Prerequisites for QoS

Before configuring standard QoS, you must have a thorough understanding of these items:

- The types of applications used and the traffic patterns on your network.
- Traffic characteristics and needs of your network. For example, is the traffic on your network bursty? Do you need to reserve bandwidth for voice and video streams?
- Bandwidth requirements and speed of the network.
- Location of congestion points in the network.

QoS ACL Guidelines

Follow these guidelines when configuring QoS with access control lists (ACLs):

- It is not possible to match IP fragments against configured IP extended ACLs to enforce QoS. IP fragments are sent as best-effort. IP fragments are denoted by fields in the IP header.
- Only one ACL per class map and only one **match** class-map configuration command per class map are supported. The ACL can have multiple ACEs, which match fields against the contents of the packet.

Policing Guidelines

- Only one policer is applied to a packet on an ingress port. Only the average rate and committed burst parameters are configurable.

- On a port configured for QoS, all traffic received through the port is classified, policed, and marked according to the policy map attached to the port. On a trunk port configured for QoS, traffic in all VLANs received through the port is classified, policed, and marked according to the policy map attached to the port.
- If you have EtherChannel ports configured on your switch, you must configure QoS classification, policing, mapping, and queueing on the individual physical ports that comprise the EtherChannel. You must decide whether the QoS configuration should match on all ports in the EtherChannel.
- If you need to modify a policy map of an existing QoS policy, first remove the policy map from all interfaces, and then modify or copy the policy map. After you finish the modification, apply the modified policy map to the interfaces. If you do not first remove the policy map from all interfaces, high CPU usage can occur, which, in turn, can cause the console to pause for a very long time.

General QoS Guidelines

These are the general QoS guidelines:

- You configure QoS only on physical ports; there is no support for it at the VLAN level and EtherChannel ports.
- Control traffic (such as spanning-tree bridge protocol data units [BPDUs] and routing update packets) received by the switch are subject to all ingress QoS processing.
- You are likely to lose data when you change queue settings; therefore, try to make changes when traffic is at a minimum.

Restrictions for QoS

The following are the restrictions for QoS:

- Ingress queueing and aggregate policy are not supported.
- Only 33 class-maps are supported per ASIC.
- Ternary content-addressable memory (TCAM) sharing of policy-map (policer/marking) across ports is not supported. Because of this, the number of interfaces on which auto-QoS/QoS policy-map can be applied is limited.
- The same TCAM region must be used for both security access control lists (ACLs) and ACLs used via policy map.
- Policy-maps with the **match ip dscp** command matches both IPv4 and IPv6 addresses, which limits the scale number to 16 class-maps. One TCAM entry is created for IPv4 and one TCAM entry for IPv6.
- Per ASIC, 8 TCP port comparators and 8 UDP port comparators are supported, and each gt (greater than)/lt (less than)/neq (not equal) operator uses 1 port comparator, and each range operator uses 2 port comparators. A policy-map with this combination affects the TCAM scale and number of interfaces to which the policy-map can be attached.
- The following restrictions apply to IPv4 ACL network interfaces:
 - When controlling access to an interface, you can use a named or numbered ACL.

- If you apply an ACL to a Layer 3 interface, and routing is not enabled on the switch, the ACL only filters packets that are intended for the CPU, such as SNMP, Telnet, or web traffic.
- You do not have to enable routing to apply ACLs on Layer 2 interfaces.
- Deny ACLs are not supported on QoS policy-maps.
- Policed action transmit is not supported; only exceed action drop is supported.
- You can configure QoS only on physical ports. VLAN-based QoS is not supported. You configure the QoS settings, such as classification, queueing, and scheduling, and apply the policy map to a port. When configuring QoS on a physical port, you apply a nonhierarchical policy map to a port.

Information About QoS

QoS Implementation

Typically, networks operate on a best-effort delivery basis, which means that all traffic has equal priority and an equal chance of being delivered in a timely manner. When congestion occurs, all traffic has an equal chance of being dropped.

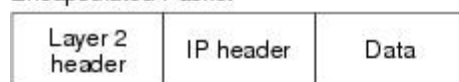
When you configure the QoS feature, you can select specific network traffic, prioritize it according to its relative importance, and use congestion-management and congestion-avoidance techniques to provide preferential treatment. Implementing QoS in your network makes network performance more predictable and bandwidth utilization more effective.

The QoS implementation is based on the Differentiated Services (Diff-Serv) architecture, a standard from the Internet Engineering Task Force (IETF). This architecture specifies that each packet is classified upon entry into the network.

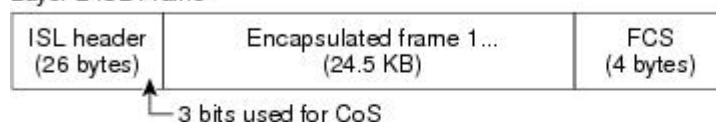
Figure 1: QoS Classification Layers in Frames and Packets

The special bits in the Layer 2 frame or a Layer 3 packet are shown in the following figure:

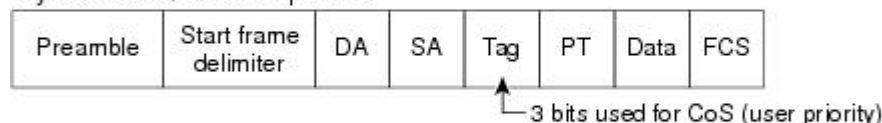
Encapsulated Packet



Layer 2 ISL Frame



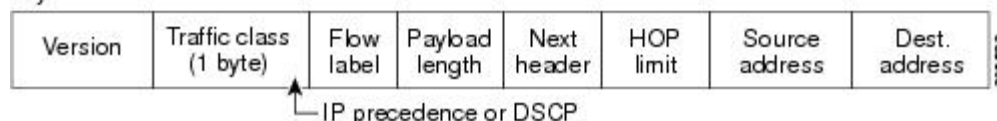
Layer 2 802.1Q and 802.1p Frame



Layer 3 IPv4 Packet



Layer 3 IPv6 Packet



Layer 2 Frame Prioritization Bits

Layer 2 Inter-Switch Link (ISL) frame headers have a 1-byte User field that carries an IEEE 802.1p class of service (CoS) value in the three least-significant bits. On ports configured as Layer 2 ISL trunks, all traffic is in ISL frames.

Layer 2 802.1Q frame headers have a 2-byte Tag Control Information field that carries the CoS value in the three most-significant bits, which are called the User Priority bits. On ports configured as Layer 2 802.1Q trunks, all traffic is in 802.1Q frames except for traffic in the native VLAN.

Other frame types cannot carry Layer 2 CoS values.

Layer 2 CoS values range from 0 for low priority to 7 for high priority.

Layer 3 Packet Prioritization Bits

Layer 3 IP packets can carry ranging from 0 to 63.

End-to-End QoS Solution Using Classification

All switches and routers that access the Internet rely on the class information to provide the same forwarding treatment to packets with the same class information and different treatment to packets with different class

information. The class information in the packet can be assigned by end hosts or by switches or routers along the way, based on a configured policy, detailed examination of the packet, or both. Detailed examination of the packet is expected to occur closer to the edge of the network, so that the core switches and routers are not overloaded with this task.

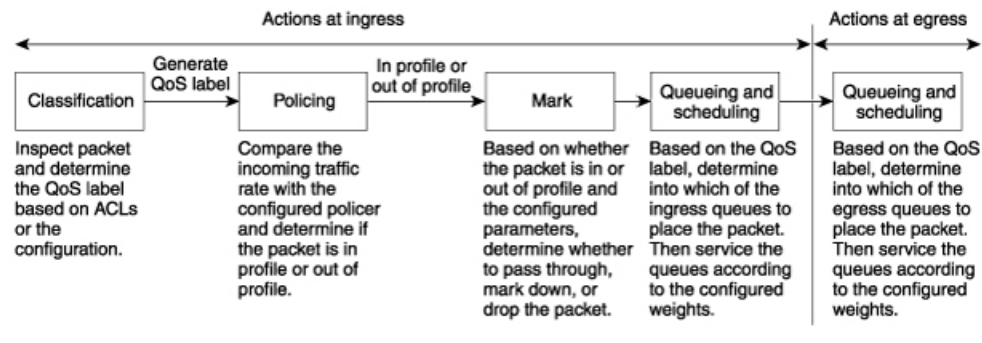
Switches and routers along the path can use the class information to limit the amount of resources allocated per traffic class. The behavior of an individual device when handling traffic in the Diff-Serv architecture is called per-hop behavior. If all devices along a path provide a consistent per-hop behavior, you can construct an end-to-end QoS solution.

Implementing QoS in your network can be a simple task or complex task and depends on the QoS features offered by your internetworking devices, the traffic types and patterns in your network, and the granularity of control that you need over incoming and outgoing traffic.

QoS Basic Model

To implement QoS, the switch must distinguish packets or flows from one another (classify), assign a label to indicate the given quality of service as the packets move through the switch, make the packets comply with the configured resource usage limits (police and mark), and provide different treatment (queue and schedule) in all situations where resource contention exists. The switch also needs to ensure that traffic sent from it meets a specific traffic profile (shape).

Figure 2: QoS Basic Wired Model



Actions at Ingress Port

Actions at the ingress port include classifying traffic, policing, and marking:

- Classifying a distinct path for a packet by associating it with a QoS label. The switch maps the CoS or DSCP in the packet to a QoS label to distinguish one kind of traffic from another. The QoS label that is generated identifies all future QoS actions to be performed on this packet.
- Policing determines whether a packet is in or out of profile by comparing the rate of the incoming traffic to the configured policer. The policer limits the bandwidth consumed by a flow of traffic. The result is passed to the marker.
- Marking evaluates the policer and configuration information for the action to be taken when a packet is out of profile and determines what to do with the packet (pass through a packet without modification, marking down the QoS label in the packet, or dropping the packet).



Note Queuing and scheduling are only supported at egress and not at ingress on the switch.

Actions at Egress Port

Actions at the egress port include queuing and scheduling:

- Queuing evaluates the QoS packet label and the corresponding CoS value before selecting which of the four egress queues to use. Because congestion can occur when multiple ingress ports simultaneously send data to an egress port, WTD differentiates traffic classes and subjects the packets to different thresholds based on the QoS label. If the threshold is exceeded, the packet is dropped.
- Scheduling services the four egress queues based on their configured SRR shared or shaped weights. One of the queues (queue 1) can be the priority queue, which is serviced until empty before the other queues are serviced.

Classification Overview

Classification is the process of distinguishing one kind of traffic from another by examining the fields in the packet. Classification is enabled only if QoS is globally enabled on the switch. By default, QoS is globally disabled, so no classification occurs.

During classification, the switch performs a lookup and assigns a QoS label to the packet. The QoS label identifies all QoS actions to be performed on the packet and from which queue the packet is sent.

The QoS label is based on the DSCP or the CoS value in the packet and decides the queuing and scheduling actions to perform on the packet. The label is mapped according to the trust setting and the packet type as shown in the Classification Flowchart.

You specify which fields in the frame or packet that you want to use to classify incoming traffic.

Non-IP Traffic Classification

The following table describes the non-IP traffic classification options for your QoS configuration.

Table 5: Non-IP Traffic Classifications

Non-IP Traffic Classification	Description
Trust the CoS value	<p>Trust the CoS value in the incoming frame (configure the port to trust CoS), and then use the configurable CoS-to-DSCP map to generate a DSCP value for the packet.</p> <p>Layer 2 ISL frame headers carry the CoS value in the 3 least-significant bits of the 1-byte User field.</p> <p>Layer 2 802.1Q frame headers carry the CoS value in the 3 most-significant bits of the Tag Control Information field. CoS values range from 0 for low priority to 7 for high priority.</p>

Non-IP Traffic Classification	Description
Trust the DSCP value	Trust the DSCP value in the incoming frame. These configurations are meaningless for non-IP traffic. If you configure a port with either of these options and non-IP traffic is received, the switch assigns a CoS value and generates an internal DSCP value from the CoS-to-DSCP map. The switch uses the internal DSCP value to generate a CoS value representing the priority of the traffic.
Perform classification based on configured Layer 2 MAC ACL	Perform the classification based on a configured Layer 2 MAC access control list (ACL), which can examine the MAC source address, the MAC destination address, and other fields. If no ACL is configured, the packet is assigned 0 as the DSCP and CoS values, which means best-effort traffic. Otherwise, the policy-map action specifies a DSCP or CoS value to assign to the incoming frame.

After classification, the packet is sent to the policing and marking stages.

IP Traffic Classification

The following table describes the IP traffic classification options for your QoS configuration.

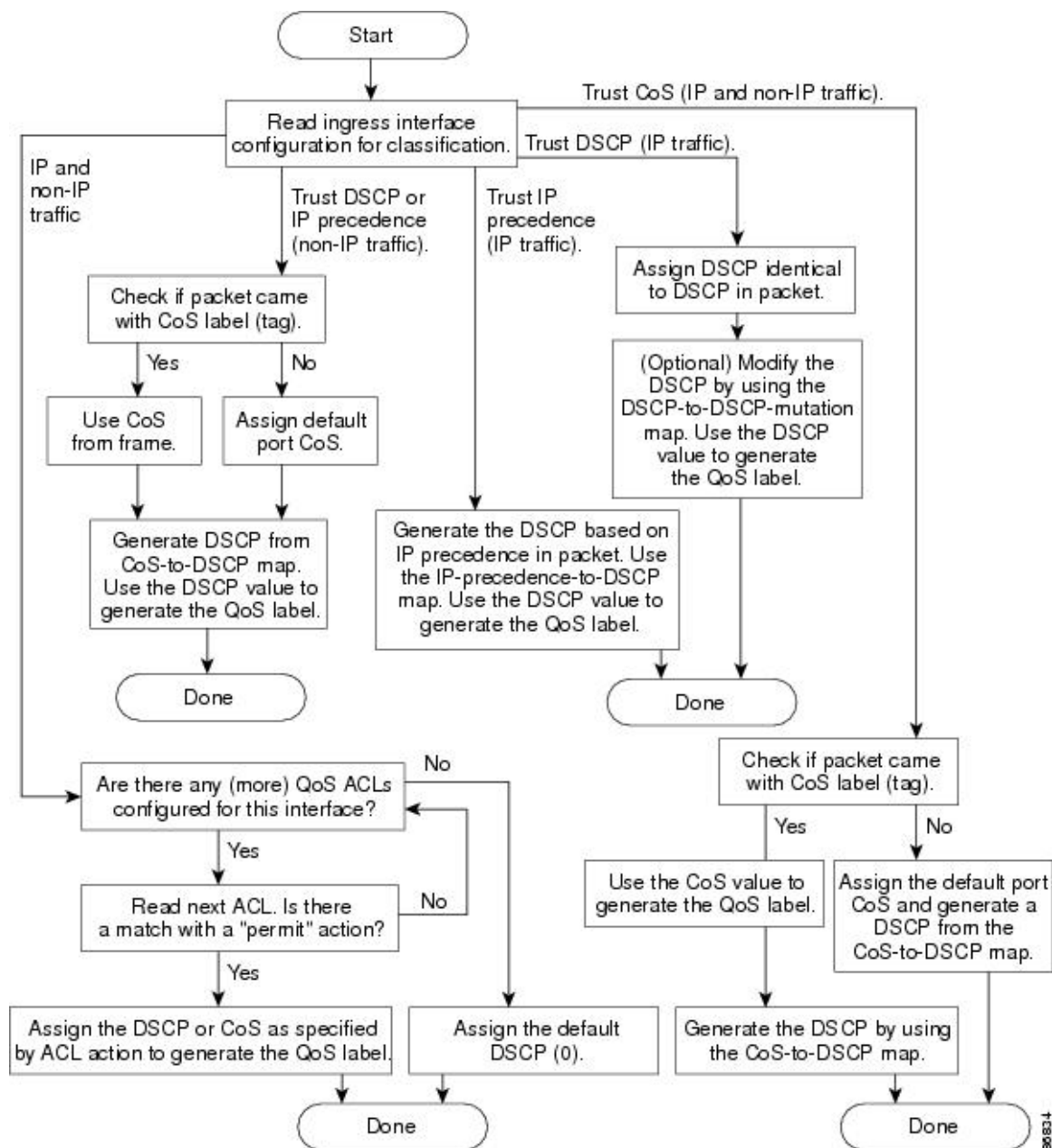
Table 6: IP Traffic Classifications

IP Traffic Classification	Description
Trust the DSCP value	Trust the DSCP value in the incoming packet (configure the port to trust DSCP), and assign the same DSCP value to the packet. The IETF defines the 6 most-significant bits of the 1-byte ToS field as the DSCP. The priority represented by a particular DSCP value is configurable. DSCP values range from 0 to 63. You can also classify IP traffic based on IPv6 DSCP. For ports that are on the boundary between two QoS administrative domains, you can modify the DSCP to another value by using the configurable DSCP-to-DSCP-mutation map.
Trust the CoS value	Trust the CoS value (if present) in the incoming packet, and generate a DSCP value for the packet by using the CoS-to-DSCP map. If the CoS value is not present, use the default port CoS value.
IP standard or an extended ACL	Perform the classification based on a configured IP standard or an extended ACL, which examines various fields in the IP header. If no ACL is configured, the packet is assigned 0 as the DSCP and CoS values, which means best-effort traffic. Otherwise, the policy-map action specifies a DSCP or CoS value to assign to the incoming frame.
Override configured CoS	Override the configured CoS of incoming packets, and apply the default port CoS value to them. For IPv6 packets, the DSCP value is rewritten by using the CoS-to-DSCP map and by using the default CoS of the port. You can do this for both IPv4 and IPv6 traffic.

After classification, the packet is sent to the policing and marking stages.

Classification Flowchart

Figure 3: Classification Flowchart



Access Control Lists

You can use IP standard, IP extended, or Layer 2 MAC ACLs to define a group of packets with the same characteristics (class). You can also classify IP traffic based on IPv6 ACLs.

In the QoS context, the permit and deny actions in the access control entries (ACEs) have different meanings from security ACLs:

- If a match with a permit action is encountered (first-match principle), the specified QoS-related action is taken.
- If a match with a deny action is encountered, the ACL being processed is skipped, and the next ACL is processed.



Note Deny action is supported in Cisco IOS Release 3.7.4E and later releases.

- If no match with a permit action is encountered and all the ACEs have been examined, no QoS processing occurs on the packet, and the device offers best-effort service to the packet.
- If multiple ACLs are configured on a port, the lookup stops after the packet matches the first ACL with a permit action, and QoS processing begins.



Note When creating an access list, note that by default the end of the access list contains an implicit deny statement for everything if it did not find a match before reaching the end.

After a traffic class has been defined with the ACL, you can attach a policy to it. A policy might contain multiple classes with actions specified for each one of them. A policy might include commands to classify the class as a particular aggregate (for example, assign a DSCP) or rate-limit the class. This policy is then attached to a particular port on which it becomes effective.

You implement IP ACLs to classify IP traffic by using the **access-list** global configuration command; you implement Layer 2 MAC ACLs to classify non-IP traffic by using the **mac access-list extended** global configuration command.

Classification Based on Class Maps and Policy Maps

A class map is a mechanism that you use to name a specific traffic flow (or class) and to isolate it from all other traffic. The class map defines the criteria used to match against a specific traffic flow to further classify it. The criteria can include matching the access group defined by the ACL or matching a specific list of DSCP values. If you have more than one type of traffic that you want to classify, you can create another class map and use a different name. After a packet is matched against the class-map criteria, you further classify it through the use of a policy map.

A policy map specifies which traffic class to act on. Actions can include trusting the CoS or DSCP values in the traffic class; setting a specific DSCP value in the traffic class; or specifying the traffic bandwidth limitations and the action to take when the traffic is out of profile. Before a policy map can be effective, you must attach it to a port.

You create a class map by using the **class-map** global configuration command or the **class** policy-map configuration command. You should use the **class-map** command when the map is shared among many ports. When you enter the **class-map** command, the switch enters the class-map configuration mode. In this mode, you define the match criterion for the traffic by using the **match** class-map configuration command.

You can configure a default class by using the **class class-default** policy-map configuration command. Unclassified traffic (traffic specified in the other traffic classes configured on the policy-map) is treated as default traffic.

You create and name a policy map by using the **policy-map** global configuration command. When you enter this command, the switch enters the policy-map configuration mode. In this mode, you specify the actions to take on a specific traffic class by using the **class** or **set** policy-map configuration and policy-map class configuration commands.

The policy map can contain the **police** policy-map class configuration commands, which define the policer, the bandwidth limitations of the traffic, and the action to take if the limits are exceeded.

To enable the policy map, you attach it to a port by using the **service-policy** interface configuration command.

Policing and Marking Overview

After a packet is classified and has a DSCP-based or CoS-based QoS label assigned to it, the policing and marking process can begin.

Policing involves creating a policer that specifies the bandwidth limits for the traffic. Packets that exceed the limits are *out of profile* or *nonconforming*. Each policer decides on a packet-by-packet basis whether the packet is in or out of profile and specifies the actions on the packet. These actions, carried out by the marker, include passing through the packet without modification, dropping the packet, or modifying (marking down) the assigned DSCP of the packet and allowing the packet to pass through. The configurable policed-DSCP map provides the packet with a new DSCP-based QoS label. Marked-down packets use the same queues as the original QoS label to prevent packets in a flow from getting out of order.



Note

All traffic, regardless of whether it is bridged or routed, is subjected to a policer, if one is configured. As a result, bridged packets might be dropped or might have their DSCP or CoS fields modified when they are policed and marked.

You can configure policing on a physical port. After you configure the policy map and policing actions, attach the policy to a port by using the **service-policy** interface configuration command.

Physical Port Policing

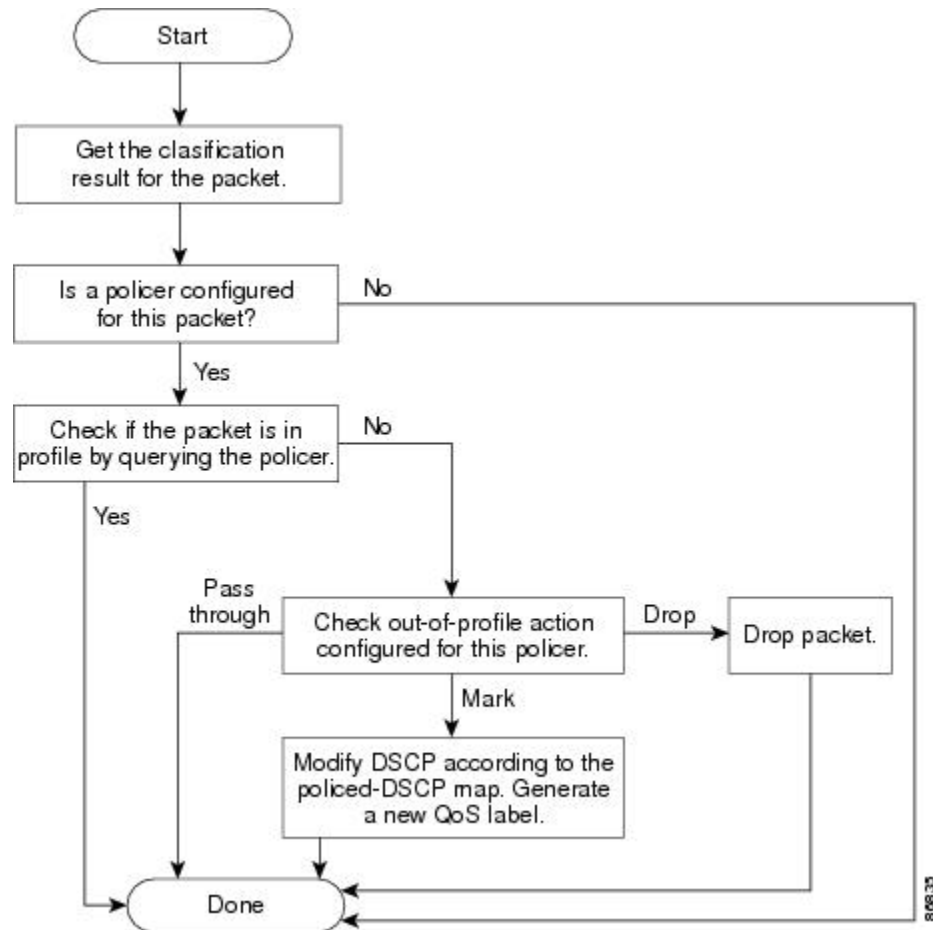
In policy maps on physical ports, you can create individual policers. QoS applies the bandwidth limits specified in the policer separately to each matched traffic class. You configure this type of policer within a policy map by using the **police** policy-map class configuration command.

Policing uses a token-bucket algorithm. As each frame is received by the switch, a token is added to the bucket. The bucket has a hole in it and leaks at a rate that you specify as the average traffic rate in bits per second. Each time a token is added to the bucket, the switch verifies that there is enough room in the bucket. If there is not enough room, the packet is marked as nonconforming, and the specified policer action is taken (dropped or marked down).

How quickly the bucket fills is a function of the bucket depth (burst-byte), the rate at which the tokens are removed (rate-bps), and the duration of the burst above the average rate. The size of the bucket imposes an upper limit on the burst length and limits the number of frames that can be transmitted back-to-back. If the burst is short, the bucket does not overflow, and no action is taken against the traffic flow. However, if a burst is long and at a higher rate, the bucket overflows, and the policing actions are taken against the frames in that burst.

You configure the bucket depth (the maximum burst that is tolerated before the bucket overflows) by using the `burst-byte` option of the **police** policy-map class configuration command. You configure how fast (the average rate) that the tokens are removed from the bucket by using the `rate-bps` option of the **police** policy-map class configuration command.

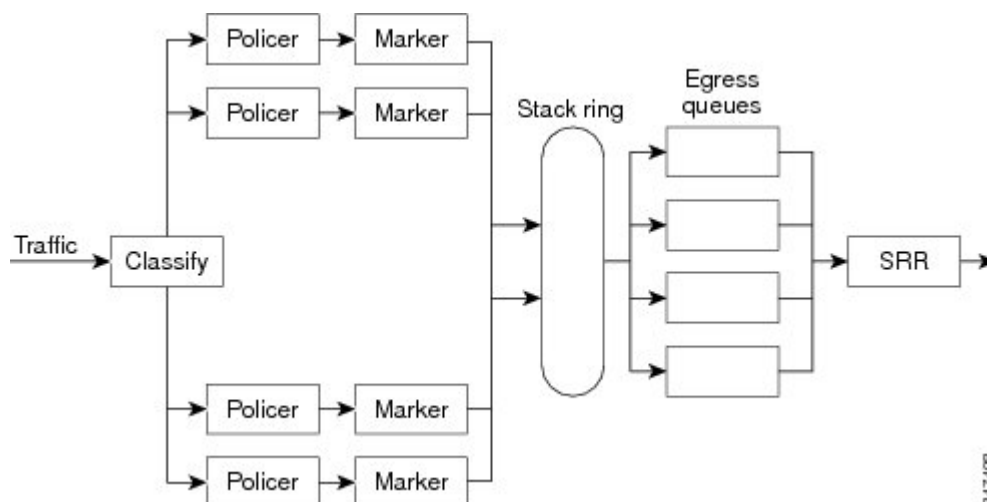
Figure 4: Policing and Marking Flowchart on Physical Ports



Queueing and Scheduling Overview

The switch has queues at specific points to help prevent congestion.

Figure 5: Egress Queue Location on Switch



Note The switch supports 4 egress queues by default and there is an option to enable a total of 8 egress queues. The 8 egress queue configuration is only supported on a standalone switch.

The Catalyst 2960-L switches support Scheduled Round Robin (SRR). They do not support Weighted Round Robin (WRR). Currently, you can configure SRR with **wrr** commands instead of **srr** commands. From Cisco IOS Release 15.2(5)E2 and later, the **wrr** commands will be replaced with the **srr** commands on the switch.

Weighted Tail Drop

Egress queues use an enhanced version of the tail-drop congestion-avoidance mechanism called weighted tail drop (WTD). WTD is implemented on queues to manage the queue lengths and to provide drop precedences for different traffic classifications.

As a frame is enqueued to a particular queue, WTD uses the frame's assigned QoS label to subject it to different thresholds. If the threshold is exceeded for that QoS label (the space available in the destination queue is less than the size of the frame), the switch drops the frame.

Each queue has three threshold values. The QoS label determines which of the three threshold values is subjected to the frame. Of the three thresholds, two are configurable (explicit) and one is not (implicit).

Figure 6: WTD and Queue Operation

The following figure shows an example of WTD operating on a queue whose size is 1000 frames. Three drop percentages are configured: 40 percent (400 frames), 60 percent (600 frames), and 100 percent (1000 frames). These percentages indicate that up to 400 frames can be queued at the 40-percent threshold, up to 600 frames at the 60-percent threshold, and up to 1000 frames at the 100-percent threshold.



In the example, CoS values 6 and 7 have a greater importance than the other CoS values, and they are assigned to the 100-percent drop threshold (queue-full state). CoS values 4 and 5 are assigned to the 60-percent threshold, and CoS values 0 to 3 are assigned to the 40-percent threshold.

Suppose the queue is already filled with 600 frames, and a new frame arrives. It contains CoS values 4 and 5 and is subjected to the 60-percent threshold. If this frame is added to the queue, the threshold will be exceeded, so the switch drops it.

SRR Shaping and Sharing

You can configure SRR on egress queues for sharing or for shaping.

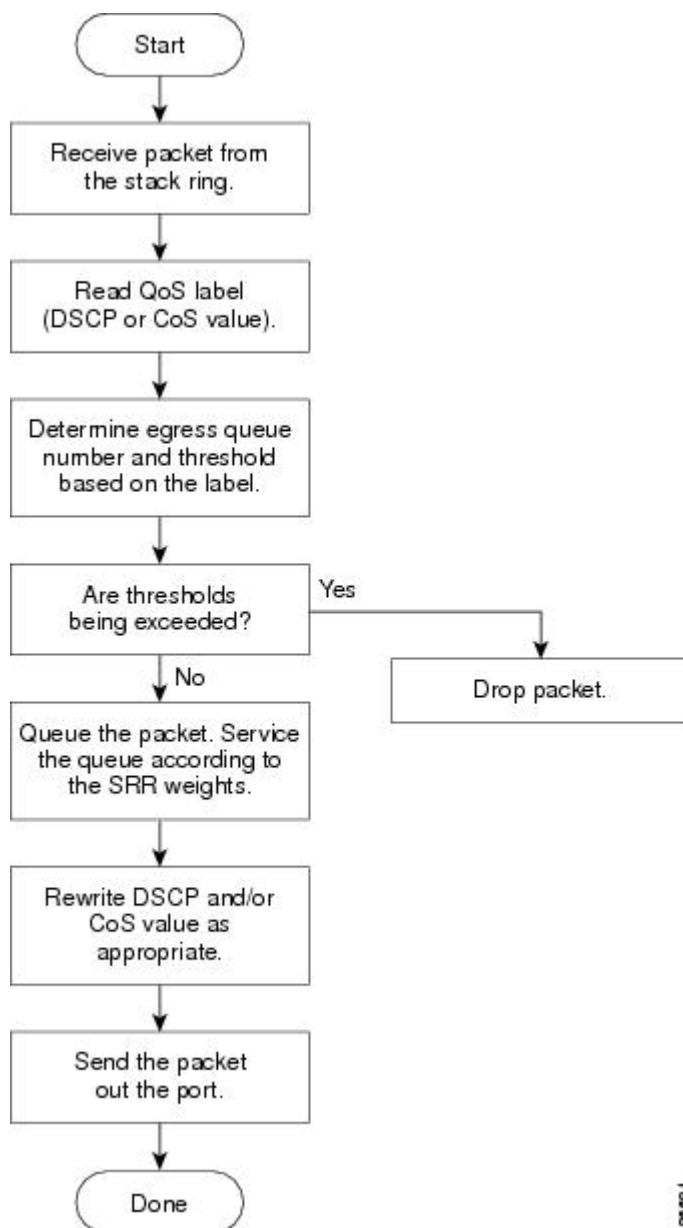
In shaped mode, the egress queues are guaranteed a percentage of the bandwidth, and they are rate-limited to that amount. Shaped traffic does not use more than the allocated bandwidth even if the link is idle. Shaping provides a more even flow of traffic over time and reduces the peaks and valleys of bursty traffic. With shaping, the absolute value of each weight is used to compute the bandwidth available for the queues.

In shared mode, the queues share the bandwidth among them according to the configured weights. The bandwidth is guaranteed at this level but not limited to it. For example, if a queue is empty and no longer requires a share of the link, the remaining queues can expand into the unused bandwidth and share it among them. With sharing, the ratio of the weights controls the frequency of dequeuing; the absolute values are meaningless. Shaping and sharing is configured per interface. Each interface can be uniquely configured.

Queueing and Scheduling on Egress Queues

The following figure shows queueing and scheduling flowcharts for egress ports on the switch.

Figure 7: Queueing and Scheduling Flowchart for Egress Ports on the Switch

**Note**

If the expedite queue is enabled, SRR services it until it is empty before servicing the other three queues.

Egress Expedite Queue

Each port supports four egress queues, one of which (queue 1) can be the egress expedite queue. These queues are assigned to a queue-set. All traffic exiting the switch flows through one of these four queues and is subjected to a threshold based on the QoS label assigned to the packet.



Note If the expedite queue is enabled, SRR services it until it is empty before servicing the other three queues.

Queues and WTD Thresholds

You can assign each packet that flows through the switch to a queue and to a threshold.

Specifically, you map DSCP or CoS values to an egress queue and map DSCP or CoS values to a threshold ID. You use the **mls qos srr-queue output dscp-map queue** *queue-id* {*dscp1...dscp8*} **threshold** *threshold-id* {*dscp1...dscp8*} or the **mls qos srr-queue output cos-map queue** *queue-id* {*cos1...cos8*} **threshold** *threshold-id* {*cos1...cos8*} global configuration command. You can display the DSCP output queue threshold map and the CoS output queue threshold map by using the **show mls qos maps** privileged EXEC command.

The queues use WTD to support distinct drop percentages for different traffic classes. Each queue has three drop thresholds: two configurable (*explicit*) WTD thresholds and one nonconfigurable (*implicit*) threshold preset to the queue-full state. You assign the two WTD threshold percentages for threshold ID 1 and ID 2. The drop threshold for threshold ID 3 is preset to the queue-full state, and you cannot modify it.

Shaped or Shared Mode

You assign shared or shaped weights to the port by using the **srr-queue bandwidth share** *weight1 weight2 weight3 weight4* or the **srr-queue bandwidth shape** *weight1 weight2 weight3 weight4* interface configuration command.

The buffer allocation together with the SRR weight ratios control how much data can be buffered and sent before packets are dropped. The weight ratio is the ratio of the frequency in which the SRR scheduler sends packets from each queue.

All four queues participate in the SRR unless the expedite queue is enabled, in which case the first bandwidth weight is ignored and is not used in the ratio calculation. The expedite queue is a priority queue, and it is serviced until empty before the other queues are serviced. You enable the expedite queue by using the **priority-queue out** interface configuration command.



Note The egress queue default settings are suitable for most situations. You should change them only when you have a thorough understanding of the egress queues and if these settings do not meet your QoS solution.

Packet Modification

A packet is classified, policed, and queued to provide QoS. The following packet modifications can occur during the process to provide QoS:

- For IP and non-IP packets, classification involves assigning a QoS label to a packet based on the DSCP or CoS of the received packet. However, the packet is not modified at this stage; only an indication of the assigned DSCP or CoS value is carried along.
- During policing, IP and non-IP packets can have another DSCP assigned to them (if they are out of profile and the policer specifies a markdown DSCP). Once again, the DSCP in the packet is not modified, but an indication of the marked-down value is carried along. For IP packets, the packet modification occurs at a later stage; for non-IP packets the DSCP is converted to CoS and used for queueing and scheduling decisions.

- Depending on the QoS label assigned to a frame and the mutation chosen, the DSCP and CoS values of the frame are rewritten. If you do not configure a table map and if you configure the port to trust the DSCP of the incoming frame, the DSCP value in the frame is not changed, but the CoS is rewritten according to the DSCP-to-CoS map. If you configure the port to trust the CoS of the incoming frame and it is an IP packet, the CoS value in the frame is not changed, but the DSCP might be changed according to the CoS-to-DSCP map.

The input mutation causes the DSCP to be rewritten depending on the new value of DSCP chosen. The set action in a policy map also causes the DSCP to be rewritten.

Standard QoS Default Configuration

QoS is disabled by default.

When QoS is disabled, there is no concept of trusted or untrusted ports because the packets are not modified. The CoS or DSCP values in the packet are not changed.

Traffic is switched in pass-through mode. The packets are switched without any rewrites and classified as best effort without any policing.

When QoS is enabled using the **mls qos** global configuration command and all other QoS settings are at their defaults, traffic is classified as best effort (the DSCP and CoS value is set to 0) without any policing. No policy maps are configured. The default port trust state on all ports is untrusted.

Default Egress Queue Configuration

The following tables describe the default egress queue configurations.

The following table shows the default egress queue configuration for each queue-set when QoS is enabled. All ports are mapped to queue-set 1. The port bandwidth limit is set to 100 percent and rate unlimited. Note that for the SRR shaped weights (absolute) feature, a shaped weight of zero indicates that the queue is operating in shared mode. Note that for the SRR shared weights feature, one quarter of the bandwidth is allocated to each queue.

Table 7: Default Egress Queue Configuration

Feature	Queue 1	Queue 2	Queue 3	Queue 4
Buffer allocation	25 percent	25 percent	25 percent	25 percent
WTD drop threshold 1	80 percent	80 percent	80 percent	80 percent
WTD drop threshold 2	80 percent	80 percent	80 percent	80 percent
Reserved threshold	1000 percent	1000 percent	1000 percent	1000 percent
Maximum threshold	400 percent	400 percent	400 percent	400 percent
SRR shaped weights (absolute)	25	0	0	0
SRR shared weights	25	25	25	25

The following table shows the default CoS output queue threshold map when QoS is enabled.

Table 8: Default CoS Output Queue Threshold Map

CoS Value	Queue ID–Threshold ID
0, 1	2–1
2, 3	3–1
4	4–1
5	1–1
6, 7	4–1

Default Mapping Table Configuration

The default DSCP-to-DSCP-mutation map is a null map, which maps an incoming DSCP value to the same DSCP value.

The default policed-DSCP map is a null map, which maps an incoming DSCP value to the same DSCP value (no markdown).

How to Configure QoS

The following sections provide information about how to configure QoS.

Enabling QoS Globally

By default, QoS is disabled on the switch.

The following procedure to enable QoS globally is required.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 2	mls qos Example: Device(config)# mls qos	Enables QoS globally. QoS operates with the default settings described in the related topic sections below. Note To disable QoS, use the no mls qos global configuration command.

	Command or Action	Purpose
Step 3	end Example: Device (config)# end	Returns to privileged EXEC mode.
Step 4	show mls qos Example: Device# show mls qos	Verifies the QoS configuration.
Step 5	copy running-config startup-config Example: Device# copy running-config startup-config	(Optional) Saves your entries in the configuration file.

Configuring Classification Using Port Trust States

These sections describe how to classify incoming traffic by using port trust states.



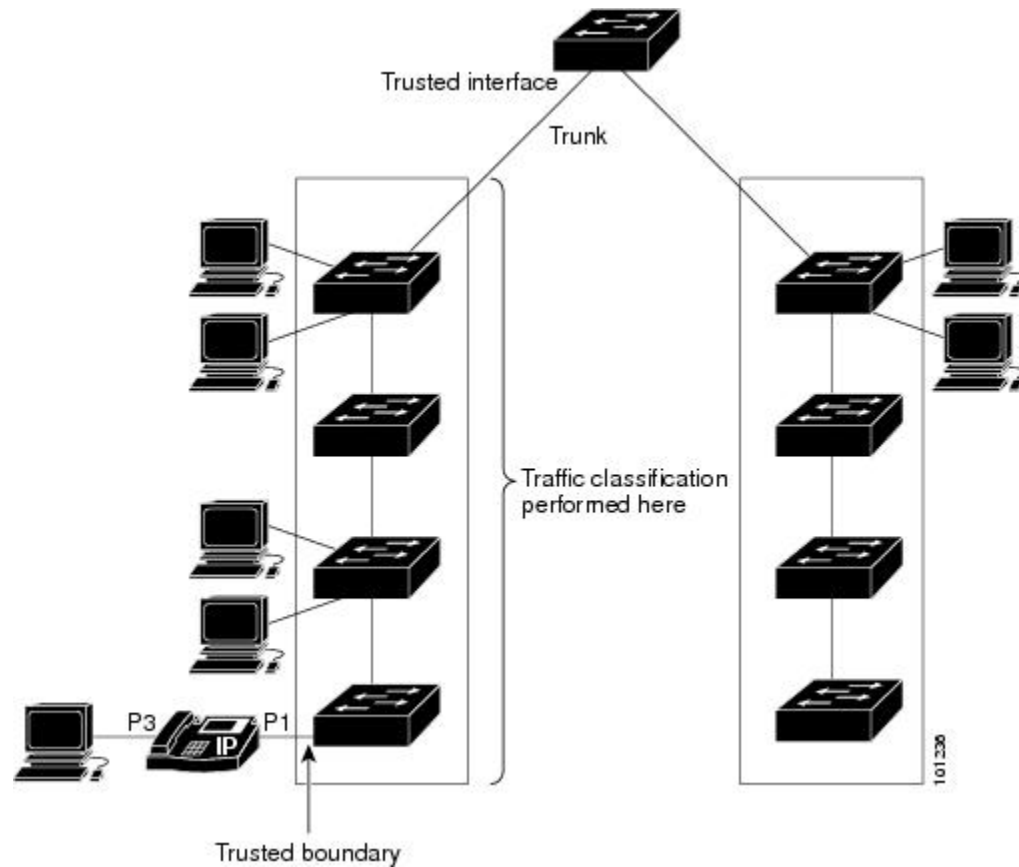
Note

Depending on your network configuration, you must perform one or more of these tasks in this module or one or more of the tasks in the [Configuring a QoS Policy, on page 38](#).

Configuring the Trust State on Ports Within the QoS Domain

Packets entering a QoS domain are classified at the edge of the QoS domain. When the packets are classified at the edge, the switch port within the QoS domain can be configured to one of the trusted states because there is no need to classify the packets at every switch within the QoS domain.

Figure 8: Port Trusted States on Ports Within the QoS Domain



Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: Device# <code>configure terminal</code>	Enters global configuration mode.
Step 2	interface interface-id Example: Device (config)# <code>interface gigabitethernet 0/1</code>	Specifies the port to be trusted, and enters interface configuration mode. Valid interfaces are physical ports.
Step 3	mls qos trust [cos dscp] Example: Device (config-if)# <code>mls qos trust cos</code>	Configures the port trust state. By default, the port is not trusted. If no keyword is specified, the default is dscp . The keywords have these meanings:

	Command or Action	Purpose
		<ul style="list-style-type: none"> • cos—Classifies an ingress packet by using the packet CoS value. For an untagged packet, the port default CoS value is used. The default port CoS value is 0. • dscp—Classifies an ingress packet by using the packet DSCP value. For a non-IP packet, the packet CoS value is used if the packet is tagged; for an untagged packet, the default port CoS is used. Internally, the switch maps the CoS value to a DSCP value by using the CoS-to-DSCP map. <p>To return a port to its untrusted state, use the no mls qos trust interface configuration command.</p>
Step 4	end Example: <pre>Device(config-if) # end</pre>	Returns to privileged EXEC mode.
Step 5	show mls qos interface Example: <pre>Device# show mls qos interface</pre>	Verifies your entries.

Configuring the CoS Value for an Interface

QoS assigns the CoS value specified with the **mls qos cos** interface configuration command to untagged frames received on trusted and untrusted ports.

Beginning in privileged EXEC mode, follow these steps to define the default CoS value of a port or to assign the default CoS to all incoming packets on the port.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>Device# configure terminal</pre>	Enters the global configuration mode.
Step 2	interface <i>interface-id</i> Example:	<p>Specifies the port to be configured, and enters interface configuration mode.</p> <p>Valid interfaces include physical ports.</p>

	Command or Action	Purpose
	Device(config)# interface gigabitethernet 0/2	
Step 3	mls qos cos {default-cos override} Example: Device(config-if)# mls qos cos override	<p>Configures the default CoS value for the port.</p> <ul style="list-style-type: none"> For <i>default-cos</i>, specify a default CoS value to be assigned to a port. If the packet is untagged, the default CoS value becomes the packet CoS value. The CoS range is 0 to 7. The default is 0. Use the override keyword to override the previously configured trust state of the incoming packet and to apply the default port CoS value to the port on all incoming packets. By default, CoS override is disabled. <p>Use the override keyword when all incoming packets on specified ports deserve higher or lower priority than packets entering from other ports. Even if a port was previously set to trust DSCP or CoS, this command overrides the previously configured trust state, and all the incoming CoS values are assigned the default CoS value configured with this command. If an incoming packet is tagged, the CoS value of the packet is modified with the default CoS of the port at the ingress port.</p> <p>Note To return to the default setting, use the no mls qos cos {default-cos override} interface configuration command.</p>
Step 4	end Example: Device(config-if)# end	Returns to privileged EXEC mode.
Step 5	show mls qos interface Example: Device# show mls qos interface	Verifies your entries.

Configuring a Trusted Boundary to Ensure Port Security

In a typical network, you connect a Cisco IP Phone to a switch port and cascade devices that generate data packets from the back of the telephone. The Cisco IP Phone guarantees the voice quality through a shared data link by marking the CoS level of the voice packets as high priority (CoS = 5) and by marking the data packets as low priority (CoS = 0). Traffic sent from the telephone to the switch is typically marked with a tag that uses the 802.1Q header. The header contains the VLAN information and the class of service (CoS) 3-bit field, which is the priority of the packet.

For most Cisco IP Phone configurations, the traffic sent from the telephone to the switch should be trusted to ensure that voice traffic is properly prioritized over other types of traffic in the network. By using the **mls qos trust cos** interface configuration command, you configure the switch port to which the telephone is connected to trust the CoS labels of all traffic received on that port. Use the **mls qos trust dscp** interface configuration command to configure a routed port to which the telephone is connected to trust the DSCP labels of all traffic received on that port.

With the trusted setting, you also can use the trusted boundary feature to prevent misuse of a high-priority queue if a user bypasses the telephone and connects the PC directly to the device. Without trusted boundary, the CoS labels generated by the PC are trusted by the device (because of the trusted CoS setting). By contrast, trusted boundary uses CDP to detect the presence of a Cisco IP Phone (such as the Cisco IP Phone 7910, 7935, 7940, and 7960) on a switch port. If the telephone is not detected, the trusted boundary feature disables the trusted setting on the switch port and prevents misuse of a high-priority queue. Note that the trusted boundary feature is not effective if the PC and Cisco IP Phone are connected to a hub that is connected to the device.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: Device# configure terminal	Enters the global configuration mode.
Step 2	cdp run Example: Device(config)# cdp run	Enables CDP globally. By default, CDP is enabled.
Step 3	interface interface-id Example: Device(config)# interface gigabitethernet 0/1	Specifies the port connected to the Cisco IP Phone, and enters interface configuration mode. Valid interfaces include physical ports.
Step 4	cdp enable Example: Device(config-if)# cdp enable	Enables CDP on the port. By default, CDP is enabled.

	Command or Action	Purpose
Step 5	Use one of the following: <ul style="list-style-type: none"> • mls qos trust cos • mls qos trust dscp Example: <pre>Device(config-if)# mls qos trust cos</pre>	Configures the switch port to trust the CoS value in traffic received from the Cisco IP Phone. or Configures the routed port to trust the DSCP value in traffic received from the Cisco IP Phone. By default, the port is not trusted.
Step 6	mls qos trust device cisco-phone Example: <pre>Device(config-if)# mls qos trust device cisco-phone</pre>	Specifies that the Cisco IP Phone is a trusted device. You cannot enable both trusted boundary and auto-QoS (auto qos voip interface configuration command) at the same time; they are mutually exclusive. Note To disable the trusted boundary feature, use the no mls qos trust device interface configuration command.
Step 7	end Example: <pre>Device(config-if)# end</pre>	Returns to privileged EXEC mode.
Step 8	show mls qos interface Example: <pre>Device# show mls qos interface</pre>	Verifies your entries.

Enabling DSCP Transparency Mode

The switch supports the DSCP transparency feature. It affects only the DSCP field of a packet at egress. By default, DSCP transparency is disabled.

If DSCP transparency is enabled by using the **no mls qos rewrite ip dscp** command, the switch does not modify the DSCP field in the incoming packet, and the DSCP field in the outgoing packet is the same as that in the incoming packet.

Regardless of the DSCP transparency configuration, the switch modifies the internal DSCP value of the packet, which the switch uses to generate a class of service (CoS) value that represents the priority of the traffic. The switch also uses the internal DSCP value to select an egress queue and threshold.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 2	mls qos Example: Device(config)# mls qos	Enables QoS globally.
Step 3	no mls qos rewrite ip dscp Example: Device(config)# no mls qos rewrite ip dscp	Enables DSCP transparency. The switch is configured to not modify the DSCP field of the IP packet.
Step 4	end Example: Device(config)# end	Returns to privileged EXEC mode.
Step 5	show mls qos interface [interface-id] Example: Device(config)# show mls qos interface gigabitethernet 0/1	Verifies your entries.

DSCP Transparency Mode

To configure the switch to modify the DSCP value based on the trust setting or on an ACL by disabling DSCP transparency, use the **mls qos rewrite ip dscp** global configuration command.

If you disable QoS by using the **no mls qos** global configuration command, the CoS and DSCP values are not changed (the default QoS setting).

If you enter the **no mls qos rewrite ip dscp** global configuration command to enable DSCP transparency and then enter the **mls qos trust [cos | dscp]** interface configuration command, DSCP transparency is still enabled.

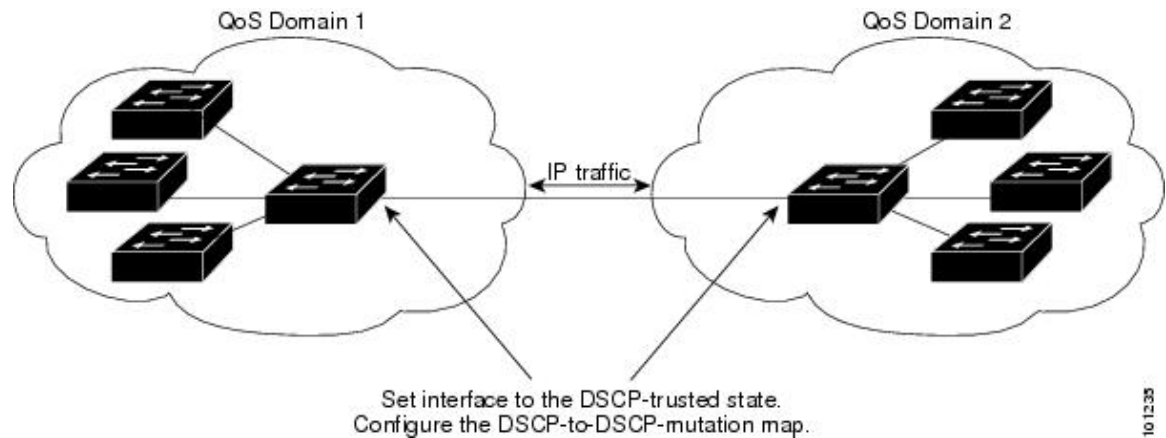
**Note**

DSCP transparency is disabled by default.

Configuring the DSCP Trust State on a Port Bordering Another QoS Domain

If you are administering two separate QoS domains between which you want to implement QoS features for IP traffic, you can configure the device ports bordering the domains to a DSCP-trusted state. The receiving port accepts the DSCP-trusted value and avoids the classification stage of QoS. If the two domains use different DSCP values, you can configure the DSCP-to-DSCP-mutation map to translate a set of DSCP values to match the definition in the other domain.

Figure 9: DSCP-Trusted State on a Port Bordering Another QoS Domain



Beginning in privileged EXEC mode, follow these steps to configure the DSCP-trusted state on a port and modify the DSCP-to-DSCP-mutation map. To ensure a consistent mapping strategy across both QoS domains, you must perform this procedure on the ports in both domains.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>Device# configure terminal</pre>	Enters the global configuration mode.
Step 2	mls qos map dscp-mutation in-dscp to out-dscp Example: <pre>Device(config)# mls qos map dscp-mutation 10 11 12 13 to 30</pre>	Modifies the DSCP-to-DSCP-mutation map. The default DSCP-to-DSCP-mutation map is a null map, which maps an incoming DSCP value to the same DSCP value. <ul style="list-style-type: none"> For <i>in-dscp</i>, enter up to eight DSCP values separated by spaces. Then enter the to keyword. For <i>out-dscp</i>, enter a single DSCP value. The DSCP range is 0 to 63.

	Command or Action	Purpose
Step 3	interface <i>interface-id</i> Example: Device (config) # interface gigabitethernet 0/2	Specifies the port to be trusted, and enter interface configuration mode. Valid interfaces include physical ports.
Step 4	mls qos trust dscp Example: Device (config-if) # mls qos trust dscp	Configures the ingress port as a DSCP-trusted port. By default, the port is not trusted. Note To return a port to its non-trusted state, use the no mls qos trust interface configuration command.
Step 5	end Example: Device (config-if) # end	Returns to privileged EXEC mode.
Step 6	show mls qos maps dscp-mutation Example: Device# show mls qos maps dscp-mutation	Verifies your entries. Note To return a port to its non-trusted state, use the no mls qos trust interface configuration command. To return to the default DSCP-to-DSCP-mutation map values, use the no mls qos map dscp-mutation dscp-mutation-name global configuration command.

Configuring a QoS Policy

Configuring a QoS policy typically requires the following tasks:

- Classifying traffic into classes
- Configuring policies applied to those traffic classes
- Attaching policies to ports

These sections describe how to classify, police, and mark traffic. Depending on your network configuration, you must perform one or more of the modules in this section.

Classifying Traffic by Using ACLs

You can classify IP traffic by using IPv4 standard ACLs, IPv4 extended ACLs, or IPv6 ACLs.

You can classify non-IP traffic by using Layer 2 MAC ACLs.

Creating an IP Standard ACL for IPv4 Traffic

Before you begin

Before you perform this task, determine which access lists you will be using for your QoS configuration.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>Device# configure terminal</pre>	Enters global configuration mode.
Step 2	access-list access-list-number {permit} source [source-wildcard] Example: <pre>Device(config)# access-list 1 permit 192.2.255.0 1.1.1.255</pre>	<p>Creates an IP standard ACL, repeating the command as many times as necessary.</p> <ul style="list-style-type: none"> For <i>access-list-number</i>, enter the access list number. The range is 1 to 99 and 1300 to 1999. Use the permit keyword to permit a certain type of traffic if the conditions are matched. For <i>source</i>, enter the network or host from which the packet is being sent. You can use the any keyword as an abbreviation for 0.0.0.0 255.255.255.255. (Optional) For <i>source-wildcard</i>, enter the wildcard bits in dotted decimal notation to be applied to the source. Place ones in the bit positions that you want to ignore. <p>When you create an access list, remember that by default the end of the access list contains an implicit deny statement for everything if it did not find a match before reaching the end.</p> <p>Note To delete an access list, use the no access-list access-list-number global configuration command.</p>
Step 3	end Example: <pre>Device(config)# end</pre>	Returns to privileged EXEC mode.

	Command or Action	Purpose
Step 4	show access-lists Example: Device# show access-lists	Verifies your entries.
Step 5	copy running-config startup-config Example: Device# copy-running-config startup-config	(Optional) Saves your entries in the configuration file.

Creating an IP Extended ACL for IPv4 Traffic

Before you begin

Before you perform this task, determine which access lists you will be using for your QoS configuration.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 2	access-list access-list-number permit protocol source source-wildcard destination destination-wildcard Example: Device(config)# access-list 100 permit ip any any dscp 32	Creates an IP extended ACL, repeating the command as many times as necessary. <ul style="list-style-type: none"> For <i>access-list-number</i>, enter the access list number. The range is 100 to 199 and 2000 to 2699. Use the permit keyword to permit a certain type of traffic if the conditions are matched. For <i>protocol</i>, enter the name or number of an IP protocol. Use the question mark (?) to see a list of available protocol keywords. For <i>source</i>, enter the network or host from which the packet is being sent. You specify this by using dotted decimal notation, by using the any keyword as an abbreviation for <i>source</i> 0.0.0.0 <i>source-wildcard</i> 255.255.255.255, or by using the host keyword for <i>source</i> 0.0.0.0.

	Command or Action	Purpose
		<ul style="list-style-type: none"> For <i>source-wildcard</i>, enter the wildcard bits by placing ones in the bit positions that you want to ignore. You specify the wildcard by using dotted decimal notation, by using the any keyword as an abbreviation for <i>source</i> 0.0.0.0 <i>source-wildcard</i> 255.255.255.255, or by using the host keyword for <i>source</i> 0.0.0.0. For <i>destination</i>, enter the network or host to which the packet is being sent. You have the same options for specifying the <i>destination</i> and <i>destination-wildcard</i> as those described by <i>source</i> and <i>source-wildcard</i>. <p>When creating an access list, remember that, by default, the end of the access list contains an implicit deny statement for everything if it did not find a match before reaching the end.</p> <p>Note To delete an access list, use the no access-list <i>access-list-number</i> global configuration command.</p>
Step 3	end Example: Device(config)# end	Returns to privileged EXEC mode.
Step 4	show access-lists Example: Device# show access-lists	Verifies your entries.
Step 5	copy running-config startup-config Example: Device# copy-running-config startup-config	(Optional) Saves your entries in the configuration file.

Creating an IPv6 ACL for IPv6 Traffic

Before you begin

Before you perform this task, determine which access lists you will be using for your QoS configuration.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>Device# configure terminal</pre>	Enters global configuration mode.
Step 2	ipv6 access-list access-list-name Example: <pre>Device(config)# ipv6 access-list ipv6_Name_ACL</pre>	<p>Creates an IPv6 ACL and enters IPv6 access-list configuration mode.</p> <p>Accesses list names cannot contain a space or quotation mark or begin with a numeric.</p> <p>Note To delete an access list, use the no ipv6 access-list access-list-number global configuration command.</p>
Step 3	<pre>{permit} protocol {source-ipv6-prefix/prefix-length any host source-ipv6-address} [operator [port-number]] {destination-ipv6-prefix/ prefix-length any host destination-ipv6-address} [operator [port-number]] [dscp value]</pre> Example: <pre>Device(config-ipv6-acl)# permit ip host 10::1 host 11::2 host</pre>	<p>Enters permit to permit the packet if conditions are matched. These are the conditions:</p> <p>For <i>protocol</i>, enter the name or number of an Internet protocol: ahp, esp, icmp, ipv6, pcp, stcp, tcp, or udp, or an integer in the range 0 to 255 representing an IPv6 protocol number.</p> <ul style="list-style-type: none"> The <i>source-ipv6-prefix/prefix-length</i> or <i>destination-ipv6-prefix/ prefix-length</i> is the source or destination IPv6 network or class of networks for which to set permit condition, specified in hexadecimal and using 16-bit values between colons (see RFC 2373). Enter any as an abbreviation for the IPv6 prefix ::/0. For host <i>source-ipv6-address</i> or <i>destination-ipv6-address</i>, enter the source or destination IPv6 host address for which to set permit condition, specified in hexadecimal using 16-bit values between colons. (Optional) For <i>operator</i>, specify an operand that compares the source or destination ports of the specified protocol. Operands are lt (less than), gt (greater than), eq (equal), neq (not equal), and range. <p>If the operator follows the <i>source-ipv6-prefix/prefix-length</i> argument,</p>

	Command or Action	Purpose
		<p>it must match the source port. If the operator follows the <i>destination-ipv6-prefix/prefix-length</i> argument, it must match the destination port.</p> <ul style="list-style-type: none"> • (Optional) The <i>port-number</i> is a decimal number from 0 to 65535 or the name of a TCP or UDP port. You can use TCP port names only when filtering TCP. You can use UDP port names only when filtering UDP. • (Optional) Enter dscp value to match a differentiated services code point value against the traffic class value in the Traffic Class field of each IPv6 packet header. The acceptable range is from 0 to 63.
Step 4	end Example: <pre>Device(config-ipv6-acl)# end</pre>	Returns to privileged EXEC mode.
Step 5	show ipv6 access-list Example: <pre>Device# show ipv6 access-list</pre>	Verifies the access list configuration.
Step 6	copy running-config startup-config Example: <pre>Device# copy-running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.

Creating a Layer 2 MAC ACL for Non-IP Traffic

Before you begin

Before you perform this task, determine that Layer 2 MAC access lists are required for your QoS configuration.

Procedure

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

	Command or Action	Purpose
	Device# configure terminal	
Step 2	mac access-list extended <i>name</i> Example: <pre>Device(config)# mac access-list extended maclist1</pre>	<p>Creates a Layer 2 MAC ACL by specifying the name of the list.</p> <p>After entering this command, the mode changes to extended MAC ACL configuration.</p> <p>Note To delete an access list, use the no mac access-list extended access-list-name global configuration command.</p>
Step 3	<pre>{permit deny} {host src-MAC-addr mask any host dst-MAC-addr dst-MAC-addr mask} [type mask]</pre> Example: <pre>Device(config-ext-macl) # permit 0001.0000.0001 0.0.0 0002.0000.0001 0.0.0</pre> <pre>Device(config-ext-macl) # permit 0001.0000.0002 0.0.0 0002.0000.0002 0.0.0 xns-idp</pre>	<p>Specifies the type of traffic to permit or deny if the conditions are matched, entering the command as many times as necessary.</p> <ul style="list-style-type: none"> For <i>src-MAC-addr</i>, enter the MAC address of the host from which the packet is being sent. You specify this by using the hexadecimal format (H.H.H), by using the any keyword as an abbreviation for <i>source</i> 0.0.0, <i>source-wildcard</i> ffff.ffff.ffff, or by using the host keyword for <i>source</i> 0.0.0. For <i>mask</i>, enter the wildcard bits by placing ones in the bit positions that you want to ignore. For <i>dst-MAC-addr</i>, enter the MAC address of the host to which the packet is being sent. You specify this by using the hexadecimal format (H.H.H), by using the any keyword as an abbreviation for <i>source</i> 0.0.0, <i>source-wildcard</i> ffff.ffff.ffff, or by using the host keyword for <i>source</i> 0.0.0. (Optional) For <i>type mask</i>, specify the Ethertype number of a packet with Ethernet II or SNAP encapsulation to identify the protocol of the packet. For <i>type</i>, the range is from 0 to 65535, typically specified in hexadecimal. For <i>mask</i>, enter the <i>don't care</i> bits applied to the Ethertype before testing for a match. <p>When creating an access list, remember that, by default, the end of the access list contains an implicit deny statement for everything if it did not find a match before reaching the end.</p>

	Command or Action	Purpose
Step 4	end Example: <pre>Device(config-ext-macl) # end</pre>	Returns to privileged EXEC mode.
Step 5	show access-lists [<i>access-list-number</i> <i>access-list-name</i>] Example: <pre>Device# show access-lists</pre>	Verifies your entries.
Step 6	copy running-config startup-config Example: <pre>Device# copy-running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.

Classifying Traffic by Using Class Maps

You use the **class-map** global configuration command to name and to isolate a specific traffic flow (or class) from all other traffic. The class map defines the criteria to use to match against a specific traffic flow to further classify it. Match statements can include criteria such as an ACL or DSCP values. The match criterion is defined with one match statement entered within the class-map configuration mode.



Note You can also create class maps during policy map creation by using the **class** policy-map configuration command.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>Device# configure terminal</pre>	Enters the global configuration mode.
Step 2	Use one of the following: <ul style="list-style-type: none"> access-list <i>access-list-number</i> {permit} <i>source</i> [<i>source-wildcard</i>] access-list <i>access-list-number</i> {permit} <i>protocol source</i> [<i>source-wildcard</i>] <i>destination</i> [<i>destination-wildcard</i>] 	Creates an IP standard or extended ACL, an IPv6 ACL for IP traffic, or a Layer 2 MAC ACL for non-IP traffic, repeating the command as many times as necessary. When creating an access list, remember that, by default, the end of the access list contains an

	Command or Action	Purpose
	<ul style="list-style-type: none"> • ipv6 access-list <i>access-list-name</i> {permit deny} {<i>source-ipv6-prefix/prefix-length</i> any host <i>source-ipv6-address</i>} [<i>operator</i> [<i>port-number</i>]] {<i>destination-ipv6-prefix/prefix-length</i> any host <i>destination-ipv6-address</i>} [<i>operator</i> [<i>port-number</i>]] [dscp <i>value</i>] • mac access-list extended <i>name</i> {permit deny} {host <i>src-MAC-addr mask</i> any host <i>dst-MAC-addr</i> <i>dst-MAC-addr mask</i>} [<i>type mask</i>] <p>Example:</p> <pre>Device(config)# access-list 103 permit ip any any dscp 10</pre>	implicit deny statement for everything if it did not find a match before reaching the end.
Step 3	<p>class-map [match-all] <i>class-map-name</i></p> <p>Example:</p> <pre>Device(config)# class-map class1</pre>	<p>Creates a class map, and enters class-map configuration mode.</p> <p>By default, no class maps are defined.</p> <ul style="list-style-type: none"> • (Optional) Use the match-all keyword to perform a logical-AND of all matching statements under this class map. All match criteria in the class map must be matched. • For <i>class-map-name</i>, specify the name of the class map. <p>Note To delete an existing class map, use the no class-map [match-all] <i>class-map-name</i> global configuration command.</p>
Step 4	<p>match {access-group <i>acl-index-or-name</i> ip dscp <i>dscp-list</i>}</p> <p>Example:</p> <pre>Device(config-cmap)# match ip dscp 10 11 12</pre>	<p>Defines the match criterion to classify traffic.</p> <p>By default, no match criterion is defined.</p> <p>Only one match criterion per class map is supported, and only one ACL per class map is supported.</p> <ul style="list-style-type: none"> • For access-group <i>acl-index-or-name</i>, specify the number or name of the ACL created in Step 2. • To filter IPv6 traffic with the match access-group command, create an IPv6 ACL, as described in Step 2.

	Command or Action	Purpose
		<ul style="list-style-type: none"> For ip dscp dscp-list, enter a list of up to eight IP DSCP values to match against incoming packets. Separate each value with a space. The range is 0 to 63. <p>Note To remove a match criterion, use the no match {access-group acl-index-or-name ip dscp} class-map configuration command.</p>
Step 5	end Example: Device(config-cmap) # end	Returns to privileged EXEC mode.
Step 6	show class-map Example: Device# show class-map	Verifies your entries.

Classifying, Policing, and Marking Traffic on Physical Ports by Using Policy Maps

You can configure a policy map on a physical port that specifies which traffic class to act on. Actions can include trusting the CoS or DSCP values in the traffic class; setting a specific DSCP value in the traffic class; and specifying the traffic bandwidth limitations for each matched traffic class (policer) and the action to take when the traffic is out of profile (marking).

A policy map also has these characteristics:

- A policy map can contain multiple class statements, each with different match criteria and policers.
- A policy map can contain a predefined default traffic class explicitly placed at the end of the map.
- A separate policy-map class can exist for each type of traffic received through a port.

Follow these guidelines when configuring policy maps on physical ports:

- You can attach only one policy map per ingress port.
- mls qos must be enabled in global configuration mode.
- If you enter or have used the **set ip dscp** command, the device changes this command to **set dscp** in its configuration.
- A policy-map and a port trust state can both run on a physical interface. The policy-map is applied before the port trust state.
- When you configure a default traffic class by using the **class class-default** policy-map configuration command, unclassified traffic (traffic that does not meet the match criteria specified in the traffic classes) is treated as the default traffic class (class-default).

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>Device# configure terminal</pre>	Enters the global configuration mode.
Step 2	class-map <i>class-map-name</i> Example: <pre>Device(config)# class-map ipclass1</pre>	<p>Creates a class map, and enters class-map configuration mode.</p> <p>By default, no class maps are defined. For <i>class-map-name</i>, specify the name of the class map.</p>
Step 3	policy-map <i>policy-map-name</i> Example: <pre>Device(config-cmap)# policy-map flowit</pre>	<p>Creates a policy map by entering the policy map name, and enters policy-map configuration mode.</p> <p>By default, no policy maps are defined.</p> <p>The default behavior of a policy map is to set the DSCP to 0 if the packet is an IP packet and to set the CoS to 0 if the packet is tagged. No policing is performed.</p> <p>Note To delete an existing policy map, use the no policy-map <i>policy-map-name</i> global configuration command.</p>
Step 4	class [<i>class-map-name</i> class-default] Example: <pre>Device(config-pmap)# class ipclass1</pre>	<p>Defines a traffic classification, and enters policy-map class configuration mode.</p> <p>By default, no policy map class-maps are defined.</p> <p>If a traffic class has already been defined by using the class-map global configuration command, specify its name for <i>class-map-name</i> in this command.</p> <p>A class-default traffic class is pre-defined and can be added to any policy. It is always placed at the end of a policy map. With an implied match any included in the class-default class, all packets that have not already matched the other traffic classes will match class-default.</p> <p>Note To delete an existing class map, use the no class <i>class-map-name</i> policy-map configuration command.</p>

	Command or Action	Purpose
Step 5	set dscp new-dscp Example: <pre>Device(config-pmap-c) # set dscp 45</pre>	Classifies IP traffic by setting a new value in the packet. <ul style="list-style-type: none"> For dscp new-dscp, enter a new DSCP value to be assigned to the classified traffic. The range is 0 to 63.
Step 6	police rate-bps burst-byte [exceed-action {drop}] Example: <pre>Device(config-pmap-c) # police 100000 80000 exceed-action drop</pre>	Defines a policer for the classified traffic. By default, no policer is defined. <ul style="list-style-type: none"> For rate-bps, specify average traffic rate in bits per second (b/s). The range is 8000 to 10000000000. For burst-byte, specify the normal burst size in bytes. <ul style="list-style-type: none"> If $8000 \leq \text{rate-bps} < 102300000$, burst-byte range is 8000 to 65535. If $102300000 \leq \text{rate-bps} < 1023000000$, burst-byte range is 8000 to 524280. If $1023000000 \leq \text{rate-bps} \leq 10\text{Gig}$, burst-byte range is 8000 to 1000000. (Optional) Specifies the action to take when the rates are exceeded. Use the exceed-action drop keywords to drop the packet. <p>Note To remove an existing policer, use the no police rate-bps burst-byte [exceed-action drop] policy-map configuration command.</p>
Step 7	exit Example: <pre>Device(config-pmap-c) # exit</pre>	Returns to policy map configuration mode.
Step 8	exit Example: <pre>Device(config-pmap) # exit</pre>	Returns to global configuration mode.

	Command or Action	Purpose
Step 9	interface <i>interface-id</i> Example: <pre>Device(config)# interface gigabitethernet 0/1</pre>	Specifies the port to attach to the policy map, and enters interface configuration mode. Valid interfaces include physical ports.
Step 10	service-policy input <i>policy-map-name</i> Example: <pre>Device(config-if)# service-policy input flowit</pre>	Specifies the policy-map name, and applies it to an ingress port. Only one policy map per ingress port is supported. Note To remove the policy map and port association, use the no service-policy input <i>policy-map-name</i> interface configuration command.
Step 11	end Example: <pre>Device(config-if)# end</pre>	Returns to privileged EXEC mode.
Step 12	show policy-map [<i>policy-map-name</i> [class <i>class-map-name</i>]] Example: <pre>Device# show policy-map</pre>	Verifies your entries.

Configuring Egress Queue Characteristics

Depending on the complexity of your network and your QoS solution, you might need to perform all of the tasks in the following modules. You need to make decisions about these characteristics:

- Which packets are mapped by DSCP or CoS value to each queue and threshold ID?
- What drop percentage thresholds apply to the queue-set (four egress queues per port), and how much reserved and maximum memory is needed for the traffic type?
- Does the bandwidth of the port need to be rate limited?
- How often should the egress queues be serviced and which technique (shaped, shared, or both) should be used?

Configuration Guidelines

Follow these guidelines when the expedite queue is enabled or the egress queues are serviced based on their SRR weights:

- If the egress expedite queue is enabled, it overrides the SRR shaped and shared weights for queue 1.
- If the egress expedite queue is disabled and the SRR shaped and shared weights are configured, the shaped mode overrides the shared mode for queue 1, and SRR services this queue in shaped mode.
- If the egress expedite queue is disabled and the SRR shaped weights are not configured, SRR services this queue in shared mode.

Mapping DSCP or CoS Values to an Egress Queue and to a Threshold ID

You can prioritize traffic by placing packets with particular DSCPs or costs of service into certain queues and adjusting the queue thresholds so that packets with lower priorities are dropped. Default number of queues is 4. You can increase it to 8 using the **mls qos srr-queue output queues 8** command.



Note

The egress queue default settings are suitable for most situations. You should change them only when you have a thorough understanding of egress queues and if these settings do not meet your QoS solution.

Beginning in privileged EXEC mode, follow these steps to map DSCP or CoS values to an egress queue and to a threshold ID. This procedure is optional.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 2	Use one of the following: <ul style="list-style-type: none"> • mls qos srr-queue output dscp-map queue <i>queue-id</i> threshold <i>threshold-id</i> dscp1...dscp8 • mls qos srr-queue output cos-map queue <i>queue-id</i> threshold <i>threshold-id</i> cos1...cos8 Example: Device(config)# mls qos srr-queue output dscp-map queue 1 threshold 2 10 11	Maps DSCP or CoS values to an egress queue and to a threshold ID. By default, DSCP values 0–15 are mapped to queue 2 and threshold 1. DSCP values 16–31 are mapped to queue 3 and threshold 1. DSCP values 32–39 and 48–63 are mapped to queue 4 and threshold 1. DSCP values 40–47 are mapped to queue 1 and threshold 1. By default, CoS values 0 and 1 are mapped to queue 2 and threshold 1. CoS values 2 and 3 are mapped to queue 3 and threshold 1. CoS values 4, 6, and 7 are mapped to queue 4 and threshold 1. CoS value 5 is mapped to queue 1 and threshold 1. <ul style="list-style-type: none"> • For <i>queue-id</i>, the range is 1 to 4. • For <i>threshold-id</i>, the range is 1 to 32. The drop-threshold percentage for threshold 3

	Command or Action	Purpose
		<p>is predefined. It is set to the queue-full state.</p> <ul style="list-style-type: none"> For <i>dscp1...dscp8</i>, enter up to eight values, and separate each value with a space. The range is 0 to 63. For <i>cos1...cos8</i>, enter up to eight values, and separate each value with a space. The range is 0 to 7. <p>Note To return to the default DSCP output queue threshold map or the default CoS output queue threshold map, use the no mls qos srr-queue output dscp-map or the no mls qos srr-queue output cos-map global configuration command.</p>
Step 3	<p>mls qos srr-queue output cos-map queue <i>queue-id</i> threshold <i>threshold-id</i> cos1...cos8</p> <p>Example:</p> <pre>Device(config)# mls qos srr-queue output cos-map queue 3 threshold 1 2 3</pre>	<p>Maps CoS values to an egress queue and to a threshold ID.</p> <p>By default, CoS values 0 and 1 are mapped to queue 2 and threshold 1. CoS values 2 and 3 are mapped to queue 3 and threshold 1. CoS values 4, 6, and 7 are mapped to queue 4 and threshold 1. CoS value 5 is mapped to queue 1 and threshold 1.</p> <ul style="list-style-type: none"> For <i>queue-id</i>, the range is 1 to 4. For <i>threshold-id</i>, the range is 1 to 2. The drop-threshold percentage for threshold 3 is predefined. It is set to the queue-full state. For <i>cos1...cos8</i>, enter up to eight values, and separate each value with a space. The range is 0 to 7. <p>Note To return to the default CoS output queue threshold map, use the no mls qos srr-queue output cos-map global configuration command.</p>
Step 4	<p>end</p> <p>Example:</p> <pre>Device(config)# end</pre>	Returns to privileged EXEC mode.
Step 5	show mls qos maps	Verifies your entries.

	Command or Action	Purpose
	Example: Device# show mls qos maps	<p>The DSCP output queue threshold map appears as a matrix. The d1 column specifies the most-significant digit of the DSCP number; the d2 row specifies the least-significant digit in the DSCP number. The intersection of the d1 and the d2 values provides the queue ID and threshold ID; for example, queue 2 and threshold 1 (02-01).</p> <p>The CoS output queue threshold map shows the CoS value in the top row and the corresponding queue ID and threshold ID in the second row; for example, queue 2 and threshold 2 (2-2).</p> <p>To return to the default DSCP output queue threshold map or the default CoS output queue threshold map, use the no mls qos srr-queue output dscp-map or the no mls qos srr-queue output cos-map global configuration command.</p>

Configuring SRR Shaped Weights on Egress Queues

You can specify how much of the available bandwidth is allocated to each queue. The ratio of the weights is the ratio of frequency in which the SRR scheduler sends packets from each queue.

You can configure the egress queues for shaped or shared weights, or both. Use shaping to smooth bursty traffic or to provide a smoother output over time.

Beginning in privileged EXEC mode, follow these steps to assign the shaped weights and to enable bandwidth shaping on the four egress queues mapped to a port. This procedure is optional.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: Device# configure terminal	Enters the global configuration mode.
Step 2	interface interface-id Example: Device(config)# interface gigabitethernet 0/1	Specifies the port of the outbound traffic, and enters interface configuration mode.
Step 3	srr-queue bandwidth shape weight1 weight2 weight3 weight4 Example: Device(config-if)# srr-queue	Assigns SRR weights to the egress queues. By default, weight1 is set to 25; weight2, weight3, and weight4 are set to 0, and these queues are in shared mode.

	Command or Action	Purpose
	<code>bandwidth shape 8 0 0 0</code>	<p>For <i>weight1 weight2 weight3 weight4</i>, enter the weights to control the percentage of the port that is shaped. The inverse ratio (1/weight) controls the shaping bandwidth for this queue. Separate each value with a space. The range is 0 to 65535.</p> <p>If you configure a weight of 0, the corresponding queue operates in shared mode. The weight specified with the srr-queue bandwidth shape command is ignored, and the weights specified with the srr-queue bandwidth share interface configuration command for a queue come into effect. When configuring queues in the same queue-set for both shaping and sharing, make sure that you configure the lowest number queue for shaping.</p> <p>The shaped mode overrides the shared mode.</p> <p>To return to the default setting, use the no srr-queue bandwidth shape interface configuration command.</p>
Step 4	end Example: <code>Device(config-if)# end</code>	Returns to privileged EXEC mode.
Step 5	show mls qos interface interface-id queueing Example: <code>Device(config)# show mls qos interface gigabitethernet 0/1 queueing</code>	Verifies your entries.

Configuring SRR Shared Weights on Egress Queues

In shared mode, the queues share the bandwidth among them according to the configured weights. The bandwidth is guaranteed at this level but not limited to it. For example, if a queue empties and does not require a share of the link, the remaining queues can expand into the unused bandwidth and share it among them. With sharing, the ratio of the weights controls the frequency of dequeuing; the absolute values are meaningless.



Note

The egress queue default settings are suitable for most situations. You should change them only when you have a thorough understanding of the egress queues and if these settings do not meet your QoS solution.

Beginning in privileged EXEC mode, follow these steps to assign the shared weights and to enable bandwidth sharing on the four egress queues mapped to a port. This procedure is optional.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 2	interface interface-id Example: Device(config)# interface gigabitethernet 0/1	Specifies the port of the outbound traffic, and enters interface configuration mode.
Step 3	srr-queue bandwidth share weight1 weight2 weight3 weight4 Example: Device(config-id)# srr-queue bandwidth share 1 2 3 4	Assigns SRR weights to the egress queues. By default, all four weights are 25 (1/4 of the bandwidth is allocated to each queue). For <i>weight1 weight2 weight3 weight4</i> , enter the weights to control the ratio of the frequency in which the SRR scheduler sends packets. Separate each value with a space. The range is 1 to 255. To return to the default setting, use the no srr-queue bandwidth share interface configuration command.
Step 4	end Example: Device(config-id)# end	Returns to privileged EXEC mode.
Step 5	show mls qos interface interface-id queueing Example: Device(config)# show mls qos interface gigabitethernet 0/1 queueing	Verifies your entries.

Configuring the Egress Expedite Queue

You can ensure that certain packets have priority over all others by queuing them in the egress expedite queue. SRR services this queue until it is empty before servicing the other queues.

Beginning in privileged EXEC mode, follow these steps to enable the egress expedite queue. This procedure is optional.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 2	mls qos Example: Device(config)# mls qos	Enables QoS on a switch.
Step 3	interface interface-id Example: Device(config)# interface gigabitethernet 0/1	Specifies the egress port, and enters interface configuration mode.
Step 4	priority-queue out Example: Device(config-if)# priority-queue out	<p>Enables the egress expedite queue, which is disabled by default.</p> <p>When you configure this command, the SRR weight and queue size ratios are affected because there is one fewer queue participating in SRR. This means that <i>weight1</i> in the srr-queue bandwidth shape or the srr-queue bandwidth share command is ignored (not used in the ratio calculation).</p> <p>Note To disable the egress expedite queue, use the no priority-queue out interface configuration command.</p>
Step 5	end Example: Device(config-if)# end	Returns to privileged EXEC mode.

Limiting the Bandwidth on an Egress Interface

You can limit the bandwidth on an egress port. For example, if a customer pays only for a small percentage of a high-speed link, you can limit the bandwidth to that amount.

**Note**

The egress queue default settings are suitable for most situations. You should change them only when you have a thorough understanding of the egress queues and if these settings do not meet your QoS solution.

Beginning in privileged EXEC mode, follow these steps to limit the bandwidth on an egress port. This procedure is optional.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 2	interface interface-id Example: Device(config)# interface gigabitethernet 0/1	Specifies the port to be rate-limited, and enters interface configuration mode.
Step 3	srr-queue bandwidth limit weight1 Example: Device(config-if)# srr-queue bandwidth limit 80	Specifies the percentage of the port speed to which the port should be limited. The range is 10 to 90. By default, the port is not rate-limited and is set to 100 percent. Note To return to the default setting, use the no srr-queue bandwidth limit interface configuration command.
Step 4	end Example: Device(config-if)# end	Returns to privileged EXEC mode.
Step 5	show mls qos interface [interface-id] queueing Example: Device(config)# show mls qos interface gigabitethernet 0/1 queueing	Verifies your entries.

Monitoring Standard QoS

Table 9: Commands for Monitoring Standard QoS on the Switch

Command	Description
show mls qos	Displays global QoS configuration information.

Command	Description
show mls qos interface [<i>interface-id</i>] [policers queueing statistics]	Displays QoS information at the port level, including the buffer allocation, which ports have configured policers, the queueing strategy, and the ingress and egress statistics.
show mls qos maps [cos-output-q dscp-mutation]	Displays QoS mapping information.
show running-config include rewrite	Displays the DSCP transparency setting.

Configuration Examples for QoS

Example: Configuring Port to the DSCP-Trusted State and Modifying the DSCP-to-DSCP-Mutation Map

This example shows how to configure a port to the DSCP-trusted state and to modify the DSCP-to-DSCP-mutation map so that incoming DSCP values 10 to 13 are mapped to DSCP 30:

```
Device(config)# mls qos map dscp-mutation
10 11 12 13 to 30
Device(config)# interface gigabitethernet 0/2
Device(config-if)# mls qos trust dscp
Device(config-if)# end
```

Examples: Classifying Traffic by Using ACLs

This example shows how to allow access for only those hosts on the three specified networks. The wildcard bits apply to the host portions of the network addresses. Any host with a source address that does not match the access list statements is rejected.

```
Device(config)# access-list 1 permit 192.5.255.0 0.0.0.255
Device(config)# access-list 1 permit 128.88.0.0 0.0.255.255
Device(config)# access-list 1 permit 36.0.0.0 0.0.0.255
! (Note: all other access implicitly denied)
```

This example shows how to create an ACL that permits IP traffic from any source to any destination that has the DSCP value set to 32:

```
Device(config)# access-list 100 permit ip any any dscp 32
```

This example shows how to create an ACL that permits IP traffic from a source host at 10.1.1.1 to a destination host at 10.1.1.2 with a precedence value of 5:

```
Device(config)# access-list 100 permit ip host 10.1.1.1 host 10.1.1.2 precedence 5
```


This example shows how to create an ACL that permits PIM traffic from any source to a destination group address of 224.0.0.2 with a DSCP set to 32:

```
Device(config)# access-list 102 permit pim any 224.0.0.2 dscp 32
```

This example shows how to create an ACL that permits IPv6 traffic from any source to any destination that has the DSCP value set to 32:

```
Device(config)# ipv6 access-list 100 permit ip any any dscp 32
```

This example shows how to create an ACL that permits IPv6 traffic from a source host at 10.1.1.1 to a destination host at 10.1.1.2 with a precedence value of 5:

```
Device(config)# ipv6 access-list ipv6_Name_ACL permit ip host 10::1 host 10.1.1.2
precedence 5
```

This example shows how to create a Layer 2 MAC ACL with two permit statements. The first statement allows traffic from the host with MAC address 0001.0000.0001 to the host with MAC address 0002.0000.0001. The second statement allows only Ethertype XNS-IDP traffic from the host with MAC address 0001.0000.0002 to the host with MAC address 0002.0000.0002.

```
Device(config)# mac access-list extended maclist1
Device(config-ext-macl)# permit 0001.0000.0001 0.0.0 0002.0000.0001 0.0.0
Device(config-ext-macl)# permit 0001.0000.0002 0.0.0 0002.0000.0002 0.0.0 xns-idp
! (Note: all other access implicitly denied)
```

Examples: Classifying Traffic by Using Class Maps

This example shows how to configure the class map called *class1*. The *class1* has one match criterion, which is access list 103. It permits traffic from any host to any destination that matches a DSCP value of 10.

```
Device(config)# access-list 103 permit ip any any dscp 10
Device(config)# class-map class1
Device(config-cmap)# match access-group 103
Device(config-cmap)# end
Device#
```

This example shows how to create a class map called *class2*, which matches incoming traffic with DSCP values of 10, 11, and 12.

```
Device(config)# class-map class2
Device(config-cmap)# match ip dscp 10 11 12
Device(config-cmap)# end
Device#
```

This example shows how to configure a class map to match IP DSCP and IPv6:

```
Device(config)# Class-map cm-1
Device(config-cmap)# match ip dscp 10
Device(config-cmap)# exit
```

```

Device(config)# Class-map cm-2
Device(config-cmap)# match ip dscp 20
Device(config-cmap)# exit
Device(config)# Policy-map pml
Device(config-pmap)# class cm-1
Device(config-pmap-c)# set dscp 4
Device(config-pmap-c)# exit
Device(config-pmap)# class cm-2
Device(config-pmap-c)# set dscp 6
Device(config-pmap-c)# exit
Device(config-pmap)# exit
Device(config)# interface G1/0/1
Device(config-if)# service-policy input pml

```

This example shows how to configure a class map that applies to both IPv4 and IPv6 traffic:

```

Device(config)# ip access-list 101 permit ip any any
Device(config)# ipv6 access-list ipv6-any permit ip any any
Device(config)# Class-map cm-1
Device(config-cmap)# match access-group 101
Device(config-cmap)# exit
Device(config)# class-map cm-2
Device(config-cmap)# match access-group name ipv6-any
Device(config-cmap)# exit
Device(config)# Policy-map pml
Device(config-pmap)# class cm-1
Device(config-pmap-c)# set dscp 4
Device(config-pmap-c)# exit
Device(config-pmap)# class cm-2
Device(config-pmap-c)# set dscp 6
Device(config-pmap-c)# exit
Device(config-pmap)# exit
Device(config)# interface G0/1
Device(config-if)# switch mode access
Device(config-if)# service-policy input pml

```

Examples: Classifying, Policing, and Marking Traffic on Physical Ports Using Policy Maps

This example shows how to create a policy map and attach it to an ingress port. In the configuration, the IP standard ACL permits traffic from network 10.1.0.0. For traffic matching this classification, the DSCP value in the incoming packet is trusted. If the matched traffic exceeds an average traffic rate of 48000 b/s and a normal burst size of 8000 bytes, its DSCP is marked down (based on the policed-DSCP map) and sent:

```

Device(config)# access-list 1 permit 10.1.0.0 0.0.255.255
Device(config)# class-map ipclass1
Device(config-cmap)# match access-group 1
Device(config-cmap)# exit
Device(config)# policy-map flow1t
Device(config-pmap)# class ipclass1
Device(config-pmap-c)# set dscp cs1
Device(config-pmap-c)# police 1000000 8000 exceed-action drop
Device(config-pmap-c)# exit
Device(config-pmap)# exit
Device(config)# interface gigabitethernet 0/1

```

```
Device(config-if)# service-policy input flow1t
```

This example shows how to create a Layer 2 MAC ACL with two permit statements and attach it to an ingress port. The first permit statement allows traffic from the host with MAC address 0001.0000.0001 destined for the host with MAC address 0002.0000.0001. The second permit statement allows only Ethertype XNS-IDP traffic from the host with MAC address 0001.0000.0002 destined for the host with MAC address 0002.0000.0002.

```
Device(config)# mac access-list extended maclist1
Device(config-ext-mac)# permit 0001.0000.0001 0.0.0 0002.0000.0001 0.0.0
Device(config-ext-mac)# permit 0001.0000.0002 0.0.0 0002.0000.0002 0.0.0 xns-idp
Device(config-ext-mac)# exit
Device(config)# mac access-list extended maclist2
Device(config-ext-mac)# permit 0001.0000.0003 0.0.0 0002.0000.0003 0.0.0
Device(config-ext-mac)# permit 0001.0000.0004 0.0.0 0002.0000.0004 0.0.0 aarp
Device(config-ext-mac)# exit
Device(config)# class-map macclass1
Device(config-cmap)# match access-group maclist1
Device(config-cmap)# exit
Device(config)# policy-map macpolicy1
Device(config-pmap)# class macclass1
Device(config-pmap-c)# set dscp 63
Device(config-pmap-c)# exit
Device(config-pmap)# class macclass2 maclist2
Device(config-pmap-c)# set dscp 45
Device(config-pmap-c)# exit
Device(config-pmap)# exit
Device(config)# interface gigabitethernet 0/1
Device(config-if)# mls qos trust cos
Device(config-if)# service-policy input macpolicy1
```

This example shows how to create a class map that applies to both IPv4 and IPv6 traffic with the default class applied to unclassified traffic:

```
Device(config)# ip access-list 101 permit ip any any
Device(config)# ipv6 access-list ipv6-any permit ip any any
Device(config)# class-map cm-1
Device(config-cmap)# match access-group 101
Device(config-cmap)# exit
Device(config)# class-map cm-2
Device(config-cmap)# match access-group name ipv6-any
Device(config-cmap)# exit
Device(config)# policy-map pml
Device(config-pmap)# class cm-1
Device(config-pmap-c)# set dscp 4
Device(config-pmap-c)# exit
Device(config-pmap)# class cm-2
Device(config-pmap-c)# set dscp 6
Device(config-pmap-c)# exit
Device(config-pmap)# class class-default
Device(config-pmap-c)# set dscp 10
Device(config-pmap-c)# exit
Device(config-pmap)# exit
Device(config)# interface G0/1
Device(config-if)# switch mode access
Device(config-if)# service-policy input pml
```

Examples: Configuring DSCP-to-DSCP Mutation Maps

This example shows how to define the DSCP-to-DSCP-mutation map. All the entries that are not explicitly configured are not modified (remains as specified in the null map):

```
Device(config)# mls qos map dscp-mutation 1 2 3 4 5 6 7 to 0
Device(config)# mls qos map dscp-mutation 8 9 10 11 12 13 to 10
Device(config)# mls qos map dscp-mutation 20 21 22 to 20
Device(config)# mls qos map dscp-mutation 30 31 32 33 34 to 30
Device(config)# interface gigabitethernet 0/1
Device(config-if)# mls qos trust dscp
Device(config-if)# end
Device# show mls qos maps dscp-mutation
Dscp-dscp mutation map:
mutation1:
  d1 : d2 0  1  2  3  4  5  6  7  8  9
-----
  0 :   00 00 00 00 00 00 00 00 10 10
  1 :   10 10 10 10 14 15 16 17 18 19
  2 :   20 20 20 23 24 25 26 27 28 29
  3 :   30 30 30 30 30 35 36 37 38 39
  4 :   40 41 42 43 44 45 46 47 48 49
  5 :   50 51 52 53 54 55 56 57 58 59
  6 :   60 61 62 63
```



Note

In the above DSCP-to-DSCP-mutation map, the mutated values are shown in the body of the matrix. The d1 column specifies the most-significant digit of the original DSCP; the d2 row specifies the least-significant digit of the original DSCP. The intersection of the d1 and d2 values provides the mutated value. For example, a DSCP value of 12 corresponds to a mutated value of 10.

Examples: Configuring Egress Queue Characteristics

This example shows how to configure bandwidth shaping on queue 1. Because the weight ratios for queues 2, 3, and 4 are set to 0, these queues operate in shared mode. The bandwidth weight for queue 1 is 1/8, which is 12.5 percent:

```
Device(config)# interface gigabitethernet 0/1
Device(config-if)# srr-queue bandwidth shape 8 0 0 0
```

This example shows how to configure the weight ratio of the SRR scheduler running on an egress port. Four queues are used, and the bandwidth ratio allocated for each queue in shared mode is $1/(1+2+3+4)$, $2/(1+2+3+4)$, $3/(1+2+3+4)$, and $4/(1+2+3+4)$, which is 10 percent, 20 percent, 30 percent, and 40 percent for queues 1, 2, 3, and 4. This means that queue 4 has four times the bandwidth of queue 1, twice the bandwidth of queue 2, and one-and-a-third times the bandwidth of queue 3.

```
Device(config)# interface gigabitethernet 0/1
Device(config-if)# srr-queue bandwidth share 1 2 3 4
```

This example shows how to enable the egress expedite queue when the SRR weights are configured. The egress expedite queue overrides the configured SRR weights.

```

Device(config)# interface gigabitethernet 0/1
Device(config-if)# srr-queue bandwidth shape 25 0 0 0
Device(config-if)# srr-queue bandwidth share 30 20 25 25
Device(config-if)# priority-queue out
Device(config-if)# end

```

This example shows how to limit the bandwidth on a port to 80 percent:

```

Device(config)# interface gigabitethernet 0/1
Device(config-if)# srr-queue bandwidth limit 80

```

When you configure this command to 80 percent, the port is idle 20 percent of the time. The line rate drops to 80 percent of the connected speed, which is 800 Mb/s. These values are not exact because the hardware adjusts the line rate in increments of six.

Feature Information for QoS

This table provides release and related information for features explained in this module.

These features are available on all releases subsequent to the one they were introduced in, unless noted otherwise.

Release	Feature	Feature Information
Cisco IOS Release 15.2(5)E	QoS	Implementing QoS in your network makes network performance more predictable and bandwidth utilization more effective.

Use Cisco Feature Navigator to find information about platform and software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>.

