



Configuring QoS

This chapter describes how to configure quality of service (QoS) on your switch. With this feature, you can provide preferential treatment to certain types of traffic. Without QoS, the switch offers best-effort service to each packet, regardless of the packet contents or size. It transmits the packets without any assurance of reliability, delay bounds, or throughput.

To use the features described in this chapter, you must have the enhanced software image installed on your switch.

If you have the standard software image installed on your switch, you cannot configure some of the features. [Table 13-1](#) lists the sections that describe the features that you can configure.

Table 13-1 Sections Describing Standard-Software Features

Topic	Section
Queueing and scheduling at the egress ports	“Queueing and Scheduling” section on page 13-8.
Configuring QoS	“Configuring QoS” section on page 13-9.
	“Default QoS Configuration” section on page 13-9.
	“Configuring the CoS Value for an Interface” section on page 13-13.
	“Configuring CoS and WRR” section on page 13-23.



Note

For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 2950 Desktop Switch Command Reference* for this release.

QoS can be configured either by using the Cluster Management Suite (CMS) or through the command-line interface (CLI). Refer to the CMS online help for step-by-step configuration procedures through CMS. For information about accessing and using CMS, see the [“Getting Started with CMS” section on page 2-1.](#)

You can also use these wizards to configure QoS:



Note

These wizards are available only if your switch is running the enhanced software image.

- **Priority data wizard**—Lets you assign priority levels to data applications based on their TCP or UDP ports. It provides a standard list of applications, and you select the ones that you want to prioritize, the priority levels, and the interfaces where the prioritization occurs. Refer to the priority data wizard online help for step-by-step procedures on using this wizard.
- **Video wizard**—Gives traffic that originates from specified video servers a higher priority than the priority of data traffic. The wizard assumes that the video servers are connected to a single device in the cluster. Refer to the video wizard online help for step-by-step procedures on using this wizard.

This chapter consists of these sections:

- [Understanding QoS, page 13-2](#)
- [Configuring QoS, page 13-9](#)
- [Displaying QoS Information, page 13-25](#)
- [QoS Configuration Examples, page 13-25](#)

Understanding QoS

This section describes how QoS is implemented on the Catalyst 2950 switch. If you have the standard software image installed on your switch, some concepts and features in this section might not apply. For a list of available features, see [Table 13-1 on page 13-1](#).

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 DiffServ architecture, an emerging standard from the Internet Engineering Task Force (IETF). This architecture specifies that each packet is classified upon entry into the network. The classification is carried in the IP packet header, using 6 bits from the deprecated IP Type-of-Service (TOS) field to carry the classification (*class*) information.

Classification can also be carried in the Layer 2 frame. These special bits in the Layer 2 frame or a Layer 3 packet are described here and shown in [Figure 13-1](#):

- **Prioritization values in Layer 2 frames**

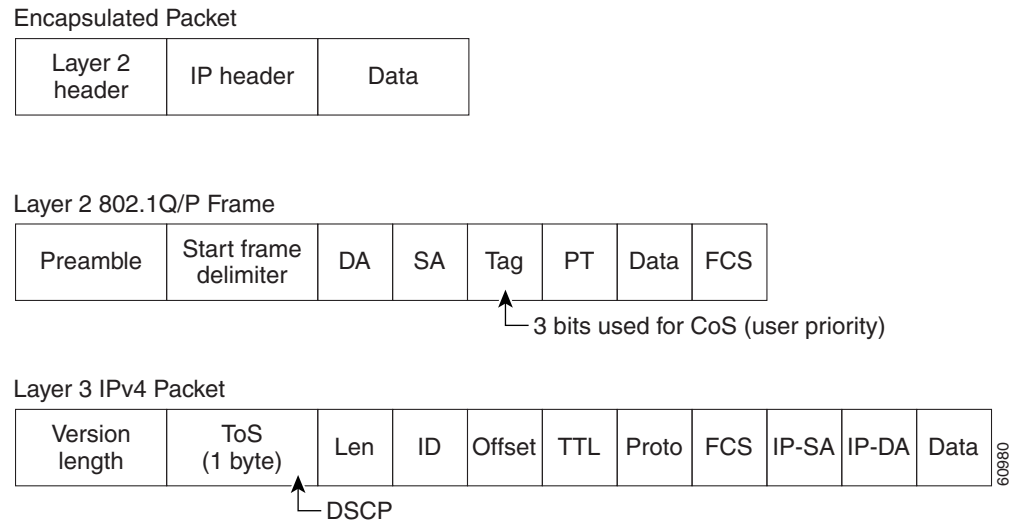
Layer 2 802.1Q frame headers have a 2-byte Tag Control Information field that carries the class of service (CoS) value in the three most-significant bits, which are called the User Priority bits. On interfaces configured as Layer 2 802.1Q trunks, all traffic is in 802.1Q frames except for traffic in 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.
- **Prioritization bits in Layer 3 packets**

Layer 3 IP packets can carry a Differentiated Services Code Point (DSCP) value. The supported DSCP values are 0, 8, 10, 16, 18, 24, 26, 32, 34, 40, 46, 48, and 56.

Figure 13-1 QoS Classification Layers in Frames and Packets



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 happen closer to the edge of the network so that the core switches and routers are not overloaded.

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 DiffServ 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 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.

Basic QoS Model

Figure 13-2 shows the basic QoS model. Actions at the ingress interface include classifying traffic, policing, and marking:



Note

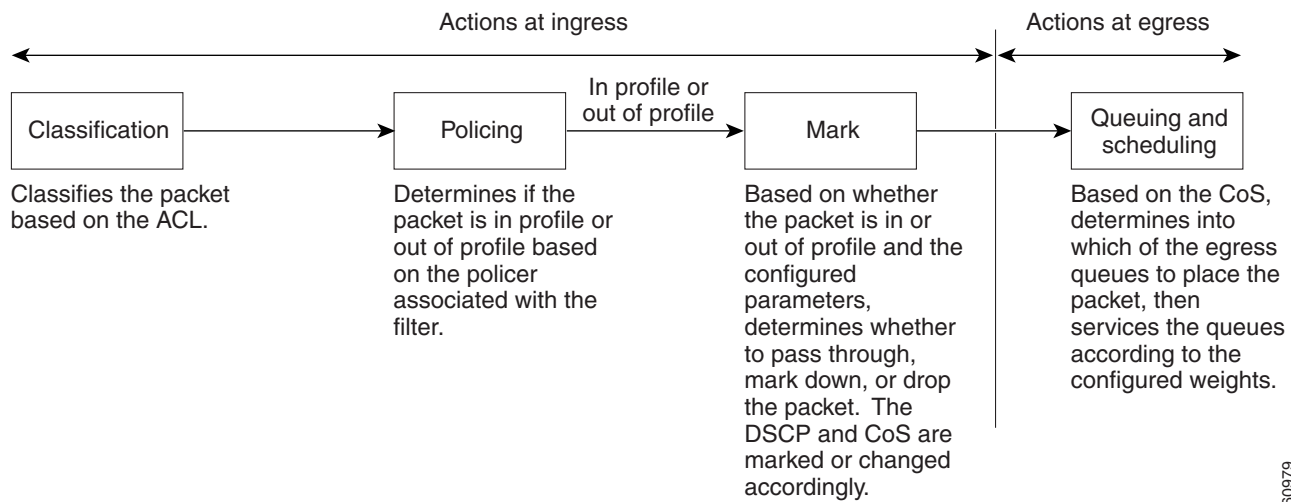
If you have the standard software image installed on your switch, only the queuing and scheduling features are available.

- Classifying distinguishes one kind of traffic from another. For more information, see the “[Classification](#)” section on page 13-4.
- Policing determines whether a packet is in or out of profile according to the configured policer, and the policer limits the bandwidth consumed by a flow of traffic. The result of this determination is passed to the marker. For more information, see the “[Policing and Marking](#)” section on page 13-6.
- Marking evaluates the policer and configuration information for the action to be taken when a packet is out of profile and decides what to do with the packet (pass through a packet without modification, mark down the DSCP value in the packet, or drop the packet). For more information, see the “[Policing and Marking](#)” section on page 13-6.

Actions at the egress interface include queuing and scheduling:

- Queuing evaluates the CoS value and determines which of the four egress queues in which to place the packet.
- Scheduling services the four egress queues based on their configured weighted round robin (WRR) weights.

Figure 13-2 Basic QoS Model



Classification



Note

This feature is available only if your switch is running the enhanced software image.

Classification is the process of distinguishing one kind of traffic from another by examining the fields in the packet.

Classification occurs only on a physical interface basis. No support exists for classifying packets at the VLAN or the switched virtual interface level.

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

Classification Based on QoS ACLs

You can use IP standard, IP extended, and Layer 2 MAC ACLs to define a group of packets with the same characteristics (*class*). In the QoS context, the permit and deny actions in the access control entries (ACEs) have different meanings than with security ACLs:

- If a match with a permit action is encountered (first-match principle), the specified QoS-related action is taken.
- If no match with a permit action is encountered and all the ACEs have been examined, no QoS processing occurs on the packet.
- If multiple ACLs are configured on an interface, the packet matches the first ACL with a permit action, and QoS processing begins.
- Configuration of a deny action is not supported in QoS ACLs on a Catalyst 2950 switch.
- System-defined masks are allowed in class maps with these restrictions:
 - A combination of system-defined and user-defined masks cannot be used in the multiple class maps that are a part of a policy map.
 - System-defined masks that are a part of a policy map must all use the same type of system mask. For example, a policy map cannot have a class map that uses the **permit tcp any any** ACE and another that uses the **permit ip any any** ACE.
 - A policy map can contain multiple class maps that all use the same user-defined mask or the same system-defined mask.

**Note**

For more information on system-defined mask, see the [“Understanding Access Control Parameters” section on page 12-4](#).

- For more information on ACL restrictions, see the [“Guidelines for Configuring ACLs on the Catalyst 2950 Switches” section on page 12-5](#).

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 Layer 2 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 isolate and name a specific traffic flow (or class) 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. 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 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 an interface.

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** global configuration command when the map is shared among many ports. When you enter the **class-map** global configuration 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 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. To make the policy map effective, you attach it to an interface by using the **service-policy** interface configuration command.

The policy map can also contain commands that define the policer, the bandwidth limitations of the traffic, and the action to take if the limits are exceeded. For more information, see the [“Policing and Marking” section on page 13-6](#).

A policy map also has these characteristics:

- A policy map can contain multiple class statements.
- A separate policy-map class can exist for each type of traffic received through an interface.
- A policy-map configuration state supersedes any actions due to an interface trust state.

For configuration information, see the [“Configuring a QoS Policy” section on page 13-13](#).

Policing and Marking



Note

This feature is available only if your switch is running the enhanced software image.

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 specifies the action to take for packets that are in or out of profile. These actions, carried out by the marker, include dropping the packet, or marking down the packet with a new value that is user-defined.

You can create this type of policer:

Individual—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 policy-map configuration command.

For non-IP traffic, you have these marking options:

- Use the port default. If the frame does not contain a CoS value, assign the default port CoS value to the incoming frame.
- Trust the CoS value in the incoming frame (configure the port to trust CoS). Layer 2 802.1Q frame headers carry the CoS value in the three most-significant bits of the Tag Control Information field. CoS values range from 0 for low priority to 7 for high priority.

The trust DSCP configurations is meaningless for non-IP traffic. If you configure a port with this option and non-IP traffic is received, the switch assigns the default port CoS value and classifies traffic based on the CoS value.

For IP traffic, you have these classification options:

- Trust the IP DSCP in the incoming packet (configure the port to trust DSCP), and assign the same DSCP to the packet for internal use. The IETF defines the 6 most-significant bits of the 1-byte Type of Service (ToS) field as the DSCP. The priority represented by a particular DSCP value is configurable. The supported DSCP values are 0, 8, 10, 16, 18, 24, 26, 32, 34, 40, 46, 48, and 56.
- Trust the CoS value (if present) in the incoming packet, and generate the DSCP by using the CoS-to-DSCP map.

When configuring policing and policers, keep these items in mind:

- By default, no policers are configured.
- Policers can only be configured on a physical port. There is no support for policing at a VLAN or switched virtual interface (SVI) level.
- Only one policer can be applied to a packet in the input direction.
- Only the average rate and committed burst parameters are configurable.
- Policing occurs on the ingress interfaces:
 - 60 policers are supported on ingress Gigabit-capable Ethernet ports.
 - 6 policers are supported on ingress 10/100 Ethernet ports.
 - Granularity for the average burst rate is 1 Mbps for 10/100 ports and 8 Mbps for Gigabit Ethernet ports.
- On an interface configured for QoS, all traffic received through the interface is classified, policed, and marked according to the policy map attached to the interface. On a trunk interface configured for QoS, traffic in *all* VLANs received through the interface is classified, policed, and marked according to the policy map attached to the interface.

**Note**

No policers can be configured on the egress interface on Catalyst 2950 switches.

Mapping Tables

**Note**

This feature is available only if your switch is running the enhanced software image.

The Catalyst 2950 switches support these types of marking to apply to the switch:

- CoS value to the DSCP value
- DSCP value to CoS value

**Note**

An interface can be configured to trust either CoS or DSCP, but not both at the same time.

Before the traffic reaches the scheduling stage, QoS uses the configurable DSCP-to-CoS map to derive a CoS value from the internal DSCP value.

The CoS-to-DSCP and DSCP-to-CoS map have default values that might or might not be appropriate for your network.

For configuration information, see the [“Configuring CoS Maps” section on page 13-21](#).

Queueing and Scheduling

**Note**

Both the enhanced and standard software images support this feature.

The Catalyst 2950 switches provide QoS-based 802.1P CoS values. QoS uses classification and scheduling to transmit network traffic from the switch in a predictable manner. QoS classifies frames by assigning priority-indexed CoS values to them and gives preference to higher-priority traffic such as telephone calls.

How Class of Service Works

Before you set up 802.1P CoS on a Catalyst 2950 that operates with the Catalyst 6000 family of switches, refer to the Catalyst 6000 documentation. There are differences in the 802.1P implementation, and they should be understood to ensure compatibility.

Port Priority

Frames received from users in the administratively-defined VLANs are classified or *tagged* for transmission to other devices. Based on rules that you define, a unique identifier (the tag) is inserted in each frame header before it is forwarded. The tag is examined and understood by each device before any broadcasts or transmissions to other switches, routers, or end stations. When the frame reaches the last switch or router, the tag is removed before the frame is transmitted to the target end station. VLANs that are assigned on trunk or access ports without identification or a tag are called *native* or *untagged* frames.

For IEEE 802.1Q frames with tag information, the priority value from the header frame is used. For native frames, the default priority of the input port is used.

Port Scheduling

Each port on the switch has a single receive queue buffer (the *ingress* port) for incoming traffic. When an untagged frame arrives, it is assigned the value of the port as its port default priority. You assign this value by using the CLI or CMS. A tagged frame continues to use its assigned CoS value when it passes through the ingress port.

CoS configures each transmit port (the *egress* port) with a normal-priority transmit queue and a high-priority transmit queue, depending on the frame tag or the port information. Frames in the normal-priority queue are forwarded only after frames in the high-priority queue are forwarded.

The Catalyst 2950 switches (802.1P user priority) have four priority queues. The frames are forwarded to appropriate queues based on priority-to-queue mapping that you defined.

CoS and WRR

The Catalyst 2950 switches support four CoS queues for each egress port. For each queue, you can specify these types of scheduling:

- Strict priority scheduling

Strict priority scheduling is based on the priority of queues. Queues can have priorities from 0 to 7, 7 being the highest. Packets in the high-priority queue always transmit first, and packets in the low-priority queue do not transmit until all the high-priority queues become empty.

- Weighted round-robin (WRR) scheduling

WRR scheduling requires you to specify a number that indicates the importance (weight) of the queue relative to the other CoS queues. WRR scheduling prevents the low-priority queues from being completely neglected during periods of high-priority traffic. The WRR scheduler transmits some packets from each queue in turn. The number of packets it transmits corresponds to the relative importance of the queue. For example, if one queue has a weight of 3 and another has a weight of 4, three packets are transmitted from the first queue for every four that are transmitted from the second queue. By using this scheduling, low-priority queues have the opportunity to transmit packets even though the high-priority queues are not empty.

Configuring QoS

Before configuring 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.

This section describes how to configure QoS on your switch:



Note

If your switch is running the standard software image, only the “[Configuring CoS and WRR](#)” and “[Displaying QoS Information](#)” sections are applicable.

- [Default QoS Configuration, page 13-9](#)
- [Configuration Guidelines, page 13-10](#)
- [Configuring Classification Using Port Trust States, page 13-10](#)
- [Configuring a QoS Policy, page 13-13](#)
- [Configuring CoS Maps, page 13-21](#)
- [Configuring CoS and WRR, page 13-23](#)
- [Displaying QoS Information, page 13-25](#)

Default QoS Configuration

[Table 13-2](#) shows the default QoS configuration.

Table 13-2 Default QoS Configuration

The default port CoS value is 0.

The default port trust state is untrusted.¹

No policy maps are configured.¹

No policers are configured.¹

No policers are configured.¹

Table 13-2 Default QoS Configuration (continued)

The default port CoS value is 0.

The default CoS-to-DSCP map is shown in [Table 13-3](#).¹

The default DSCP-to-CoS map is shown in [Table 13-4](#).¹

For default QoS and WRR values, see the “[Configuring CoS and WRR](#)” section on page 13-23.

1. Available only on a switch running the enhanced software image.

Configuration Guidelines

**Note**

These guidelines are applicable only if your switch is running the enhanced software image.

Before beginning the QoS configuration, you should be aware of this information:

- If you have EtherChannel ports configured on your switch, you must configure QoS classification, policing, mapping, and queuing on the individual physical ports that comprise the EtherChannel. You must decide whether the QoS configuration should match on all ports in the EtherChannel.
- It is not possible to match IP fragments against configured IP extended ACLs to enforce QoS. IP fragments are transmitted as best-effort. IP fragments are denoted by fields in the IP header.
- 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.
- Only one ACL per class map and only one **match** command per class map are supported. The ACL can have multiple access control entries, which are commands that match fields against the contents of the packet.
- Policy maps with ACL classification in the egress direction are not supported and cannot be attached to an interface by using the **service-policy input** *policy-map-name* interface configuration command.
- In a policy map, the class named *class-default* is not supported. The switch does not filter traffic based on the policy map defined by the **class class-default** policy-map configuration command.
- For more information on guidelines for configuring ACLs, see the “[Classification Based on QoS ACLs](#)” section on page 13-5.

Configuring Classification Using Port Trust States

This section describes how to classify incoming traffic by using port trust states:

- [Configuring the Trust State on Ports within the QoS Domain, page 13-11](#)
- [Configuring the CoS Value for an Interface, page 13-13](#)

Configuring the Trust State on Ports within the QoS Domain

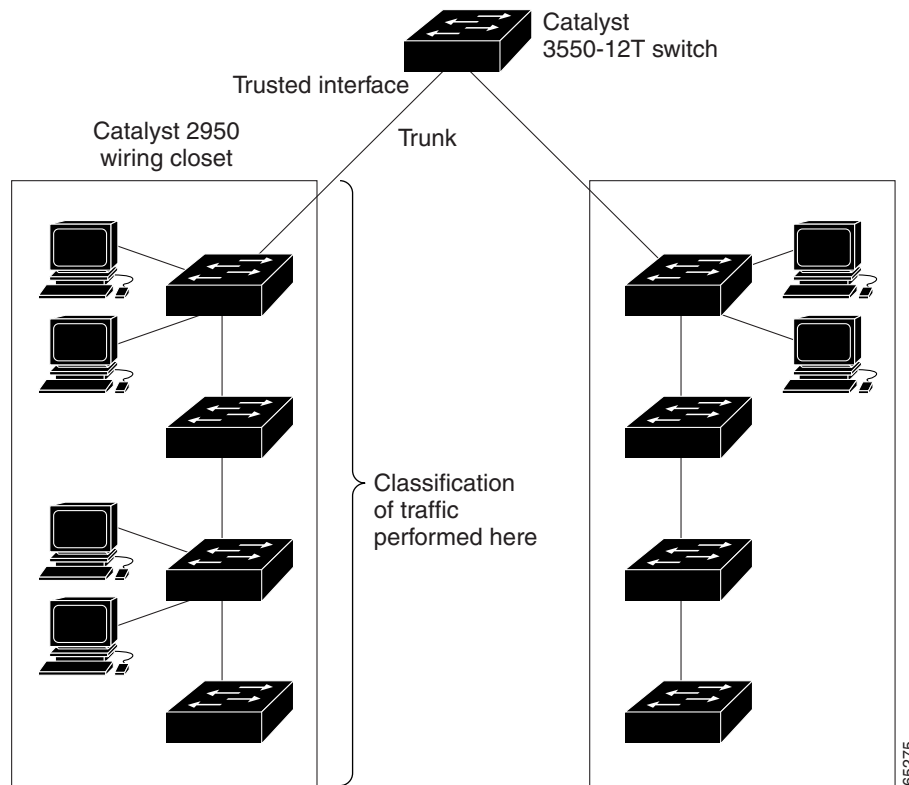


Note

This feature is available only if your switch is running the enhanced software image.

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 13-3](#) shows a sample network topology.

Figure 13-3 Port Trusted States within the QoS Domain



Beginning in privileged EXEC mode, follow these steps to configure the port to trust the classification of the traffic that it receives:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface <i>interface-id</i>	Enter interface configuration mode, and specify the interface to be trusted. Valid interfaces include physical interfaces.
Step 3	mls qos trust [cos dscp]	Configure the port trust state. By default, the port is not trusted. Use the cos keyword setting if your network is composed of Ethernet LANs, Catalyst 2950 switches, and has no more than two types of traffic. Use the dscp keyword if your network is not composed of only Ethernet LANs and if you are familiar with sophisticated QoS features and implementations. Enter the cos keyword if you want ingress packets to be classified with the packet CoS values. For tagged IP packets, the DSCP value of the packet is modified based on the CoS-to-DSCP map. The egress queue assigned to the packet is based on the packet CoS value. Enter the dscp keyword if you want ingress packets to be classified with packet DSCP values. For non-IP packets, the packet CoS value is used for tagged packets; the default port CoS is used for untagged packets. Internally, the switch modifies the CoS value by using the DSCP-to-CoS map. For more information on this command, refer to the <i>Catalyst 2950 Desktop Switch Command Reference</i> .
Step 4	end	Return to privileged EXEC mode.
Step 5	show mls qos interface [<i>interface-id</i>] [policers]	Verify your entries.
Step 6	copy running-config startup-config	(Optional) Save your entries in the configuration file.

To return a port to its untrusted state, use the **no mls qos trust** interface configuration command.

For information on how to change the default CoS value, see the [“Configuring the CoS Value for an Interface”](#) section on page 13-13. For information on how to configure the CoS-to-DSCP map, see the [“Configuring the CoS-to-DSCP Map”](#) section on page 13-21.

Configuring the CoS Value for an Interface



Note

Both the enhanced and standard software images support this feature.

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:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface <i>interface-id</i>	Enter interface configuration mode, and specify the interface to be trusted. Valid interfaces include physical interfaces.
Step 3	mls qos cos { <i>default-cos</i> override }	Configure the default CoS value for the port. For <i>default-cos</i> , specify a default CoS value to be assigned to a port. If the port is CoS trusted and packets are untagged, the default CoS value becomes the CoS value for the packet. 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 packets and to apply the default port CoS value to all incoming packets. By default, CoS override is disabled. Use the override keyword when all incoming packets on certain ports deserve higher priority than packets entering from other ports. Even if a port was previously set to trust DSCP, 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 egress port.
Step 4	end	Return to privileged EXEC mode.
Step 5	show mls qos interface	Verify your entries.
Step 6	copy running-config startup-config	(Optional) Save your entries in the configuration file.

To return to the default setting, use the **no mls qos cos** {*default-cos* | **override**} interface configuration command.

Configuring a QoS Policy



Note

This feature is available only if your switch is running the enhanced software image.

Configuring a QoS policy typically requires classifying traffic into classes, configuring policies applied to those traffic classes, and attaching policies to interfaces.

For background information, see the [“Classification” section on page 13-4](#) and the [“Policing and Marking” section on page 13-6](#).

This section contains this configuration information:

- [Classifying Traffic by Using ACLs, page 13-14](#)
- [Classifying Traffic by Using Class Maps, page 13-17](#)
- [Classifying, Policing, and Marking Traffic by Using Policy Maps, page 13-18](#)

Classifying Traffic by Using ACLs

You can classify IP traffic by using IP standard or IP extended ACLs; you can classify Layer 2 traffic by using Layer 2 MAC ACLs.

Beginning in privileged EXEC mode, follow these steps to create an IP standard ACL for IP traffic:

	Command	Purpose
Step 1	<code>configure terminal</code>	Enter global configuration mode.
Step 2	<code>access-list access-list-number {deny permit remark} {source source-wildcard host source any}</code>	<p>Create an IP standard ACL, repeating the command as many times as necessary.</p> <p>For <i>access-list-number</i>, enter the ACL number. The range is 1 to 99 and 1300 to 1999.</p> <p>Enter deny or permit to specify whether to deny or permit access if The <i>source</i> is the source address of the network or host from which the packet is being sent, specified in one of three ways:</p> <ul style="list-style-type: none"> • The 32-bit quantity in dotted-decimal format. • The keyword any as an abbreviation for <i>source</i> and <i>source-wildcard</i> of 0.0.0.0 255.255.255.255. You do not need to enter a source-wildcard. • The keyword host as an abbreviation for source and source-wildcard of <i>source</i> 0.0.0.0. <p>(Optional) The <i>source-wildcard</i> applies wildcard bits to the source (see first bullet item).</p> <p>Note Deny statements are not supported for QoS ACLS. See the “Classification Based on QoS ACLs” section on page 13-5 for more details.</p>
Step 3	<code>end</code>	Return to privileged EXEC mode.
Step 4	<code>show access-lists</code>	Verify your entries.
Step 5	<code>copy running-config startup-config</code>	(Optional) Save your entries in the configuration file.

To delete an ACL, use the **no access-list access-list-number** global configuration command.

This example shows how to allow access for only those hosts on the two 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 ACL statements is rejected.

```
Switch(config)# access-list 1 permit 192.5.255.0 0.0.0.255
Switch(config)# access-list 1 permit 36.0.0.0 0.0.0.255
```

Beginning in privileged EXEC mode, follow these steps to create an IP extended ACL for IP traffic:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	access-list <i>access-list-number</i> { deny permit remark } <i>protocol</i> { <i>source source-wildcard</i> host source any } [<i>operator port</i>] { <i>destination</i> <i>destination-wildcard</i> host destination any } [<i>operator port</i>]	<p>Create an IP extended ACL, repeating the command as many times as necessary.</p> <p>For <i>access-list-number</i>, enter the ACL number. The range is 100 to 199 and 2000 to 2699.</p> <p>Enter deny or permit to specify whether to deny or permit access if conditions are matched.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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> <p>Define a destination or source port.</p> <ul style="list-style-type: none"> • The <i>operator</i> can be only eq (equal). • If operator is after <i>source source-wildcard</i>, conditions match when the source port matches the defined port. • If operator is after <i>destination destination-wildcard</i>, conditions match when the destination port matches the defined port. • The <i>port</i> is a decimal number or name of a TCP or UDP port. The number can be from 0 to 65535. • Use TCP port names only for TCP traffic. • Use UDP port names only for UDP traffic. <p>Note Deny statements are not supported for QoS ACLS. See the “Classification Based on QoS ACLs” section on page 13-5 for more details.</p>
Step 3	end	Return to privileged EXEC mode.
Step 4	show access-lists	Verify your entries.
Step 5	copy running-config startup-config	(Optional) Save your entries in the configuration file.

To delete an ACL, use the **no access-list** *access-list-number* global configuration command.

This example shows how to create an ACL that permits only TCP traffic from the destination IP address 128.88.1.2 with TCP port number 25:

```
Switch(config)# access-list 102 permit tcp 0.0.0.0 255.255.255.255 128.88.1.2 0.0.0.0 eq 25
```

Beginning in privileged EXEC mode, follow these steps to create a Layer 2 MAC ACL for Layer 2 traffic:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	mac access-list extended <i>name</i>	Create a Layer 2 MAC ACL by specifying the name of the list. After entering this command, the mode changes to extended MAC ACL configuration.
Step 3	{deny permit} {any host <i>source MAC address</i> {any host <i>destination MAC address</i> [aarp amber dec-spanning decnet-iv diagnostic dsm etype-6000 etype-8042 lat lavc-sca mop-console mop-dump msdos mumps netbios vines-echo vines-ip xns-idp]	Enter deny or permit to specify whether to deny or permit access if conditions are matched. 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> 255.255.255, or by using the host keyword for <i>source</i> 0.0.0. 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-wildcard</i> 255.255.255, or by using the host keyword for <i>source</i> 0.0.0. (Optional) You can also enter these options: aarp amber dec-spanning decnet-iv diagnostic dsm etype-6000 etype-8042 lat lavc-sca mop-console mop-dump msdos mumps netbios vines-echo vines-ip xns-idp (a non-IP protocol). Note Deny statements are not supported for QoS ACLS. See the “Classification Based on QoS ACLs” section on page 13-5 for more details.
Step 4	end	Return to privileged EXEC mode.
Step 5	show access-lists [<i>number</i> <i>name</i>]	Verify your entries.
Step 6	copy running-config startup-config	(Optional) Save your entries in the configuration file.

To delete an ACL, use the **no mac access-list extended** *access-list-name* global configuration command.

This example shows how to create a Layer 2 MAC ACL with a permit statement. The statement allows traffic from the host with MAC address 0001.0000.0001 to the host with MAC address 0002.0000.0001.

```
Switch(config)# mac access-list extended maclist1
Switch(config-ext-macl)# permit host 0001.0000.0001 host 0002.0000.0001
```

Classifying Traffic by Using Class Maps

You use the **class-map** global configuration command to isolate a specific traffic flow (or class) from all other traffic and to name it. The class map defines the criteria to use to match against a specific traffic flow to further classify it. Match statements can include criterion such as an ACL, IP precedence values, 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. For more information, see the “[Classifying, Policing, and Marking Traffic by Using Policy Maps](#)” section on page 13-18.

Beginning in privileged EXEC mode, follow these steps to create a class map and to define the match criterion to classify traffic:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	access-list <i>access-list-number</i> { deny permit } { <i>source source-wildcard</i> host source any } or access-list <i>access-list-number</i> { deny permit remark } <i>protocol</i> { <i>source source-wildcard</i> host source any } [<i>operator port</i>] { <i>destination destination-wildcard</i> host destination any } [<i>operator port</i>] or mac access-list extended <i>name</i> { deny permit } { any host source MAC address any host destination MAC address } [aarp amber dec-spanning decnet-iv diagnostic dsm etype-6000 etype-8042 lat lavc-sca mop-console mop-dump msdos mumps netbios vines-echo vines-ip xns-idp]	Create an IP standard or extended ACL for IP traffic or a Layer 2 MAC ACL for non-IP traffic, repeating the command as many times as necessary. For more information, see the “ Classifying Traffic by Using ACLs ” section on page 13-14. For more information on this command, see the “ Creating Named MAC Extended ACLs ” section on page 12-20. Note Deny statements are not supported for QoS ACLs. See the “ Classification Based on QoS ACLs ” section on page 13-5 for more details.
Step 3	class-map <i>class-map-name</i>	Create a class map, and enter class-map configuration mode. By default, no class maps are defined. For <i>class-map-name</i> , specify the name of the class map.
Step 4	match { access-group <i>acl-index</i> name <i>acl-name</i> }	Define the match criterion to classify traffic. By default, no match criterion is supported. Only one match criterion per class map is supported, and only one ACL per class map is supported. For access-group <i>acl-index</i> name <i>acl-name</i> , specify the number or name of the ACL created in Step 3.

	Command	Purpose
Step 5	end	Return to privileged EXEC mode.
Step 6	show class-map [<i>class-map-name</i>]	Verify your entries.
Step 7	copy running-config startup-config	(Optional) Save your entries in the configuration file.

To delete an existing class map, use the **no class-map** *class-map-name* global configuration command. To remove a match criterion, use the **no match** {*acl-index* | **name** *acl-name*} class-map configuration command.

This example shows how to configure the class map called *class1*. The *class1* has one match criterion, which is an ACL called *103*.

```
Switch(config)# access-list 103 permit any any tcp eq 80
Switch(config)# class-map class1
Switch(config-cmap)# match access-group 103
Switch(config-cmap)# end
Switch#
```

Classifying, Policing, and Marking Traffic by Using Policy Maps

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; 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 separate policy-map class can exist for each type of traffic received through an interface.

You can attach only one policy map per interface in the input direction.

Beginning in privileged EXEC mode, follow these steps to create a policy map:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	<p>access-list <i>access-list-number</i> { deny permit } { <i>source source-wildcard</i> host source any }</p> <p>or</p> <p>access-list <i>access-list-number</i> { deny permit remark } <i>protocol</i> { <i>source source-wildcard</i> host source any } [<i>operator port</i>] { <i>destination destination-wildcard</i> host destination any } [<i>operator port</i>]</p> <p>or</p> <p>mac access-list extended <i>name</i></p> <p>(deny permit) { any host source MAC address } { any host destination MAC address } [aarp amber dec-spanning decnet-iv diagnostic dsm etype-6000 etype-8042 lat lvc-sca mop-console mop-dump msdos mumps netbios vines-echo vines-ip xns-idp]</p>	<p>Create an IP standard or extended ACL for IP traffic or a Layer 2 MAC ACL for non-IP traffic, repeating the command as many times as necessary.</p> <p>For more information, see the “Classifying Traffic by Using ACLs” section on page 13-14.</p> <p>Note Deny statements are not supported for QoS ACLS. See the “Classification Based on QoS ACLs” section on page 13-5 for more details.</p> <p>For more information on this command, see the “Creating Named MAC Extended ACLs” section on page 12-20.</p>
Step 3	policy-map <i>policy-map-name</i>	<p>Create a policy map by entering the policy map name, and enter 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>
Step 4	class <i>class-map-name</i> [access-group <i>acl-index-or-name</i>]	<p>Define a traffic classification, and enter 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>For access-group <i>acl-index-or-name</i>, specify the number or name of the ACL created in Step 2.</p> <p>Note In a policy map, the class named <i>class-default</i> is not supported. The switch does not filter traffic based on the policy map defined by the class class-default policy-map configuration command.</p>
Step 5	set { ip dscp <i>new-dscp</i> }	<p>Classify IP traffic by setting a new value in the packet.</p> <p>For ip dscp <i>new-dscp</i>, enter a new DSCP value to be assigned to the classified traffic. The supported DSCP values are 0, 8, 10, 16, 18, 24, 26, 32, 34, 40, 46, 48, and 56.</p>

	Command	Purpose
Step 6	police <i>rate-bps burst-byte</i> [exceed-action { drop dscp <i>dscp-value</i> }]	<p>Define a policer for the classified traffic.</p> <p>You can configure up to 60 policers on ingress Gigabit-capable Ethernet ports and up to 6 policers on ingress 10/100 Ethernet ports.</p> <p>For <i>rate-bps</i>, specify average traffic rate in bits per second (bps). The range is 1 Mbps to 100 Mbps for 10/100 Ethernet ports and 8 Mbps to 1000 Mbps for the Gigabit-capable Ethernet ports.</p> <p>For <i>burst-byte</i>, specify the normal burst size in bytes. The values supported on the 10/100 ports are 4096, 8192, 16384, 32768, and 65536. The values supported on the Gigabit-capable Ethernet ports are 4096, 8192, 16348, 32768, 65536, 131072, 262144, and 524288.</p> <p>(Optional) Specify the action to take when the rates are exceeded. Use the exceed-action drop keywords to drop the packet. Use the exceed-action dscp <i>dscp-value</i> keywords to mark down the DSCP value and transmit the packet.</p>
Step 7	exit	Return to policy-map configuration mode.
Step 8	exit	Return to global configuration mode.
Step 9	interface <i>interface-id</i>	<p>Enter interface configuration mode, and specify the interface to attach to the policy map.</p> <p>Valid interfaces include physical interfaces.</p>
Step 10	service-policy { input <i>policy-map-name</i> }	<p>Apply a policy map to the input of a particular interface.</p> <p>Only one policy map per interface per direction is supported.</p> <p>Use input <i>policy-map-name</i> to apply the specified policy map to the input of an interface.</p>
Step 11	end	Return to privileged EXEC mode.
Step 12	show policy-map [<i>policy-map-name</i> class <i>class-name</i>]	Verify your entries.
Step 13	copy running-config startup-config	(Optional) Save your entries in the configuration file.

To delete an existing policy map, use the **no policy-map** *policy-map-name* global configuration command. To delete an existing class map, use the **no class** *class-map-name* policy-map configuration command. To remove an assigned DSCP value, use the **no set** {**ip dscp** *new-dscp*} policy-map configuration command. To remove an existing policer, use the **no police** *rate-bps burst-byte* [**exceed-action** {**drop** | **dscp** *dscp-value*}] policy-map configuration command. To remove the policy map and interface association, use the **no service-policy** {**input** *policy-map-name*} interface configuration command.

This example shows how to create a policy map and attach it to an ingress interface. 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 bps and a normal burst size of 8000 bytes, its DSCP is marked down to a value of 10 and transmitted.

```
Switch(config)# access-list 1 permit 10.1.0.0 0.0.255.255
Switch(config)# class-map ipclass1
Switch(config-cmap)# match access-group 1
Switch(config-cmap)# exit
Switch(config)# policy-map flow1t
Switch(config-pmap)# class ipclass1
Switch(config-pmap-c)# police 5000000 8192 exceed-action dscp 10
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport mode access
Switch(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 interface. 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.

```
Switch(config)# mac access-list extended maclist1
Switch(config-ext-mac)# permit host 0001.0000.0001 host 0002.0000.0001
Switch(config-ext-mac)# exit
Switch(config)# mac access-list extended maclist2
Switch(config-ext-mac)# permit host 0001.0000.0003 host 0002.0000.0003
Switch(config-ext-mac)# exit
Switch(config)# class-map macclass1
Switch(config-cmap)# match access-group name maclist1
Switch(config-cmap)# exit
Switch(config)# policy-map macpolicy1
Switch(config-pmap)# class macclass1
Switch(config-pmap-c)# set ip dscp 56
Switch(config-pmap-c)# exit
Switch(config-pmap)# class macclass2 maclist2
Switch(config-pmap-c)# set ip dscp 48
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport mode trunk
Switch(config-if)# mls qos trust cos
Switch(config-if)# service-policy input macpolicy1
```

Configuring CoS Maps



Note

This feature is available only if your switch is running the enhanced software image.

This section describes how to configure the DSCP maps:

- [Configuring the CoS-to-DSCP Map, page 13-21](#)
- [Configuring the DSCP-to-CoS Map, page 13-22](#)

All the maps are globally defined.

Configuring the CoS-to-DSCP Map

You use the CoS-to-DSCP map to map CoS values in incoming packets to a DSCP value that QoS uses internally to represent the priority of the traffic.

[Table 13-3](#) shows the default CoS-to-DSCP map.

Table 13-3 Default CoS-to-DSCP Map

CoS value	0	1	2	3	4	5	6	7
DSCP value	0	8	16	24	32	40	48	56

If these values are not appropriate for your network, you need to modify them.

Beginning in privileged EXEC mode, follow these steps to modify the CoS-to-DSCP map:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	mls qos map cos-dscp dscp1...dscp8	Modify the CoS-to-DSCP map. For <i>dscp1...dscp8</i> , enter 8 DSCP values that correspond to CoS values 0 to 7. Separate each DSCP value with a space. The supported DSCP values are 0, 8, 10, 16, 18, 24, 26, 32, 34, 40, 46, 48, and 56.
Step 3	end	Return to privileged EXEC mode.
Step 4	show mls qos maps cos-dscp	Verify your entries.
Step 5	copy running-config startup-config	(Optional) Save your entries in the configuration file.

To return to the default map, use the **no mls qos map cos-dscp** global configuration command.

This example shows how to modify and display the CoS-to-DSCP map:

```
Switch# configure terminal
Switch(config)# mls qos map cos-dscp 8 8 8 8 24 32 56 56
Switch(config)# end
Switch# show mls qos maps cos-dscp

Cos-dscp map:
  cos:  0  1  2  3  4  5  6  7
-----
  dscp:  8  8  8  8 24 32 56 56
```

Configuring the DSCP-to-CoS Map

You use the DSCP-to-CoS map to map DSCP values in incoming packets to a CoS value, which is used to select one of the four egress queues.

The Catalyst 2950 switches support these DSCP values: 0, 8, 10, 16, 18, 24, 26, 32, 34, 40, 46, 48, and 56.

Table 13-4 shows the default DSCP-to-CoS map.

Table 13-4 Default DSCP-to-CoS Map

DSCP values	0	8, 10	16, 18	24, 26	32, 34	40, 46	48	56
CoS values	0	1	2	3	4	5	6	7

If these values are not appropriate for your network, you need to modify them.

Beginning in privileged EXEC mode, follow these steps to modify the DSCP-to-CoS map:

	Command	Purpose
Step 1	<code>configure terminal</code>	Enter global configuration mode.
Step 2	<code>mls qos map dscp-cos dscp-list to cos</code>	Modify the DSCP-to-CoS map. For <i>dscp-list</i> , enter up to 13 DSCP values separated by spaces. Then enter the to keyword. For <i>cos</i> , enter the CoS value to which the DSCP values correspond. The supported DSCP values are 0, 8, 10, 16, 18, 24, 26, 32, 34, 40, 46, 48, and 56. The CoS range is 0 to 7.
Step 3	<code>end</code>	Return to privileged EXEC mode.
Step 4	<code>show mls qos maps dscp-to-cos</code>	Verify your entries.
Step 5	<code>copy running-config startup-config</code>	(Optional) Save your entries in the configuration file.

To return to the default map, use the **no mls qos map dscp-cos** global configuration command.

This example shows how the DSCP values 26 and 48 are mapped to CoS value 7. For the remaining DSCP values, the DSCP-to-CoS mapping is the default.

```
Switch(config)#mls qos map dscp-cos 26 48 to 7
Switch(config)#exit

Switch#show mls qos maps dscp-cos

Dscp-cos map:
  dscp:  0  8 10 16 18 24 26 32 34 40 46 48 56
-----
  cos:  0  1  1  2  2  3  7  4  4  5  5  7  7
```

Configuring CoS and WRR



Note

Both the enhanced and standard software images support this feature.

This section describes how to configure CoS priorities and weighted round-robin (WRR):

- [CLI: Configuring CoS Priority Queues, page 13-24](#)
- [Configuring WRR, page 13-24](#)

CLI: Configuring CoS Priority Queues

Beginning in privileged EXEC mode, follow these steps to configure the CoS priority queues:

	Command	Purpose										
Step 1	configure terminal	Enter global configuration mode.										
Step 2	wrr-queue cos-map <i>qid cos1..cosn</i>	Specify the queue id of the CoS priority queue. (Ranges are 1 to 4 where 1 is the lowest CoS priority queue.) Specify the CoS values that are mapped to the queue id. Default values are as follows: <table border="1"> <thead> <tr> <th>CoS Value</th> <th>CoS Priority Queues</th> </tr> </thead> <tbody> <tr> <td>0, 1</td> <td>1</td> </tr> <tr> <td>2, 3</td> <td>2</td> </tr> <tr> <td>4, 5</td> <td>3</td> </tr> <tr> <td>6, 7</td> <td>4</td> </tr> </tbody> </table>	CoS Value	CoS Priority Queues	0, 1	1	2, 3	2	4, 5	3	6, 7	4
CoS Value	CoS Priority Queues											
0, 1	1											
2, 3	2											
4, 5	3											
6, 7	4											
Step 3	end	Return to privileged EXEC mode.										
Step 4	show wrr-queue cos-map	Display the mapping of the CoS priority queues.										

To disable the new CoS settings and return to default settings, use the **no wrr-queue cos-map** global configuration command.

Configuring WRR

Beginning in privileged EXEC mode, follow these steps to configure the WRR priority:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	wrr-queue bandwidth <i>weight1...weight4</i>	Assign WRR weights to the four CoS queues. (Ranges for the WRR values are 1 to 255.)
Step 3	end	Return to privileged EXEC mode.
Step 4	show wrr-queue bandwidth	Display the WRR bandwidth allocation for the CoS priority queues.

To disable the WRR scheduler and enable the strict priority scheduler, use the **no wrr-queue bandwidth** global configuration command.

Displaying QoS Information

To display the current QoS information, use one or more of the privileged EXEC commands in [Table 13-5](#):

Table 13-5 Commands for Displaying QoS Information

Command	Purpose
<code>show class-map [class-map-name]¹</code>	Display QoS class maps, which define the match criteria to classify traffic.
<code>show policy-map [policy-map-name [class class-name]]¹</code>	Display QoS policy maps, which define classification criteria for incoming traffic.
<code>show mls qos maps [cos-dscp dscp-cos]¹</code>	Display QoS mapping information. Maps are used to generate an internal DSCP value, which represents the priority of the traffic.
<code>show mls qos interface [interface-id] [policers]¹</code>	Display QoS information at the interface level, including the configuration of the egress queues and the CoS-to-egress-queue map, which interfaces have configured policers, and ingress and egress statistics (including the number of bytes dropped). ²
<code>show mls masks [qos security]¹</code>	Display details regarding the masks ³ used for QoS and security ACLs.
<code>show wrr-queue cos-map</code>	Display the mapping of the CoS priority queues.
<code>show wrr-queue bandwidth</code>	Display the WRR bandwidth allocation for the CoS priority queues.

1. Available only on a switch running the enhanced software image.
2. You can define up to 16 DSCP values for which byte or packet statistics are gathered by hardware by using the `mls qos monitor {bytes | dscp dscp1 ... dscp8 | packets}` interface configuration command and the `show mls qos interface statistics` privileged EXEC command.
3. Access Control Parameters are called masks in the switch CLI commands and output.

This example shows how to display the DSCP-to-CoS maps:

```
Switch# show mls qos maps dscp-cos

Dscp-cos map:
  dscp:  0  8 10 16 18 24 26 32 34 40 46 48 56
-----
  cos:   0  1  1  2  2  3  3  4  4  5  5  6  7
```

QoS Configuration Examples



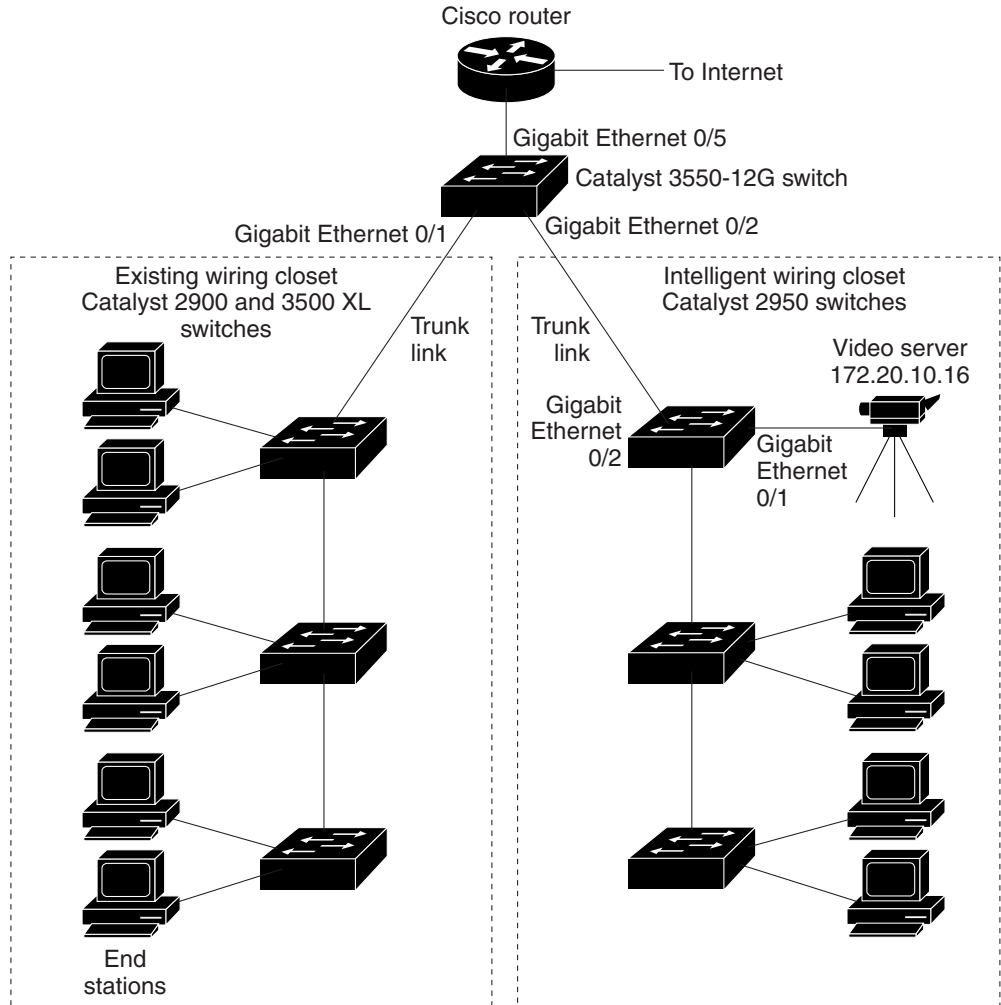
Note

These examples are applicable only if your switch is running the enhanced software image.

This section provides a QoS migration path to help you quickly implement QoS features based on your existing network and planned changes to your network, as shown in [Figure 13-4](#). It contains this information:

- [QoS Configuration for the Common Wiring Closet, page 13-26](#)
- [QoS Configuration for the Intelligent Wiring Closet, page 13-27](#)

Figure 13-4 QoS Configuration Example Network



QoS Configuration for the Common Wiring Closet

The common wiring closet in [Figure 13-4](#) consists of existing Catalyst 2900 XL and 3500 XL switches. These switches are running IOS release 12.0(5)XP or later, which supports the QoS-based IEEE 802.1P CoS values. QoS classifies frames by assigning priority-indexed CoS values to them and gives preference to higher-priority traffic.

Recall that on the Catalyst 2900 and 3500 XL switches, you can classify untagged (native) Ethernet frames at the ingress ports by setting a default CoS priority (**switchport priority default default-priority-id** interface configuration command) for each port. For IEEE 802.1Q frames with tag information, the priority value from the header frame is used. On the Catalyst 3524-PWR XL and 3548 XL switches, you can override this priority with the default value by using the **switchport priority default override** interface configuration command. For Catalyst 2950 and Catalyst 2900 XL switches and other 3500 XL models that do not have the override feature, the Catalyst 3550-12T switch at the distribution layer can override the 802.1P CoS value by using the **mls qos cos override** interface configuration command.

For the Catalyst 2900 and 3500 XL switches, CoS configures each transmit port (the egress port) with a normal-priority transmit queue and a high-priority transmit queue, depending on the frame tag or the port information. Frames in the normal-priority queue are forwarded only after frames in the high-priority queue are forwarded. Frames that have 802.1P CoS values of 0 to 3 are placed in the normal-priority transmit queue while frames with CoS values of 4 to 7 are placed in the expedite (high-priority) queue.

QoS Configuration for the Intelligent Wiring Closet

The intelligent wiring closet in [Figure 13-4](#) is composed of Catalyst 2950 switches. One of the switches is connected to a video server, which has an IP address of 172.20.10.16.

The object of this example is to prioritize the video traffic over all other traffic. To do so, a DSCP of 46 is assigned to the video traffic. This traffic is stored in queue 4, which is serviced more frequently than the other queues.

Beginning in privileged EXEC mode, follow these steps to configure the switch to prioritize video packets over all other traffic:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	access-list 1 permit 172.20.10.16	Define an IP standard ACL, and permit traffic from the video server at 172.20.10.16.
Step 3	class-map videoclass	Create a class map called <i>videoclass</i> , and enter class-map configuration mode.
Step 4	match access-group 1	Define the match criterion by matching the traffic specified by ACL 1.
Step 5	exit	Return to global configuration mode.
Step 6	policy-map videopolicy	Create a policy map called <i>videopolicy</i> , and enter policy-map configuration mode.
Step 7	class videoclass	Specify the class on which to act, and enter policy-map class configuration mode.
Step 8	set ip dscp 46	For traffic matching ACL 1, set the DSCP of incoming packets to 46.
Step 9	police 5000000 8192 exceed-action drop	Define a policer for the classified video traffic to drop traffic that exceeds 5-Mbps average traffic rate with a 8-K burst size.
Step 10	exit	Return to policy-map configuration mode.
Step 11	exit	Return to global configuration mode.
Step 12	interface gigabitethernet0/1	Enter interface configuration mode, and specify the ingress interface.
Step 13	service-policy input videopolicy	Apply the policy to the ingress interface.
Step 14	exit	Return to global configuration mode.
Step 15	interface gigabitethernet0/2	Enter interface configuration mode, and specify the egress interface (to configure the queues).
Step 16	wrr-queue bandwidth 1 2 3 4	Assign a higher WRR weight to queue 4.
Step 17	wrr-queue cos-map 4 6 7	Configure the CoS-to-egress-queue map so that CoS values 6 and 7 select queue 4.

	Command	Purpose
Step 18	end	Return to privileged EXEC mode.
Step 19	show class-map videoclass show policy-map videopolicy show mls qos maps [cos-dscp dscp-cos]	Verify your entries.
Step 20	copy running-config startup-config	(Optional) Save your entries in the configuration file.