



## 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 traffic at the expense of others. Without QoS, the switch offers best-effort service to each packet, regardless of the packet contents or size. It sends the packets without any assurance of reliability, delay bounds, or throughput.



### Note

---

For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 3550 Multilayer Switch Command Reference* for this release.

---

This chapter consists of these sections:

- [Understanding QoS, page 27-1](#)
- [Configuring QoS, page 27-18](#)
- [Displaying QoS Information, page 27-56](#)
- [QoS Configuration Examples, page 27-56](#)



### Note

---

When you are configuring QoS parameters for the switch, in order to allocate system resources to maximize the number of possible QoS access control entries (ACEs) allowed, you can use the **sdm prefer access** global configuration command to set the Switch Database Management feature to the access template. For more information on the SDM templates, see the [“Optimizing System Resources for User-Selected Features”](#) section on page 7-58.

---

## Understanding QoS

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 27-1](#):

- Prioritization values in Layer 2 frames:

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 interfaces 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 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:

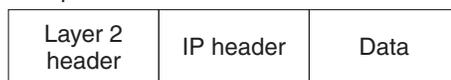
Layer 3 IP packets can carry either an IP precedence value or a Differentiated Services Code Point (DSCP) value. QoS supports the use of either value because DSCP values are backward-compatible with IP precedence values.

IP precedence values range from 0 to 7.

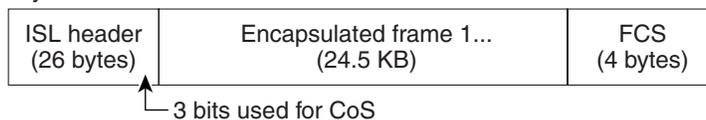
DSCP values range from 0 to 63.

**Figure 27-1 QoS Classification Layers in Frames and Packets**

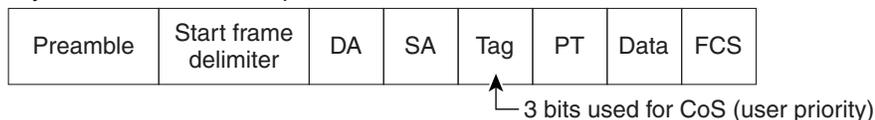
Encapsulated Packet



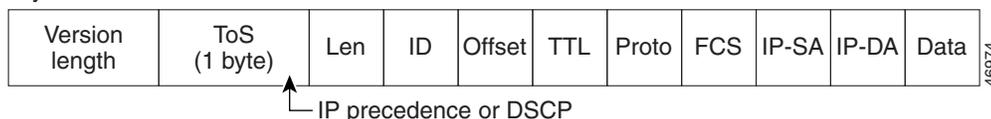
Layer 2 ISL Frame



Layer 2 802.1Q and 802.1p Frame



Layer 3 IPv4 Packet



**Note**

Layer 3 IPv6 packets are treated as non-IP packets and are bridged by the switch.

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 27-2 shows the basic QoS model. Actions at the ingress interface include classifying traffic, policing, and marking:

- Classifying distinguishes one kind of traffic from another. The process generates an internal DSCP for a packet, which identifies all the future QoS actions to be performed on this packet. For more information, see the “[Classification](#)” section on page 27-4.
- Policing determines whether a packet is in or out of profile by comparing the internal DSCP 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 27-8.
- 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 27-8.

Actions at the egress interface include queueing and scheduling:

- Queueing evaluates the internal DSCP and determines which of the four egress queues in which to place the packet. The DSCP value is mapped to a CoS value, which selects one of the queues.
- Scheduling services the four egress queues based on their configured weighted round robin (WRR) weights and thresholds. One of the queues can be the expedite queue, which is serviced until empty before the other queues are serviced. Congestion avoidance techniques include tail drop and Weighted Random Early Detection (WRED) on Gigabit-capable Ethernet ports and tail drop (with only one threshold) on 10/100 Ethernet ports.



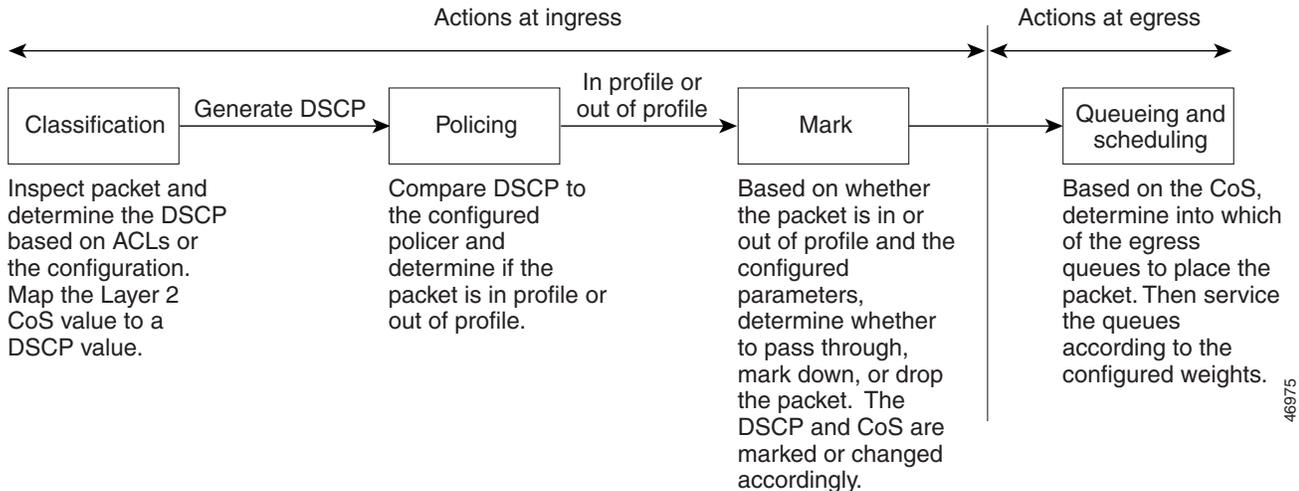
---

**Note**

Policing and marking can also occur on egress interfaces.

---

Figure 27-2 Basic QoS Model



## Classification

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.



### Note

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

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

For non-IP traffic, you have these classification options as shown in [Figure 27-3](#):

- Use the port default. If the frame does not contain a CoS value, assign the default port CoS value to the incoming frame. Then use the configurable CoS-to-DSCP map to generate the internal DSCP value.
- Trust the CoS value in the incoming frame (configure the port to trust CoS). Then use the configurable CoS-to-DSCP map to generate the internal DSCP value. Layer 2 ISL frame headers carry the CoS value in the three least-significant bits of the 1-byte User field. 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 and trust IP precedence 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 the default port CoS value and generates the internal DSCP from the CoS-to-DSCP map.

- Perform the classification based on the configured Layer 2 MAC access control list (ACL), which can examine the MAC source address, the MAC destination address, and the Ethertype field. If no ACL is configured, the packet is assigned the default DSCP of 0, which means best-effort traffic; otherwise, the policy map specifies the DSCP to assign to the incoming frame.

For IP traffic, you have these classification options as shown in [Figure 27-3](#):

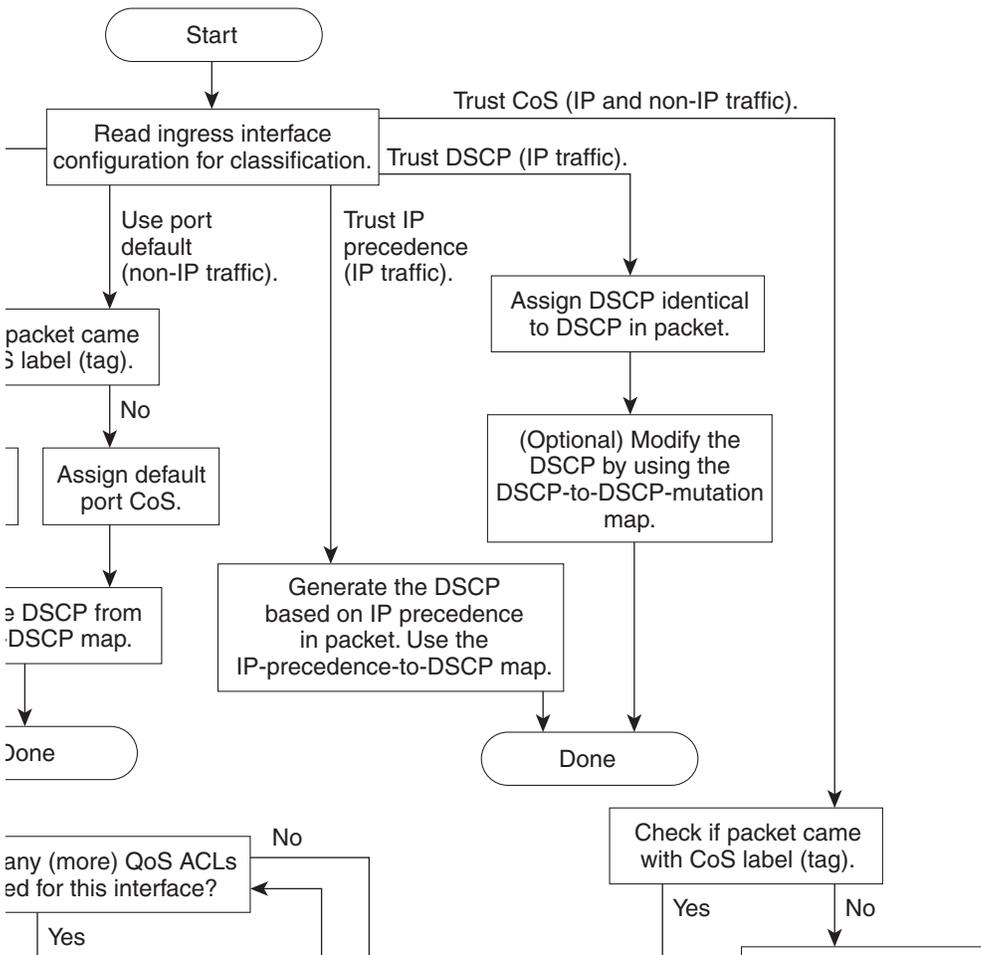
- Trust the IP DSCP in the incoming packet (configure the port to trust DSCP), and assign the same DSCP to the packet for internal use. The IETF defines the 6 most-significant bits of the 1-byte Type of Service (ToS) field as the DSCP. The priority represented by a particular DSCP value is configurable. DSCP values range from 0 to 63.

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 IP precedence in the incoming packet (configure the port to trust IP precedence), and generate a DSCP by using the configurable IP-precedence-to-DSCP map. The IP version 4 specification defines the three most-significant bits of the 1-byte ToS field as the IP precedence. IP precedence values range from 0 for low priority to 7 for high priority.
- Trust the CoS value (if present) in the incoming packet, and generate the DSCP by using the CoS-to-DSCP map.
- 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 the default DSCP of 0, which means best-effort traffic; otherwise, the policy map specifies the DSCP to assign to the incoming frame.

For information on the maps described in this section, see the [“Mapping Tables” section on page 27-11](#). For configuration information on port trust states, see the [“Configuring Classification Using Port Trust States” section on page 27-21](#).

Figure 27-3 Classification Flowchart



## 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 a match with a deny action is encountered, the ACL being processed is skipped, and the next ACL is processed.
- 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 switch offers best-effort service to the packet.
- If multiple ACLs are configured on an interface, the lookup stops after the packet matches the first ACL with a permit action, and QoS processing begins.

**Note**

---

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.

---

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. For configuration information, see the [“Configuring a QoS Policy” section on page 27-26](#).

## 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 or matching a specific list of DSCP or IP precedence 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, DSCP, or IP precedence values in the traffic class; setting a specific DSCP or IP precedence 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** 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 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**, **trust**, 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 27-8](#).

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.
- The policy-map trust state and an interface trust state are mutually exclusive, and whichever is configured last takes affect.

For configuration information, see the [“Configuring a QoS Policy” section on page 27-26](#).

## Policing and Marking

After a packet is classified and has an internal DSCP value assigned to it, the policing and marking process can begin as shown in [Figure 27-4](#).

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 passing through the packet without modification, dropping the packet, or marking down the packet with a new DSCP value that is obtained from the configurable policed-DSCP map. For information on the policed-DSCP map, see the [“Mapping Tables” section on page 27-11](#).

You can create these types of policers:

- 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 **police** policy-map configuration command.
- Aggregate  
QoS applies the bandwidth limits specified in an aggregate policer cumulatively to all matched traffic flows. You configure this type of policer by specifying the aggregate policer name within a policy map by using the **police aggregate** policy-map configuration command. You specify the bandwidth limits of the policer by using the **mls qos aggregate-policer** global configuration command. In this way, the aggregate policer is shared by multiple classes of traffic within a policy map.

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 performs a check to determine if 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 determines 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.

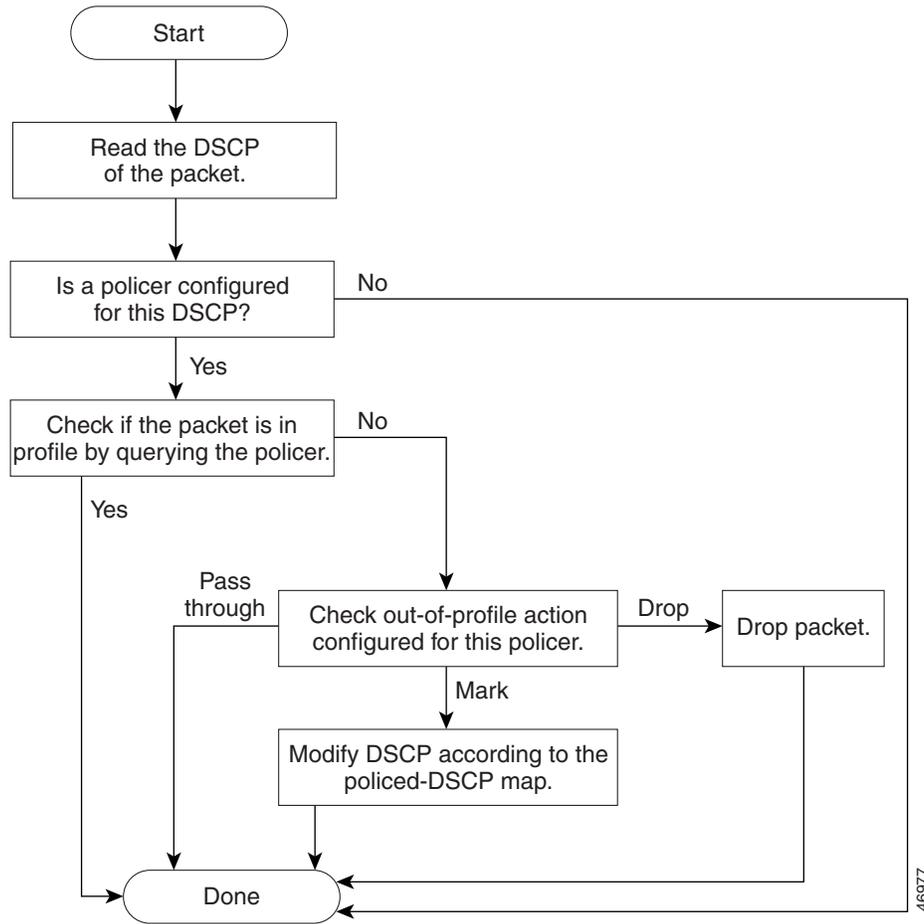
You configure the bucket depth (the maximum burst that is tolerated before the bucket overflows) by using the *burst-byte* option of the **police** policy-map class configuration command or the **mls qos aggregate-policer** global configuration command. You configure how fast (the average rate) that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

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

- By default, no policers are configured.
- Policers can be configured only on a physical port. There is no support for policing at a VLAN or switch virtual interface level.
- Only one policer can be applied to a packet per direction.
- Only the average rate and committed burst parameters are configurable.
- Policing can occur on ingress and egress interfaces:
  - 128 policers are supported on ingress Gigabit-capable Ethernet ports.
  - 8 policers are supported on ingress 10/100 Ethernet ports.
  - 8 policers are supported on all egress ports.
  - Ingress policers can be individual or aggregate.
- 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.

After you configure the policy map and policing actions, attach the policy to an ingress or egress interface by using the **service-policy** interface configuration command. For configuration information, see the “[Classifying, Policing, and Marking Traffic by Using Policy Maps](#)” section on page 27-32 and the “[Classifying, Policing, and Marking Traffic by Using Aggregate Policers](#)” section on page 27-37.

Figure 27-4 Policing and Marking Flowchart



46977

## Mapping Tables

During QoS processing, the switch represents the priority of all traffic (including non-IP traffic) with an internal DSCP value:

- During classification, QoS uses configurable mapping tables to derive the internal DSCP (a 6-bit value) from received CoS or IP precedence (3-bit) values. These maps include the CoS-to-DSCP map and the IP-precedence-to-DSCP map.

On an ingress interface configured in the DSCP-trusted state, if the DSCP values are different between the QoS domains, you can apply the configurable DSCP-to-DSCP-mutation map to the interface that is on the boundary between the two QoS domains.

- During policing, QoS can assign another DSCP value to an IP or non-IP packet (if the packet is out of profile and the policer specifies a marked down DSCP value). This configurable map is called the policed-DSCP map.
- 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. Through the CoS-to-egress-queue map, the CoS values select one of the four egress queues for output processing.

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

The default DSCP-to-DSCP-mutation map and the default policed-DSCP map are null maps; they map an incoming DSCP value to the same DSCP value. The DSCP-to-DSCP-mutation map is the only map you apply to a specific Gigabit-capable Ethernet port or to a group of 10/100 Ethernet ports. All other maps apply to the entire switch.

For configuration information, see the [“Configuring DSCP Maps” section on page 27-39](#).

## Queueing and Scheduling

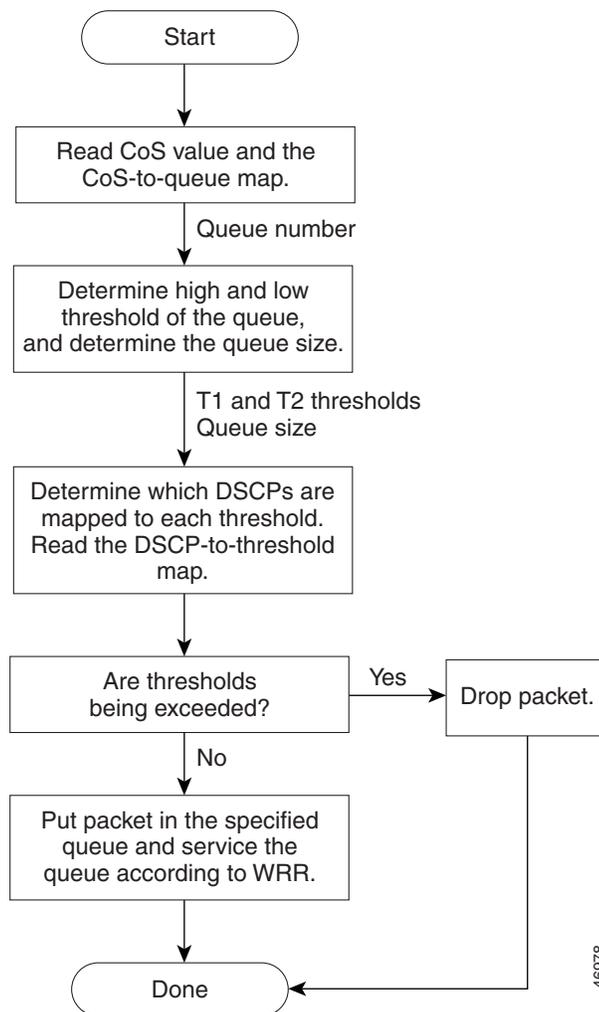
After a packet is policed and marked, the queueing and scheduling process begins as described in these sections:

- [Queueing and Scheduling on Gigabit-Capable Ports, page 27-12](#)
- [Queueing and Scheduling on 10/100 Ethernet Ports, page 27-15](#)

### Queueing and Scheduling on Gigabit-Capable Ports

Figure 27-5 shows the queueing and scheduling flowchart for Gigabit-capable Ethernet ports.

**Figure 27-5 Queueing and Scheduling Flowchart for Gigabit-Capable Ethernet Ports**



**Note**

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

During the queuing and scheduling process, the switch uses egress queues and WRR for congestion management, and tail drop or WRED algorithms for congestion avoidance on Gigabit-capable Ethernet ports.

Each Gigabit-capable Ethernet port has four egress queues, one of which can be the egress expedite queue. You can configure the buffer space allocated to each queue as a ratio of weights by using the **wrr-queue queue-limit** interface configuration command, where the relative size differences in the numbers indicates the relative differences in the queue sizes. To display the absolute value of the queue size, use the **show mls qos interface *interface-id* statistics** privileged EXEC command, and examine the FreeQ information.

You assign two drop thresholds to each queue, map DSCPs to the thresholds through the DSCP-to-threshold map, and enable either tail drop or WRED on the interface. The queue size, drop thresholds, tail-drop or WRED algorithm, and the DSCP-to-threshold map work together to determine when and which packets are dropped when the thresholds are exceeded. You configure the drop percentage thresholds by using either the **wrr-queue threshold** interface configuration command for tail drop or the **wrr-queue random-detect max-threshold** interface configuration command for WRED; in either case, you map DSCP values to the thresholds (DSCP-to-threshold map) by using the **wrr-queue dscp-map** interface configuration command. For more information, see the “Tail Drop” section on page 27-13 and “WRED” section on page 27-14.

The available bandwidth of the egress link is divided among the queues. You configure the queues to be serviced according to the ratio of WRR weights by using the **wrr-queue bandwidth** interface configuration command. Queues are selected by the CoS value that is mapped to an egress queue (CoS-to-egress-queue map) through the **wrr-queue cos-map** interface configuration command.

All four queues participate in the WRR unless the expedite queue is enabled, in which case, the fourth bandwidth weight is ignored and not used in the ratio calculation. The expedite queue is a strict-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.

You can combine the commands described in this section to prioritize traffic by placing packets with particular DSCPs into certain queues, allocate a larger queue size or service the particular queue more frequently, and adjust queue thresholds so that packets with lower priorities are dropped. For configuration information, see the “Configuring Egress Queues on Gigabit-Capable Ethernet Ports” section on page 27-44.

## Tail Drop

Tail drop is the default congestion-avoidance technique on Gigabit-capable Ethernet ports. With tail drop, packets are queued until the thresholds are exceeded. Specifically, all packets with DSCPs assigned to the first threshold are dropped until the threshold is no longer exceeded. However, packets assigned to the second threshold continue to be queued and sent as long as the second threshold is not exceeded.

You can modify the two tail-drop threshold percentages assigned to the four egress queues by using the **wrr-queue threshold** interface configuration command. Each threshold value is a percentage of the total number of allocated queue descriptors for the queue. The default threshold is 100 percent for thresholds 1 and 2.

You modify the DSCP-to-threshold map to determine which DSCPs are mapped to which threshold ID by using the **wrr-queue dscp-map** interface configuration command. By default, all DSCPs are mapped to threshold 1, and when this threshold is exceeded, all the packets are dropped.

If you use tail-drop thresholds, you cannot use WRED, and vice versa. If tail drop is disabled, WRED is automatically enabled with the previous configuration (or the default if it was not previously configured).

## WRED

Cisco's implementation of Random Early Detection (RED), called Weighted Random Early Detection (WRED), differs from other congestion-avoidance techniques because it attempts to anticipate and avoid congestion, rather than controlling congestion once it occurs.

WRED takes advantage of TCP congestion control to try to control the average queue size by indicating to end hosts when they should temporarily stop sending packets. By randomly dropping packets before periods of high congestion, it tells the packet source to decrease its transmission rate. Assuming the packet source is using TCP, WRED tells it to decrease its transmission rate until all the packets reach their destination, meaning that the congestion is cleared.

WRED reduces the chances of tail drop by selectively dropping packets when the output interface begins to show signs of congestion. By dropping some packets early rather than waiting until the queue is full, WRED avoids dropping large numbers of packets at once. Thus, WRED allows the transmission line to be fully used at all times. WRED also drops more packets from large users than small. Therefore, traffic sources that generate the most traffic are more likely to be slowed down than traffic sources that generate little traffic.

You can enable WRED and configure the two threshold percentages assigned to the four egress queues on a Gigabit-capable Ethernet port by using the **wrr-queue random-detect max-threshold** interface configuration command. Each threshold percentage represents where WRED starts to randomly drop packets. After a threshold is exceeded, WRED randomly begins to drop packets assigned to this threshold. As the queue limit is approached, WRED continues to drop more and more packets. When the queue limit is reached, WRED drops all packets assigned to the threshold. By default, WRED is disabled.

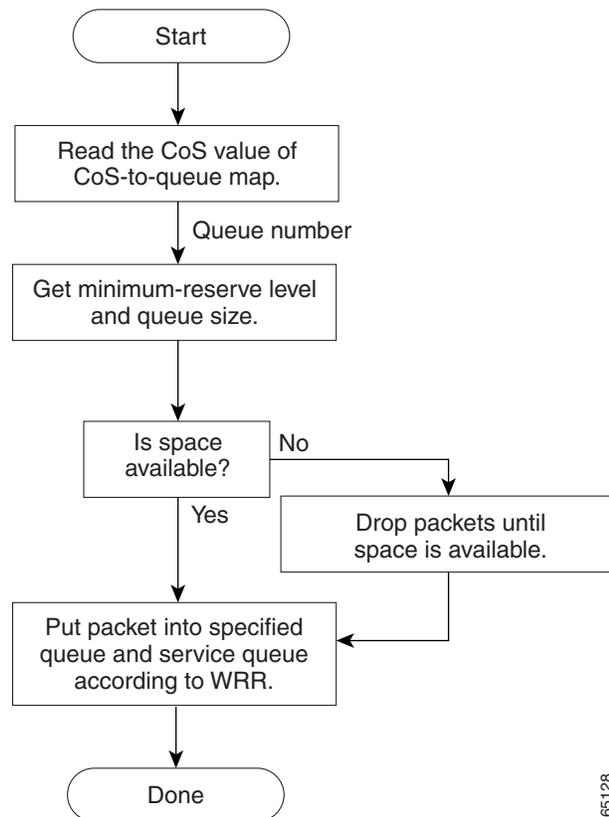
You modify the DSCP-to-threshold map to determine which DSCPs are mapped to which threshold ID by using the **wrr-queue dscp-map** interface configuration command. By default, all DSCPs are mapped to threshold 1, and when this threshold is exceeded, all the packets are randomly dropped.

If you use WRED thresholds, you cannot use tail drop, and vice versa. If WRED is disabled, tail drop is automatically enabled with the previous configuration (or the default if it was not previously configured).

## Queueing and Scheduling on 10/100 Ethernet Ports

Figure 27-6 shows the queueing and scheduling flowchart for 10/100 Ethernet ports.

**Figure 27-6 Queueing and Scheduling Flowchart for 10/100 Ethernet Ports**



### Note

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

During the queueing and scheduling process, the switch uses egress queues, which select the minimum-reserve level and buffer size, and WRR to provide congestion management.

Each 10/100 Ethernet port has four egress queues, one of which can be the egress expedite queue. Each queue can access one of eight minimum-reserve levels; each level has 100 packets of buffer space by default for queueing packets. When the buffer specified for the minimum-reserve level is full, packets are dropped until space is available.

Figure 27-7 is an example of the 10/100 Ethernet port queue assignments, minimum-reserve levels, and buffer sizes. The figure shows four egress queues per port, with each queue assigned to a minimum-reserve level. For example, for Fast Ethernet port 0/1, queue 1 is assigned to minimum-reserve level 1, queue 2 is assigned to minimum-reserve level 3, queue 3 is assigned to minimum-reserve level 5, and queue 4 is assigned to minimum-reserve level 7. You assign the minimum-reserve level to a queue by using the **wrr-queue min-reserve** interface configuration command.

Each minimum-reserve level is configured with a buffer size. As shown in the figure, queue 4 of Fast Ethernet port 0/1 has a buffer size of 70 packets, queue 4 of Fast Ethernet port 0/2 has a buffer size of 80 packets, queue 4 of Fast Ethernet port 0/3 has a buffer size of 40 packets, and Fast Ethernet port 0/4 has a buffer size of 80 packets. You configure the buffer size by using the **mls qos min-reserve** global configuration command.

**Figure 27-7 10/100 Ethernet Port Queue Assignment, Minimum-Reserve Levels, and Buffer Size**

Fast Ethernet Port Number	Q1	Q2	Q3	Q4	MRL	Buffer size
	MRL*	MRL	MRL	MRL		
0/1	1	3	5	7	1	10
0/2	2	4	6	8	2	20
0/3	1	2	3	4	3	30
0/4	5	6	7	8	4	40
•					5	50
•					6	60
•					7	70
					8	80

65127

\* MRL = Minimum-reserve level

The available bandwidth of the egress link is divided among the queues. You configure the queues to be serviced according to the ratio of WRR weights by using the **wrr-queue bandwidth** interface configuration command. Queues are selected by the CoS value that is mapped to an egress queue (CoS-to-egress-queue map) through the **wrr-queue cos-map** interface configuration command.

All four queues participate in the WRR unless the egress expedite queue is enabled, in which case, the fourth bandwidth weight is ignored and not used in the ratio calculation. The expedite queue is a strict-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.

You can combine the commands described in this section to prioritize traffic by placing packets with particular DSCPs into certain queues, allocate a larger minimum-reserve buffer size, and service a particular queue more frequently. For configuration information, see the [“Configuring Egress Queues on 10/100 Ethernet Ports”](#) section on page 27-51.

## Packet Modification

A packet is classified, policed, and queued to provide QoS. Packet modifications can occur during this process:

- For IP packets, classification involves assigning a DSCP to the packet. However, the packet is not modified at this stage; only an indication of the assigned DSCP is carried along. The reason for this is that QoS classification and ACL lookup occur in parallel, and it is possible that the ACL specifies that the packet should be denied and logged. In this situation, the packet is forwarded with its original DSCP to the CPU, where it is again processed through ACL software. However, route lookup is performed based on classified DSCPs.
- For non-IP packets, classification involves assigning an internal DSCP to the packet, but because there is no DSCP in the non-IP packet, no overwrite occurs. Instead, the internal DSCP is translated to the CoS and is used both for queueing and scheduling decisions and for writing the CoS priority value in the tag if the packet is being sent on either an ISL or 802.1Q trunk port. Because the CoS priority is written in the tag, Catalyst 3500 series XL switches that use the 802.1P priority can interoperate with the QoS implementation on the Catalyst 3550 switches.
- 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.

# 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. It contains this configuration information:

- [Default QoS Configuration, page 27-18](#)
- [Configuration Guidelines, page 27-20](#)
- [Enabling QoS Globally, page 27-21](#)
- [Configuring Classification Using Port Trust States, page 27-21](#)
- [Configuring a QoS Policy, page 27-26](#)
- [Configuring DSCP Maps, page 27-39](#)
- [Configuring Egress Queues on Gigabit-Capable Ethernet Ports, page 27-44](#)
- [Configuring Egress Queues on 10/100 Ethernet Ports, page 27-51](#)

## Default QoS Configuration

[Table 27-1](#) shows the default QoS configuration when QoS is disabled.

**Table 27-1** Default QoS Parameters when QoS is Disabled

Port Type	QoS State	Egress traffic (DSCP and CoS Value)	Queue	Queue Weights	Tail-drop Thresholds	CoS Mapping to Queue
Gigabit-capable Ethernet ports	Disabled	Pass through.	All of the queue RAM is allocated to queue 1 (no expedite queue).	–	100%, 100% WRED is disabled.	All CoS values map to queue 1.
10/100 Ethernet ports	Disabled	Pass through.	Each of the eight minimum-reserve levels have a buffer size of 100 packets. The queue selects the level.	–	–	All CoS values map to queue 1.

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

[Table 27-2](#) shows the default QoS parameters without any further configuration when QoS is enabled.

**Table 27-2 Default QoS Parameters when QoS is Enabled**

Port Type	QoS State	Egress traffic (DSCP and CoS Value)	Queue	Queue Weights	Tail-drop Thresholds	CoS Mapping to Queue
Gigabit-capable Ethernet ports	Enabled (no policing)	DSCP=0 CoS=0 (0 means best-effort delivery.)	Four queues are available (no expedite queue).	Each queue has the same weight.	100%, 100% WRED is disabled.	0, 1: queue 1 2, 3: queue 2 4, 5: queue 3 6, 7: queue 4
10/100 Ethernet ports	Enabled (no policing)	DSCP=0 CoS=0 (0 means best-effort delivery.)	Each of the eight minimum-reserve levels have a buffer size of 100 packets. The queue selects the level.	Each queue has the same weight.	–	0, 1: queue 1 2, 3: queue 2 4, 5: queue 3 6, 7: queue 4

The default port CoS value is 0.

The default port trust state on all ports is untrusted.

No policy maps are configured.

No policers are configured.

The default CoS-to-DSCP map is shown in [Table 27-3 on page 27-39](#).

The default IP-precedence-to-DSCP map is shown in [Table 27-4 on page 27-40](#).

The default DSCP-to-CoS map is shown in [Table 27-5 on page 27-42](#).

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).

The default DSCP-to-switch-priority map maps DSCPs 0 to 15 to priority 0, DSCPs 16 to 31 to priority 1, DSCPs 32 to 47 to priority 2, and DSCPs 48 to 63 to priority 3.

## Configuration Guidelines

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 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.
- You configure QoS only on physical ports; there is no support for it on the VLAN or switch virtual interface level.
- 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.
- You can match IP options against configured IP extended ACLs to enforce QoS. These packets are sent to the CPU and processed by software. IP options 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.
- You must disable the IEEE 802.3X flowcontrol on all ports before enabling QoS on the switch. To disable it, use the **flowcontrol receive off** and **flowcontrol send off** interface configuration commands.
- Only one ACL per class map and only one **match** class-map configuration 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.
- Use only the **match ip dscp dscp-list** class-map configuration command in a policy map that is attached to an egress interface.
- Policy maps with ACL classification in the egress direction are not supported and cannot be attached to an interface by using the **service-policy output policy-map-name** interface configuration command. Policy maps containing **set** or **trust** policy-map class configuration commands cannot be attached to an egress interface; instead, you can use the **police** policy-map class configuration command to mark down (reduce) the DSCP value at the egress interface.
- You can create an aggregate policer that is shared by multiple traffic classes within the same policy map. However, you cannot use the aggregate policer across different policy maps or interfaces.
- Layer 3 QoS ACLs and other QoS features related to Layer 3 information are not supported on tunnel ports. MAC-based QoS is supported on tunnel ports. When applied to trunk ports, Layer 3 QoS ACLs do not work for VLANs that include tunnel ports.

## Enabling QoS Globally

By default, QoS is disabled on the switch, which means that the switch offers best-effort service to each packet regardless of the packet contents or size. All CoS values map to egress queue 1 with both tail-drop thresholds set to 100 percent of the total queue size for Gigabit-capable Ethernet ports. On 10/100 Ethernet ports, all CoS values map to egress queue 1, which uses minimum-reserve level 1 and can hold up to 100 packets. When the buffer is full, packets are dropped.

Beginning in privileged EXEC mode, follow these steps to enable QoS:

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface range</b> <i>port-range</i>	Enter interface configuration mode, and execute a command on multiple interfaces.  You can define up to five interface ranges with a single command, with each range separated by a comma.  All interfaces in a range must be the same type; that is, all Fast Ethernet ports or all Gigabit Ethernet ports.
Step 3	<b>flowcontrol receive off</b> <b>flowcontrol send off</b>	Disable flowcontrol on all interfaces.
Step 4	<b>exit</b>	Return to global configuration mode.
Step 5	<b>mls qos</b>	Enable QoS globally.
Step 6	<b>end</b>	Return to privileged EXEC mode.
Step 7	<b>show mls qos</b>	Verify your entries.
Step 8	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

After QoS is enabled, the default settings are as shown in [Table 27-1 on page 27-18](#).

To disable QoS, use the **no mls qos** global configuration command.

## Configuring Classification Using Port Trust States

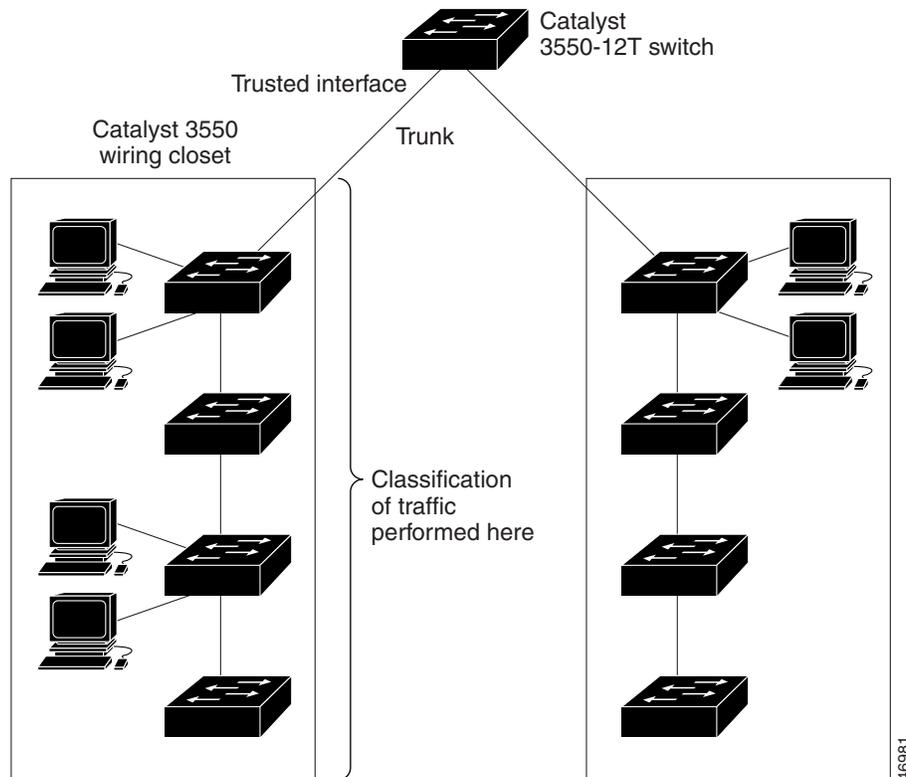
This section describes how to classify incoming traffic by using port trust states. It contains this configuration information:

- [Configuring the Trust State on Ports within the QoS Domain, page 27-22](#)
- [Configuring the CoS Value for an Interface, page 27-24](#)
- [Configuring the DSCP Trust State on a Port Bordering Another QoS Domain, page 27-25](#)

## 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 27-8](#) shows a sample network topology.

**Figure 27-8** Port Trusted States within the QoS Domain



46981

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	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>mls qos</b>	Enable QoS globally.
Step 3	<b>interface</b> <i>interface-id</i>	Enter interface configuration mode, and specify the interface to be trusted.  Valid interfaces include physical interfaces.
Step 4	<b>mls qos trust {cos   dscp   ip-precedence}</b>	Configure the port trust state.  By default, the port is not trusted.  The keywords have these meanings: <ul style="list-style-type: none"> <li>• <b>cos</b>—Classifies ingress packets with the packet CoS values. For untagged packets, the port default CoS value is used. The default port CoS value is 0.</li> <li>• <b>dscp</b>—Classifies ingress packets with packet DSCP values. For non-IP packets, the packet CoS value is used if the packet is tagged; for untagged packets, the default port CoS is used. Internally, the switch maps the CoS value to a DSCP value by using the CoS-to-DSCP map.</li> <li>• <b>ip-precedence</b>—Classifies ingress packets with the packet IP-precedence values. For non-IP packets, the packet CoS value is used if the packet is tagged; for untagged packets, the default port CoS is used. Internally, the switch maps the CoS value to a DSCP value by using the CoS-to-DSCP map.</li> </ul> <p>Use the <b>cos</b> keyword setting if your network is composed of Ethernet LANs, Catalyst 3500 XL and 2900 XL switches, and has no more than two types of traffic. Recall that on Catalyst 3500 XL and 2900 XL switches, CoS configures each transmit port with a normal-priority transmit queue and a high-priority transmit queue.</p> <p>Use the <b>dscp</b> or <b>ip-precedence</b> keyword if your network is not composed of only Ethernet LANs and if you are familiar with sophisticated QoS features and implementations.</p>
Step 5	<b>end</b>	Return to privileged EXEC mode.
Step 6	<b>show mls qos interface</b>	Verify your entries.
Step 7	<b>copy running-config startup-config</b>	(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 27-24. For information on how to configure the CoS-to-DSCP map, see the [“Configuring the CoS-to-DSCP Map”](#) section on page 27-39.

## 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:

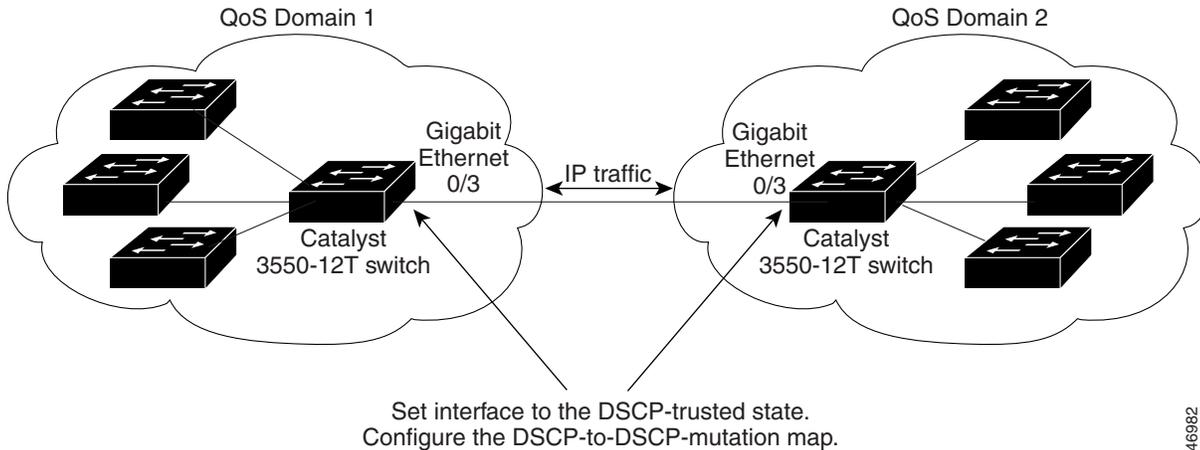
	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>mls qos</b>	Enable QoS globally.
Step 3	<b>interface</b> <i>interface-id</i>	Enter interface configuration mode, and specify the interface to be trusted. Valid interfaces include physical interfaces.
Step 4	<b>mls qos cos</b> { <i>default-cos</i>   <b>override</b> }	Configure the default CoS value for the port. <ul style="list-style-type: none"> <li>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.</li> <li>Use the <b>override</b> 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.</li> </ul> <p>Use the <b>override</b> keyword when all incoming packets on certain ports deserve higher or lower priority than packets entering from other ports. Even if a port was previously set to trust DSCP, CoS, or IP precedence, 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>
Step 5	<b>end</b>	Return to privileged EXEC mode.
Step 6	<b>show mls qos interface</b>	Verify your entries.
Step 7	<b>copy running-config startup-config</b>	(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 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 switch ports bordering the domains to a DSCP-trusted state as shown in Figure 27-9. Then 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 27-9 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:

	Command	Purpose
Step 1	<code>configure terminal</code>	Enter global configuration mode.
Step 2	<code>mls qos</code>	Enable QoS on the switch.
Step 3	<code>mls qos map dscp-mutation</code> <code>dscp-mutation-name in-dscp to out-dscp</code>	Modify 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"> <li>For <i>dscp-mutation-name</i>, enter the mutation map name. You can create more than one map by specifying a new name.</li> <li>For <i>in-dscp</i>, enter up to eight DSCP values separated by spaces. Then enter the <b>to</b> keyword.</li> <li>For <i>out-dscp</i>, enter up to eight DSCP values separated by spaces.</li> </ul> The DSCP range is 0 to 63.
Step 4	<code>interface interface-id</code>	Enter interface configuration mode, and specify the interface to be trusted. Valid interfaces include physical interfaces.
Step 5	<code>mls qos trust dscp</code>	Configure the ingress port as a DSCP-trusted port.

	Command	Purpose
Step 6	<b>mls qos dscp-mutation</b> <i>dscp-mutation-name</i>	Apply the map to the specified ingress DSCP-trusted port.  You can apply the map to different Gigabit-capable Ethernet ports. However, on 10/100 Ethernet ports, you can attach only one DSCP-to-DSCP-mutation map to a group of twelve ports. For example, Fast Ethernet ports 0/1 to 0/12 are a group, Fast Ethernet ports 0/13 to 0/24 are a group, Gigabit Ethernet 0/1 is a group, and Gigabit Ethernet 0/2 is a group. When applying a mutation map to any port in a group, all ports in the same group are automatically configured with the same map.
Step 7	<b>end</b>	Return to privileged EXEC mode.
Step 8	<b>show mls qos maps dscp-mutation</b>	Verify your entries.
Step 9	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

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-map-name* global configuration command.

This example shows how to configure Gigabit Ethernet port 0/2 to the DSCP-trusted state and to modify the DSCP-to-DSCP-mutation map (named *gi0/2-mutation*) so that incoming DSCP values 10 to 13 are mapped to DSCP values 30 to 33:

```
Switch# configure terminal
Switch(config)# mls qos map dscp-mutation gi0/2-mutation 10 11 12 13 to 30 31 32 33
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# mls qos trust dscp
Switch(config-if)# mls qos dscp-mutation gi0/2-mutation
Switch(config-if)# end
```

## Configuring a QoS Policy

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 27-4 and the “Policing and Marking” section on page 27-8.

This section contains this configuration information:

- [Classifying Traffic by Using ACLs, page 27-27](#)
- [Classifying Traffic by Using Class Maps, page 27-30](#)
- [Classifying, Policing, and Marking Traffic by Using Policy Maps, page 27-32](#)
- [Classifying, Policing, and Marking Traffic by Using Aggregate Policers, page 27-37](#)

## Classifying Traffic by Using ACLs

You can classify IP traffic by using IP standard or IP extended ACLs; you can classify non-IP 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>mls qos</code>	Enable QoS on the switch.
Step 3	<code>access-list access-list-number {deny   permit} source [source-wildcard]</code>	<p>Create an IP standard ACL, repeating the command as many times as necessary.</p> <ul style="list-style-type: none"> <li>For <i>access-list-number</i>, enter the access list number. The range is 1 to 99 and 1300 to 1999.</li> <li>Use the <b>permit</b> keyword to permit a certain type of traffic if the conditions are matched. Use the <b>deny</b> keyword to deny a certain type of traffic if conditions are matched.</li> <li>For <i>source</i>, enter the network or host from which the packet is being sent. You can use the <b>any</b> keyword as an abbreviation for 0.0.0.0 255.255.255.255.</li> <li>(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.</li> </ul> <p><b>Note</b> 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>
Step 4	<code>end</code>	Return to privileged EXEC mode.
Step 5	<code>show access-lists</code>	Verify your entries.
Step 6	<code>copy running-config startup-config</code>	(Optional) Save your entries in the configuration file.

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

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.

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

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

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>mls qos</b>	Enable QoS on the switch.
Step 3	<b>access-list</b> <i>access-list-number</i> { <b>deny</b>   <b>permit</b> } <i>protocol source source-wildcard destination destination-wildcard</i>	<p>Create an IP extended ACL, repeating the command as many times as necessary.</p> <ul style="list-style-type: none"> <li>For <i>access-list-number</i>, enter the access list number. The range is 100 to 199 and 2000 to 2699.</li> <li>Use the <b>permit</b> keyword to permit a certain type of traffic if the conditions are matched. Use the <b>deny</b> keyword to deny a certain type of traffic if conditions are matched.</li> <li>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.</li> <li>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 <b>any</b> keyword as an abbreviation for <i>source</i> 0.0.0.0 <i>source-wildcard</i> 255.255.255.255, or by using the <b>host</b> keyword for <i>source</i> 0.0.0.0.</li> <li>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 <b>any</b> keyword as an abbreviation for <i>source</i> 0.0.0.0 <i>source-wildcard</i> 255.255.255.255, or by using the <b>host</b> keyword for <i>source</i> 0.0.0.0.</li> <li>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>.</li> </ul> <p><b>Note</b> 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>
Step 4	<b>end</b>	Return to privileged EXEC mode.
Step 5	<b>show access-lists</b>	Verify your entries.
Step 6	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

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

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:

```
Switch(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:

```
Switch(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:

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

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

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>mls qos</b>	Enable QoS on the switch.
Step 3	<b>mac access-list extended</b> <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 4	<b>{permit   deny} {host</b> <i>src-MAC-addr mask</i>   <b>any</b>   <b>host</b> <i>dst-MAC-addr</i>   <i>dst-MAC-addr mask</i> } [ <i>type mask</i> ]	Specify the type of traffic to permit or deny if the conditions are matched, entering the command as many times as necessary. <ul style="list-style-type: none"> <li>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 <b>any</b> keyword as an abbreviation for <i>source</i> 0.0.0, <i>source-wildcard</i> 255.255.255, or by using the <b>host</b> keyword for <i>source</i> 0.0.0.</li> <li>For <i>mask</i>, enter the wildcard bits by placing ones in the bit positions that you want to ignore.</li> <li>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 <b>any</b> keyword as an abbreviation for <i>source</i> 0.0.0, <i>source-wildcard</i> 255.255.255, or by using the <b>host</b> keyword for <i>source</i> 0.0.0.</li> <li>(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.</li> </ul> <p><b>Note</b> 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>
Step 5	<b>end</b>	Return to privileged EXEC mode.
Step 6	<b>show access-lists</b> [ <i>access-list-number</i>   <i>access-list-name</i> ]	Verify your entries.
Step 7	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

To delete an access list, 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 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.

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

## 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 27-32.

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	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>mls qos</b>	Enable QoS on the switch.
Step 3	<b>access-list access-list-number {deny   permit} source [source-wildcard]</b> or <b>access-list access-list-number {deny   permit} protocol source [source-wildcard] destination [destination-wildcard]</b> or <b>mac access-list extended name</b> <b>{permit   deny} {host src-MAC-addr mask   any   host dst-MAC-addr   dst-MAC-addr mask} [type mask]</b>	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 “ <a href="#">Classifying Traffic by Using ACLs</a> ” section on page 27-27.  <b>Note</b> 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.

	Command	Purpose
Step 4	<b>class-map</b> <i>class-map-name</i> [ <b>match-all</b>   <b>match-any</b> ]	<p>Create a class map, and enter class-map configuration mode.</p> <p>By default, no class maps are defined.</p> <ul style="list-style-type: none"> <li>For <i>class-map-name</i>, specify the name of the class map.</li> <li>(Optional) Use the <b>match-all</b> keyword to perform a logical-AND of all matching statements under this class map. All match criteria in the class map must be matched.</li> <li>(Optional) Use the <b>match-any</b> keyword to perform a logical-OR of all matching statements under this class map. One or more match criteria must be matched.</li> </ul> <p>If neither the <b>match-all</b> or <b>match-any</b> keyword is specified, the default is <b>match-all</b>.</p> <p><b>Note</b> Because only one <b>match</b> command per class map is supported, the <b>match-all</b> and <b>match-any</b> keywords function the same.</p>
Step 5	<b>match</b> { <b>access-group</b> <i>acl-index-or-name</i>   <b>ip dscp</b> <i>dscp-list</i>   <b>ip precedence</b> <i>ip-precedence-list</i> }	<p>Define the match criterion to classify traffic.</p> <p>By default, no match criterion is supported.</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"> <li>For <b>access-group</b> <i>acl-index-or-name</i>, specify the number or name of the ACL created in Step 3.</li> <li>For <b>ip dscp</b> <i>dscp-list</i>, 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.</li> <li>For <b>ip precedence</b> <i>ip-precedence-list</i>, enter a list of up to eight IP-precedence values to match against incoming packets. Separate each value with a space. The range is 0 to 7.</li> </ul> <p><b>Note</b> You can use the <b>match ip dscp</b> <i>dscp-list</i> class-map configuration command only in a policy map that is attached to an egress interface.</p>
Step 6	<b>end</b>	Return to privileged EXEC mode.
Step 7	<b>show class-map</b>	Verify your entries.
Step 8	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

To delete an existing class map, use the **no class-map** *class-map-name* [**match-all** | **match-any**] global configuration command. To remove a match criterion, use the **no match** {**access-group** *acl-index-or-name* | **ip dscp** | **ip precedence**} class-map configuration command.

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.

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

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

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

This example shows how to create a class map called *class3*, which matches incoming traffic with IP-precedence values of 5, 6, and 7:

```
Switch(config)# class-map class3
Switch(config-cmap)# match ip precedence 5 6 7
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, DSCP, or IP precedence values in the traffic class; setting a specific DSCP or IP precedence 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.
- A policy-map trust state supersedes an interface trust state.

You can attach only one policy map per interface per direction.

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

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>mls qos</b>	Enable QoS on the switch.
Step 3	<b>access-list access-list-number {deny   permit} source [source-wildcard]</b> or <b>access-list access-list-number {deny   permit} protocol source [source-wildcard] destination [destination-wildcard]</b> or <b>mac access-list extended access-list name {permit   deny} {source-MAC-addr mask   any   host} {destination-MAC-addr mask   any   host} [ethertype]</b>	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 <a href="#">“Classifying Traffic by Using ACLs” section on page 27-27</a> .  <b>Note</b> 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.

	Command	Purpose
Step 4	<b>policy-map</b> <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 5	<b>class</b> <i>class-map-name</i> [ <b>access-group</b> <i>acl-index-or-name</i>   <b>dscp</b> <i>dscp-list</i>   <b>precedence</b> <i>ip-precedence-list</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 <b>class-map</b> global configuration command, specify its name for <i>class-map-name</i> in this command.</p> <p>To define a class map that uses an access list to filter traffic or that matches traffic to the specified DSCP or IP precedence values, use one of these keywords:</p> <ul style="list-style-type: none"> <li>• For <b>access-group</b> <i>acl-index-or-name</i>, specify the number or name of the ACL created in Step 3.</li> <li>• For <b>dscp</b> <i>dscp-list</i>, specify a list of up to eight IP DSCP values to be matched against incoming packets. Separate each value with a space. The range is 0 to 63.</li> <li>• For <b>precedence</b> <i>ip-precedence-list</i>, specify a list of up to eight IP-precedence values to be matched against incoming packets. Separate each value with a space. The range is 0 to 7.</li> </ul>

Command	Purpose
<b>Step 6</b> <code>trust [cos   dscp   ip-precedence]</code>	<p>Configure the trust state, which selects the value that QoS uses as the source of the internal DSCP value.</p> <p><b>Note</b> This command is mutually exclusive with the <code>set</code> command within the same policy map. If you enter the <code>trust</code> command, then skip Step 7.</p> <p>By default, the port is not trusted. If no keyword is specified when the command is entered, the default is <code>dscp</code>.</p> <p>The keywords have these meanings:</p> <ul style="list-style-type: none"> <li>• <b>cos</b>—QoS derives the internal DSCP value by using the received or default port CoS value and the CoS-to-DSCP map.</li> <li>• <b>dscp</b>—QoS derives the internal DSCP value by using the DSCP value from the ingress packet. For non-IP packets that are tagged, QoS derives the internal DSCP value by using the received CoS value; for non-IP packets that are untagged, QoS derives the internal DSCP value by using the default port CoS value. In either case, the internal DSCP value is derived from the CoS-to-DSCP map.</li> <li>• <b>ip-precedence</b>—QoS derives the internal DSCP value by using the IP precedence value from the ingress packet and the IP-precedence-to-DSCP map. For non-IP packets that are tagged, QoS derives the internal DSCP value by using the received CoS value; for non-IP packets that are untagged, QoS derives the internal DSCP value by using the default port CoS value. In either case, the internal DSCP value is derived from the CoS-to-DSCP map.</li> </ul> <p>For more information, see the <a href="#">“Configuring the CoS-to-DSCP Map” section on page 27-39</a>.</p>
<b>Step 7</b> <code>set {ip dscp new-dscp   ip precedence new-precedence}</code>	<p>Classify IP traffic by setting a new value in the packet.</p> <ul style="list-style-type: none"> <li>• For <code>ip dscp new-dscp</code>, enter a new DSCP value to be assigned to the classified traffic. The range is 0 to 63.</li> <li>• For <code>ip precedence new-precedence</code>, enter a new IP-precedence value to be assigned to the classified traffic. The range is 0 to 7.</li> </ul>

	Command	Purpose
Step 8	<b>police</b> <i>rate-bps burst-byte</i> [ <b>exceed-action</b> { <b>drop</b>   <b>policed-dscp-transmit</b> }]	<p>Define a policer for the classified traffic.</p> <p>You can configure up to 128 policers on ingress Gigabit-capable Ethernet ports, up to 8 policers on ingress 10/100 Ethernet ports, and up to 8 policers on egress ports.</p> <ul style="list-style-type: none"> <li>For <i>rate-bps</i>, specify average traffic rate in bits per second (bps). The range is 8000 to 2000000000.</li> <li>For <i>burst-byte</i>, specify the normal burst size in bytes. The range is 8000 to 512000000.</li> <li>(Optional) Specify the action to take when the rates are exceeded. Use the <b>exceed-action drop</b> keywords to drop the packet. Use the <b>exceed-action policed-dscp-transmit</b> keywords to mark down the DSCP value (by using the policed-DSCP map) and send the packet. For more information, see the “<a href="#">Configuring the Policed-DSCP Map</a>” section on page 27-41.</li> </ul>
Step 9	<b>exit</b>	Return to policy map configuration mode.
Step 10	<b>exit</b>	Return to global configuration mode.
Step 11	<b>interface</b> <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 12	<b>service-policy</b> { <b>input</b> <i>policy-map-name</i>   <b>output</b> <i>policy-map-name</i> }	<p>Apply a policy map to the input or output of a particular interface.</p> <p>Only one policy map per interface per direction is supported.</p> <ul style="list-style-type: none"> <li>Use <b>input</b> <i>policy-map-name</i> to apply the specified policy-map to the input of an interface.</li> <li>Use <b>output</b> <i>policy-map-name</i> to apply the specified policy-map to the output of an interface.</li> </ul> <p><b>Note</b> Policy maps that contain <b>set</b> or <b>trust</b> policy-map class configuration commands or that have ACL classification cannot be attached to an output interface.</p>
Step 13	<b>end</b>	Return to privileged EXEC mode.
Step 14	<b>show policy-map</b> [ <i>policy-map-name</i> [ <b>class</b> <i>class-name</i> ]]	Verify your entries.
Step 15	<b>copy running-config startup-config</b>	(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 return to the default trust state, use the **no trust** [**cos** | **dscp** | **ip-precedence**] policy-map configuration command. To remove an assigned DSCP or IP precedence value, use the **no set** {**ip dscp** *new-dscp* | **ip precedence** *new-precedence*} policy-map configuration command. To remove an existing policer, use the **no police** *rate-bps burst-byte* [**exceed-action** {**drop** | **policed-dscp-transmit**}] policy-map configuration command. To remove the policy map and interface association, use the **no service-policy** {**input** *policy-map-name* | **output** *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 (based on the policed-DSCP map) and sent:

```
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)# trust dscp
Switch(config-pmap-c)# police 48000 8000 exceed-action policed-dscp-transmit
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# service-policy input flow1t
```

This example shows how to create a policy map and attach it to an ingress interface. In the configuration, the IP extended ACL permits Transmission Control Protocol (TCP) traffic with an IP precedence of 4 from any host destined for the host at 224.0.0.5. For traffic matching this classification, the DSCP value in the incoming packet is set to 63.

```
Switch(config)# access-list 104 permit tcp any host 224.0.0.5 precedence 4
Switch(config)# policy-map ip104
Switch(config-pmap)# class ipclass104 access-group 104
Switch(config-pmap-c)# set ip dscp 63
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# service-policy input ip104
```

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. 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.

```
Switch(config)# mac access-list extended maclist1
Switch(config-ext-mac)# permit 0001.0000.0001 0.0.0 0002.0000.0001 0.0.0
Switch(config-ext-mac)# permit 0001.0000.0002 0.0.0 0002.0000.0002 0.0.0 xns-idp
Switch(config-ext-mac)# exit
Switch(config)# mac access-list extended maclist2
Switch(config-ext-mac)# permit 0001.0000.0003 0.0.0 0002.0000.0003 0.0.0
Switch(config-ext-mac)# permit 0001.0000.0004 0.0.0 0002.0000.0004 0.0.0 aarp
Switch(config-ext-mac)# exit
Switch(config)# class-map macclass1
Switch(config-cmap)# match access-group maclist1
Switch(config-cmap)# exit
Switch(config)# policy-map macpolicy1
Switch(config-pmap)# class macclass1
Switch(config-pmap-c)# set ip dscp 63
Switch(config-pmap-c)# exit
Switch(config-pmap)# class macclass2 maclist2
Switch(config-pmap-c)# set ip dscp 45
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# mls qos trust cos
Switch(config-if)# service-policy input macpolicy1
```

## Classifying, Policing, and Marking Traffic by Using Aggregate Policers

By using an aggregate policer, you can create a policer that is shared by multiple traffic classes within the same policy map. However, you cannot use the aggregate policer across different policy maps or interfaces.

Beginning in privileged EXEC mode, follow these steps to create an aggregate policer:

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>mls qos</b>	Enable QoS on the switch.
Step 3	<b>mls qos aggregate-police</b> <i>aggregate-policer-name rate-bps</i> <i>burst-byte</i> <b>exceed-action</b> { <b>drop</b>   <b>policed-dscp-transmit</b> }	<p>Define the policer parameters that can be applied to multiple traffic classes within the same policy map.</p> <p>By default, no aggregate policer is defined.</p> <p>You can configure up to 128 policers on ingress Gigabit-capable Ethernet ports, up to 8 policers on ingress 10/100 Ethernet ports, and up to 8 policers on egress ports.</p> <ul style="list-style-type: none"> <li>For <i>aggregate-policer-name</i>, specify the name of the aggregate policer.</li> <li>For <i>rate-bps</i>, specify average traffic rate in bits per second (bps). The range is 8000 to 2000000000.</li> <li>For <i>burst-byte</i>, specify the normal burst size in bytes. The range is 8000 to 512000000.</li> <li>(Optional) Specify the action to take when the rates are exceeded. Use the <b>exceed-action drop</b> keywords to drop the packet. Use the <b>exceed-action policed-dscp-transmit</b> keywords to mark down the DSCP value (by using the policed-DSCP map) and send the packet. For more information, see the “<a href="#">Configuring the Policed-DSCP Map</a>” section on page 27-41.</li> </ul>
Step 4	<b>class-map</b> <i>class-map-name</i> [ <b>match-all</b>   <b>match-any</b> ]	Create a class map to classify traffic as necessary. For more information, see the “ <a href="#">Classifying Traffic by Using Class Maps</a> ” section on page 27-30.
Step 5	<b>policy-map</b> <i>policy-map-name</i>	Create a policy map by entering the policy map name, and enter policy-map configuration mode.  For more information, see the “ <a href="#">Classifying, Policing, and Marking Traffic by Using Policy Maps</a> ” section on page 27-32.
Step 6	<b>class</b> <i>class-map-name</i> [ <b>access-group</b> <i>acl-index-or-name</i>   <b>dscp</b> <i>dscp-list</i>   <b>precedence</b> <i>ip-precedence-list</i> ]	Define a traffic classification, and enter policy-map class configuration mode.  For more information, see the “ <a href="#">Classifying, Policing, and Marking Traffic by Using Policy Maps</a> ” section on page 27-32.
Step 7	<b>police aggregate</b> <i>aggregate-policer-name</i>	Apply an aggregate policer to multiple classes in the same policy map.  For <i>aggregate-policer-name</i> , enter the name specified in Step 3.
Step 8	<b>exit</b>	Return to global configuration mode.

	Command	Purpose
Step 9	<b>interface</b> <i>interface-id</i>	Enter interface configuration mode, and specify the interface to attach to the policy map.  Valid interfaces include physical interfaces.
Step 10	<b>service-policy</b> { <b>input</b> <i>policy-map-name</i>   <b>output</b> <i>policy-map-name</i> }	Apply a policy map to the input or output of a particular interface.  Only one policy map per interface per direction is supported. <ul style="list-style-type: none"> <li>Use <b>input</b> <i>policy-map-name</i> to apply the specified policy-map to the input of an interface.</li> <li>Use <b>output</b> <i>policy-map-name</i> to apply the specified policy-map to the output of an interface. Policy maps that contain <b>set</b> or <b>trust</b> policy-map class configuration commands or that have ACL classification cannot be attached to an egress interface.</li> </ul>
Step 11	<b>end</b>	Return to privileged EXEC mode.
Step 12	<b>show mls qos aggregate-policer</b> [ <i>aggregate-policer-name</i> ]	Verify your entries.
Step 13	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

To remove the specified aggregate policer from a policy map, use the **no police aggregate** *aggregate-policer-name* policy map configuration mode. To delete an aggregate policer and its parameters, use the **no mls qos aggregate-policer** *aggregate-policer-name* global configuration command.

This example shows how to create an aggregate policer and attach it to multiple classes within a policy map. In the configuration, the IP ACLs permit traffic from network 10.1.0.0 and from host 11.3.1.1. For traffic coming from network 10.1.0.0, the DSCP in the incoming packets is trusted. For traffic coming from host 11.3.1.1, the DSCP in the packet is changed to 56. The traffic rate from the 10.1.0.0 network and from host 11.3.1.1 is policed. If the traffic exceeds an average rate of 48000 bps and a normal burst size of 8000 bytes, its DSCP is marked down (based on the policed-DSCP map) and sent. The policy map is attached to an ingress interface.

```
Switch(config)# access-list 1 permit 10.1.0.0 0.0.255.255
Switch(config)# access-list 2 permit 11.3.1.1
Switch(config)# mls qos aggregate-police transmit1 48000 8000 exceed-action
policed-dscp-transmit
Switch(config)# policy-map aggflow1
Switch(config-pmap)# class ipclass1 access-group 1
Switch(config-pmap-c)# trust dscp
Switch(config-pmap-c)# police aggregate transmit1
Switch(config-pmap-c)# exit
Switch(config-pmap)# class ipclass2 access-group 2
Switch(config-pmap-c)# set ip dscp 56
Switch(config-pmap-c)# police aggregate transmit1
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# service-policy input aggflow1
Switch(config-if)# exit
```

## Configuring DSCP Maps

This section describes how to configure the DSCP maps. It contains this configuration information:

- [Configuring the CoS-to-DSCP Map, page 27-39](#)
- [Configuring the IP-Precedence-to-DSCP Map, page 27-40](#)
- [Configuring the Policed-DSCP Map, page 27-41](#)
- [Configuring the DSCP-to-CoS Map, page 27-42](#)
- [Configuring the DSCP-to-DSCP-Mutation Map, page 27-43](#)

All the maps, except the DSCP-to-DSCP-mutation map, are globally defined and are applied to all ports. You can have multiple DSCP-to-DSCP-mutation maps and apply them to different Gigabit-capable Ethernet ports. However, on 10/100 Ethernet ports, you can attach only one DSCP-to-DSCP-mutation map to a group of twelve ports.

### 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 27-3](#) shows the default CoS-to-DSCP map.

**Table 27-3 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	<code>configure terminal</code>	Enter global configuration mode.
Step 2	<code>mls qos map cos-dscp dscp1...dscp8</code>	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 DSCP range is 0 to 63.
Step 3	<code>end</code>	Return to privileged EXEC mode.
Step 4	<code>show mls qos maps cos-dscp</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 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 10 15 20 25 30 35 40 45
Switch(config)# end
Switch# show mls qos maps cos-dscp

Cos-dscp map:
   cos:   0  1  2  3  4  5  6  7
-----
   dscp:  10 15 20 25 30 35 40 45
```

## Configuring the IP-Precedence-to-DSCP Map

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

Table 27-4 shows the default IP-precedence-to-DSCP map:

**Table 27-4 Default IP-Precedence-to-DSCP Map**

IP precedence 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 IP-precedence-to-DSCP map:

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>mls qos map ip-prec-dscp</b> <i>dscp1...dscp8</i>	Modify the IP-precedence-to-DSCP map.  For <i>dscp1...dscp8</i> , enter 8 DSCP values that correspond to the IP precedence values 0 to 7. Separate each DSCP value with a space.  The DSCP range is 0 to 63.
Step 3	<b>end</b>	Return to privileged EXEC mode.
Step 4	<b>show mls qos maps ip-prec-dscp</b>	Verify your entries.
Step 5	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

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

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

```
Switch# configure terminal
Switch(config)# mls qos map ip-prec-dscp 10 15 20 25 30 35 40 45
Switch(config)# end
Switch# show mls qos maps ip-prec-dscp

IpPrecedence-dscp map:
  ipprec:  0  1  2  3  4  5  6  7
-----
   dscp:  10 15 20 25 30 35 40 45
```

## Configuring the Policed-DSCP Map

You use the policed-DSCP map to mark down a DSCP value to a new value as the result of a policing and marking action.

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

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

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>mls qos map policed-dscp</b> <i>dscp-list</i> <b>to</b> <i>mark-down-dscp</i>	Modify the policed-DSCP map. <ul style="list-style-type: none"> <li>For <i>dscp-list</i>, enter up to 8 DSCP values separated by spaces. Then enter the <b>to</b> keyword.</li> <li>For <i>mark-down-dscp</i>, enter the corresponding policed (marked down) DSCP value.</li> </ul>
Step 3	<b>end</b>	Return to privileged EXEC mode.
Step 4	<b>show mls qos maps policed-dscp</b>	Verify your entries.
Step 5	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

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

This example shows how to map DSCP 50 to 57 to a marked-down DSCP value of 0:

```
Switch# configure terminal
Switch(config)# mls qos map policed-dscp 50 51 52 53 54 55 56 57 to 0
Switch(config)# end
Switch# show mls qos maps policed-dscp
Policed-dscp map:
  d1 :  d2 0  1  2  3  4  5  6  7  8  9
-----
  0 :    00 01 02 03 04 05 06 07 08 09
  1 :    10 11 12 13 14 15 16 17 18 19
  2 :    20 21 22 23 24 25 26 27 28 29
  3 :    30 31 32 33 34 35 36 37 38 39
  4 :    40 41 42 43 44 45 46 47 48 49
  5 :    00 00 00 00 00 00 00 00 58 59
  6 :    60 61 62 63
```



### Note

In this policed-DSCP map, the marked-down DSCP 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 marked-down value. For example, an original DSCP value of 53 corresponds to a marked-down DSCP value of 0.

## Configuring the DSCP-to-CoS Map

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

Table 27-5 shows the default DSCP-to-CoS map.

**Table 27-5 Default DSCP-to-CoS Map**

DSCP value	0–7	8–15	16–23	24–31	32–39	40–47	48–55	56–63
CoS value	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. <ul style="list-style-type: none"> <li>For <i>dscp-list</i>, enter up to 8 DSCP values separated by spaces. Then enter the <b>to</b> keyword.</li> <li>For <i>cos</i>, enter the CoS value to which the DSCP values correspond.</li> </ul> The DSCP range is 0 to 63; 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 dscp-cos` global configuration command.

This example shows how to map DSCP values 0, 8, 16, 24, 32, 40, 48, and 50 to CoS value 0 and to display the map:

```
Switch# configure terminal
Switch(config)# mls qos map dscp-cos 0 8 16 24 32 40 48 50 to 0
Switch(config)# end
Switch# show mls qos maps dscp-cos
Dscp-cos map:
  d1 :  d2 0  1  2  3  4  5  6  7  8  9
-----
  0 :   00 00 00 00 00 00 00 00 00 00 01
  1 :   01 01 01 01 01 01 00 02 02 02
  2 :   02 02 02 02 00 03 03 03 03 03
  3 :   03 03 00 04 04 04 04 04 04 04
  4 :   00 05 05 05 05 05 05 05 00 06
  5 :   00 06 06 06 06 06 06 07 07 07
  6 :   07 07 07 07
```



### Note

In the above DSCP-to-CoS map, the CoS values are shown in the body of the matrix. The d1 column specifies the most-significant digit of the DSCP; the d2 row specifies the least-significant digit of the DSCP. The intersection of the d1 and d2 values provides the CoS value. For example, in the DSCP-to-CoS map, a DSCP value of 08 corresponds to a CoS value of 0.

## Configuring the DSCP-to-DSCP-Mutation Map

You apply the DSCP-to-DSCP-mutation map to a port at the boundary of a QoS administrative domain. If the two domains have different DSCP definitions between them, you use the DSCP-to-DSCP-mutation map to translate a set of DSCP values to match the definition of the other domain.

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

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

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>mls qos map dscp-mutation</b> <i>dscp-mutation-name in-dscp to out-dscp</i>	Modify the DSCP-to-DSCP-mutation map. <ul style="list-style-type: none"> <li>For <i>dscp-mutation-name</i>, enter the mutation map name. You can create more than one map by specifying a new name.</li> <li>For <i>in-dscp</i>, enter up to 8 DSCP values separated by spaces. Then enter the <b>to</b> keyword.</li> <li>For <i>out-dscp</i>, enter up to 8 DSCP values separated by spaces.</li> </ul> The DSCP range is 0 to 63.
Step 3	<b>interface</b> <i>interface-id</i>	Enter interface configuration mode, and specify the interface to which to attach the map.  Valid interfaces include physical interfaces.
Step 4	<b>mls qos trust dscp</b>	Configure the ingress port as a DSCP-trusted port.
Step 5	<b>mls qos dscp-mutation</b> <i>dscp-mutation-name</i>	Apply the map to the specified ingress DSCP-trusted port.  For <i>dscp-mutation-name</i> , enter the mutation map name specified in Step 2.  You can apply the map to different Gigabit-capable Ethernet ports. However, on 10/100 Ethernet ports, you can attach only one DSCP-to-DSCP-mutation map to a group of twelve ports. For example, Fast Ethernet ports 0/1 to 0/12 are a group, Fast Ethernet ports 0/13 to 0/24 are a group, Gigabit Ethernet port 0/1 is a group, and Gigabit Ethernet port 0/2 is a group. When applying a mutation map to any port in a group, all ports in the same group are automatically configured with the same map.
Step 6	<b>end</b>	Return to privileged EXEC mode.
Step 7	<b>show mls qos maps dscp-mutation</b>	Verify your entries.
Step 8	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

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

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):

```
Switch# configure terminal
Switch(config)# mls qos map dscp-mutation mutation1 1 2 3 4 5 6 7 to 0
Switch(config)# mls qos map dscp-mutation mutation1 8 9 10 11 12 13 to 10
Switch(config)# mls qos map dscp-mutation mutation1 20 21 22 to 20
Switch(config)# mls qos map dscp-mutation mutation1 30 31 32 33 34 to 30
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# mls qos trust dscp
Switch(config-if)# mls qos dscp-mutation mutation1
Switch(config-if)# end
Switch# show mls qos maps dscp-mutation mutation1
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.

## Configuring Egress Queues on Gigabit-Capable Ethernet Ports

This section describes how to configure the egress queues on Gigabit-capable Ethernet ports. For information on configuring 10/100 Ethernet ports, see [“Configuring Egress Queues on 10/100 Ethernet Ports”](#) section on page 27-51.

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

- Which packets are assigned (by CoS value) to each queue?
- How much of the available buffer space (limit) is allotted to each queue?
- What drop percentage thresholds apply to each queue and which DSCP values map to each threshold?
- Is one of the queues the expedite (high-priority) egress queue?
- How much of the available bandwidth is allotted to each queue?

This section contains this configuration information:

- [Mapping CoS Values to Select Egress Queues, page 27-45](#)
- [Configuring the Egress Queue Size Ratios, page 27-46](#)
- [Configuring Tail-Drop Threshold Percentages, page 27-47](#)
- [Configuring WRED Drop Thresholds Percentages, page 27-48](#)
- [Configuring the Egress Expedite Queue, page 27-50](#)
- [Allocating Bandwidth among Egress Queues, page 27-50](#)

## Mapping CoS Values to Select Egress Queues

Beginning in privileged EXEC mode, follow these steps to map CoS ingress values to select one of the egress queues:

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>mls qos</b>	Enable QoS on the switch.
Step 3	<b>interface</b> <i>interface-id</i>	Enter interface configuration mode, and specify the egress Gigabit-capable Ethernet interface.
Step 4	<b>wrr-queue cos-map</b> <i>queue-id cos1 ... cos8</i>	Map assigned CoS values to select one of the egress queues.  The default map has these values: CoS value 0, 1 selects queue 1. CoS value 2, 3 selects queue 2. CoS value 4, 5 selects queue 3. CoS value 6, 7 selects queue 4.  <ul style="list-style-type: none"> <li>For <i>queue-id</i>, specify the ID of the egress queue. The range is 1 to 4, where 4 can be configured as the expedite queue. For more information, see the <a href="#">“Configuring the Egress Expedite Queue” section on page 27-50</a>.</li> <li>For <i>cos1 ... cos8</i>, specify the CoS values that select a queue. Enter up to eight CoS values. Separate each value with a space. The range is 0 to 7.</li> </ul>
Step 5	<b>end</b>	Return to privileged EXEC mode.
Step 6	<b>show mls qos interface queueing</b>	Verify your entries.
Step 7	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

To return the default CoS-to-egress-queue map, use the **no wrr-queue cos-map** [*queue-id*] interface configuration command.

This example shows how to map CoS values 6 and 7 to queue 1, 4 and 5 to queue 2, 2 and 3 to queue 3, 0 and 1 to queue 4.

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# wrr-queue cos-map 1 6 7
Switch(config-if)# wrr-queue cos-map 2 4 5
Switch(config-if)# wrr-queue cos-map 3 2 3
Switch(config-if)# wrr-queue cos-map 4 0 1
```

## Configuring the Egress Queue Size Ratios

Beginning in privileged EXEC mode, follow these steps to configure the egress queue size ratios:

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>mls qos</b>	Enable QoS on the switch.
Step 3	<b>interface</b> <i>interface-id</i>	Enter interface configuration mode, and specify the egress Gigabit-capable Ethernet interface.
Step 4	<b>wrr-queue queue-limit</b> <i>weight1 weight2 weight3 weight4</i>	Configure the egress queue size ratios. The defaults weights are 25 (1/4 of the buffer size is allocated to each queue). For <i>weight1</i> , <i>weight2</i> , <i>weight3</i> , and <i>weight4</i> , specify a weight from 1 to 100. Separate each value with a space. The relative size difference in the numbers indicates the relative differences in the queue sizes. The port enters a <i>halt</i> mode when this command is issued.
Step 5	<b>end</b>	Return to privileged EXEC mode.
Step 6	<b>show mls qos interface buffers</b>	Verify your entries.
Step 7	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

To return to the default weights, use the **no wrr-queue queue-limit** interface configuration command.

This example shows how to configure the size ratio of the four queues. The ratio of the size allocated for each queue is 1/10, 2/10, 3/10, and 4/10 to queue 1, 2, 3, and 4. (Queue 4 is four times larger than queue 1, twice as large as queue 2, and 1.33 times as large as queue 3.)

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# wrr-queue queue-limit 1 2 3 4
```

## Configuring Tail-Drop Threshold Percentages

Tail drop is the default congestion-avoidance technique on Gigabit-capable Ethernet ports. With tail drop, packets are queued until the thresholds are exceeded. For example, all packets with DSCPs assigned to the first threshold are dropped until the threshold is no longer exceeded. However, packets assigned to a second threshold continue to be queued and sent as long as the second threshold is not exceeded.

You modify the DSCP-to-threshold map to determine which DSCPs are mapped to which threshold ID by using the **wrr-queue dscp-map** interface configuration command. By default, all DSCPs are mapped to threshold 1, and when this threshold is exceeded, all the packets are dropped.

If you use tail-drop thresholds, you cannot use WRED, and vice versa.

Beginning in privileged EXEC mode, follow these steps to configure the tail-drop threshold percentage values on Gigabit-capable Ethernet ports:

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>mls qos</b>	Enable QoS on the switch.
Step 3	<b>interface</b> <i>interface-id</i>	Enter interface configuration mode, and specify the egress Gigabit-capable Ethernet interface.
Step 4	<b>wrr-queue threshold</b> <i>queue-id</i> <i>threshold-percentage1</i> <i>threshold-percentage2</i>	Configure tail-drop threshold percentages on each egress queue. The default threshold is 100 percent for thresholds 1 and 2. <ul style="list-style-type: none"> <li>For <i>queue-id</i>, specify the ID of the egress queue. The range is 1 to 4.</li> <li>For <i>threshold-percentage1 threshold-percentage2</i>, specify the tail-drop threshold percentage values. Separate each value with a space. The range is 1 to 100.</li> </ul>
Step 5	<b>exit</b>	Return to global configuration mode.
Step 6	<b>interface</b> <i>interface-id</i>	Enter interface configuration mode, and specify the ingress Gigabit-capable Ethernet interface.
Step 7	<b>wrr-queue dscp-map</b> <i>threshold-id dscp1</i> <i>... dscp8</i>	Map DSCP values to the tail-drop thresholds of the egress queues. By default, all DSCP values are mapped to threshold 1. <ul style="list-style-type: none"> <li>For <i>threshold-id</i>, specify the threshold ID of the queue. The range is 1 to 2.</li> <li>For <i>dscp1 ... dscp8</i>, specify the DSCP values that are mapped to the threshold ID. Enter up to eight DSCP values per command. Separate each value with a space. The range is 0 to 63.</li> </ul>
Step 8	<b>end</b>	Return to privileged EXEC mode.
Step 9	<b>show running-config</b>  or <b>show mls qos interface</b> <i>interface-id</i> <b>queueing</b>	Verify the DSCP-to-threshold map.
Step 10	<b>show mls qos interface buffers</b>	Verify the thresholds.
Step 11	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

To return to the default thresholds, use the **no wrr-queue threshold** *queue-id* interface configuration command. To return to the default DSCP-to-threshold map, use the **no wrr-queue dscp-map** [*threshold-id*] interface configuration command.

This example shows how to configure the tail-drop queue threshold values for queue 1 to 10 percent and 100 percent, for queue 2 to 40 percent and 100 percent, for queue 3 to 60 percent and 100 percent, and for queue 4 to 80 percent and 100 percent on the egress interface (Gigabit Ethernet 0/1). The ingress interface (Gigabit Ethernet 0/2) is configured to trust the DSCP in the incoming packets, to map DSCPs 0, 8, 16, 24, 32, 40, 48, and 56 to threshold 1, and to map DSCPs 10, 20, 30, 40, 50, and 60 to threshold 2:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport mode access
Switch(config-if)# wrr-queue threshold 1 10 100
Switch(config-if)# wrr-queue threshold 2 40 100
Switch(config-if)# wrr-queue threshold 3 60 100
Switch(config-if)# wrr-queue threshold 4 80 100
Switch(config-if)# exit
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# mls qos trust dscp
Switch(config-if)# wrr-queue dscp-map 1 0 8 16 24 32 40 48 56
Switch(config-if)# wrr-queue dscp-map 2 10 20 30 40 50 60
```

As a result of this configuration, when queue 1 is filled above 10 percent, packets with DSCPs 0, 8, 16, 24, 32, 40, 48, and 56 are dropped. The same packets are dropped when queue 2 is filled above 40 percent, queue 3 above 60 percent, and queue 4 above 80 percent. When the second threshold (100 percent) is exceeded, all queues drop packets with DSCPs 10, 20, 30, 40, 50, and 60.

## Configuring WRED Drop Thresholds Percentages

WRED reduces the chances of tail drop by selectively dropping packets when the output interface begins to show signs of congestion. By dropping some packets early rather than waiting until the queue is full, WRED avoids dropping large numbers of packets at once.

All packets with DSCPs assigned to the first threshold are randomly dropped when the first threshold is exceeded. However, packets with DSCPs assigned to the second threshold continue to be queued and sent as long as the second threshold is not exceeded. Each threshold percentage represents where WRED starts to randomly drop packets. By default, WRED is disabled.

Beginning in privileged EXEC mode, follow these steps to configure the WRED drop threshold percentage values on Gigabit-capable Ethernet ports:

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>mls qos</b>	Enable QoS on the switch.
Step 3	<b>interface</b> <i>interface-id</i>	Enter interface configuration mode, and specify the egress Gigabit-capable Ethernet interface.

	Command	Purpose
Step 4	<b>wrr-queue random-detect max-threshold</b> <i>queue-id</i> <i>threshold-percentage1</i> <i>threshold-percentage2</i>	Configure WRED drop threshold percentages on each egress queue. The default, WRED is disabled, and no thresholds are configured. <ul style="list-style-type: none"> <li>For <i>queue-id</i>, specify the ID of the egress queue. The range is 1 to 4, where queue 4 can be configured as the expedite queue. For more information, see the <a href="#">“Configuring the Egress Expedite Queue”</a> section on page 27-50.</li> <li>For <i>threshold-percentage1 threshold-percentage2</i>, specify the threshold percentage values. Separate each value with a space. The range is 1 to 100.</li> </ul>
Step 5	<b>exit</b>	Return to global configuration mode.
Step 6	<b>interface</b> <i>interface-id</i>	Enter interface configuration mode, and specify the ingress Gigabit-capable Ethernet interface.
Step 7	<b>wrr-queue dscp-map</b> <i>threshold-id dscp1</i> ... <i>dscp8</i>	Map DSCP values to the WRED drop thresholds of the egress queues. By default, all DSCP values are mapped to threshold 1. <ul style="list-style-type: none"> <li>For <i>threshold-id</i>, specify the threshold ID of the queue. The range is 1 to 2.</li> <li>For <i>dscp1 ... dscp8</i>, specify the DSCP values that are mapped to the threshold ID. Enter up to eight DSCP values per command. Separate each value with a space. The range is 0 to 63.</li> </ul>
Step 8	<b>show running-config</b>	Verify the DSCP-to-threshold map.
Step 9	<b>show mls qos interface buffers</b>	Verify the thresholds.
Step 10	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

To disable WRED, use the **no wrr random-detect max-threshold** [*queue-id*] interface configuration command. To return to the default DSCP-to-threshold map, use the **no wrr-queue dscp-map** [*threshold-id*] interface configuration command.

This example shows how to configure the WRED queue threshold values for queue 1 to 50 percent and 100 percent, for queue 2 to 70 percent and 100 percent, for queue 3 to 50 percent and 100 percent, and for queue 4 to 70 percent and 100 percent on the egress interface (Gigabit Ethernet 0/1). The ingress interface (Gigabit Ethernet 0/2) is configured to trust the DSCP in the incoming packets, to map DSCPs 0, 8, 16, 24, 32, 40, 48, and 56 to threshold 1, and to map DSCPs 10, 20, 30, 40, 50, and 60 to threshold 2.

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# wrr-queue random-detect max-threshold 1 50 100
Switch(config-if)# wrr-queue random-detect max-threshold 2 70 100
Switch(config-if)# wrr-queue random-detect max-threshold 3 50 100
Switch(config-if)# wrr-queue random-detect max-threshold 4 70 100
Switch(config-if)# exit
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# mls qos trust dscp
Switch(config-if)# wrr-queue dscp-map 1 0 8 16 24 32 40 48 56
Switch(config-if)# wrr-queue dscp-map 2 10 20 30 40 50 60
```

As a result of this configuration, when the queues 1 and 3 are filled above 50 percent, packets with DSCPs 0, 8, 16, 24, 32, 40, 48, and 56 are randomly dropped. The same packets are randomly dropped when queues 2 and 4 are filled above 70 percent. When the second threshold (100 percent) is exceeded, all queues randomly drop packets with DSCPs 10, 20, 30, 40, 50, and 60.

## Configuring the Egress Expedite Queue

You can ensure that certain packets have priority over all others by queuing them in the egress expedite queue. This queue is serviced until it is empty and before the other queues are serviced.

Beginning in privileged EXEC mode, follow these steps to enable the egress expedite queue:

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>mls qos</b>	Enable QoS on the switch.
Step 3	<b>interface</b> <i>interface-id</i>	Enter interface configuration mode, and specify the egress Gigabit-capable Ethernet interface.
Step 4	<b>priority-queue out</b>	Enable the egress expedite queue, which is disabled by default.  When you configure this command, the WRR weight and queue size ratios are affected because there is one fewer queue participating in WRR. This means that <i>weight4</i> in the <b>wrr-queue bandwidth</b> command is ignored (not used in the ratio calculation).
Step 5	<b>end</b>	Return to privileged EXEC mode.
Step 6	<b>show running-config</b>	Verify your entries.
Step 7	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

To disable the egress expedite queue, use the **no priority-queue out** interface configuration command.

## Allocating Bandwidth among Egress Queues

You need to 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 WRR scheduler drops packets from each queue.

Beginning in privileged EXEC mode, follow these steps to allocate bandwidth to each queue:

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>mls qos</b>	Enable QoS on the switch.
Step 3	<b>interface</b> <i>interface-id</i>	Enter interface configuration mode, and specify the egress Gigabit-capable Ethernet interface.

	Command	Purpose
Step 4	<b>wrr-queue bandwidth</b> <i>weight1 weight2 weight3 weight4</i>	Assign WRR weights to the egress queues.  By default, all the weights are set to 25 (1/4 of the bandwidth is allocated to each queue).  For <i>weight1 weight2 weight3 weight4</i> , enter the ratio, which determines the ratio of the frequency in which the WRR scheduler drops packets. Separate each value with a space. The range is 0 to 65536.  All four queues participate in the WRR unless the expedite queue (queue 4) is enabled, in which case <i>weight4</i> is ignored (not used in the ratio calculation). The expedite queue is a strict-priority queue, and it is serviced until empty before the other queues are serviced.  A weight of 0 means no bandwidth is allocated for that queue, and the available bandwidth is shared among the remaining queues.
Step 5	<b>end</b>	Return to privileged EXEC mode.
Step 6	<b>show mls qos interface queueing</b>	Verify your entries.
Step 7	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

To return to the default bandwidth setting, use the **no wrr-queue bandwidth** interface configuration command.

This example shows how to configure the weight ratio of the WRR scheduler running on the egress queues. In this example, four queues are used (no expedite queue), and the ratio of the bandwidth allocated for each queue is  $1/(1+2+3+4)$ ,  $2/(1+2+3+4)$ ,  $3/(1+2+3+4)$ , and  $4/(1+2+3+4)$ , which is 1/10, 1/5, 3/10, and 2/5 for queues 1, 2, 3, and 4.

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# wrr-queue bandwidth 1 2 3 4
```

## Configuring Egress Queues on 10/100 Ethernet Ports

This section describes how to configure the egress queues on 10/100 Ethernet ports. For information on configuring Gigabit-capable Ethernet ports, see the [“Configuring Egress Queues on Gigabit-Capable Ethernet Ports”](#) section on page 27-44.

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

- Which packets are assigned (by CoS value) to each queue?
- How much of the available buffer space is allotted to each queue?
- Is one of the queues the expedite (high-priority) egress queue?
- How much of the available bandwidth is allotted to each queue?

This section contains this configuration information:

- [Mapping CoS Values to Select Egress Queues, page 27-52](#)
- [Configuring the Minimum-Reserve Levels, page 27-53](#)
- [Configuring the Egress Expedite Queue, page 27-54](#)
- [Allocating Bandwidth among Egress Queues, page 27-54](#)

## Mapping CoS Values to Select Egress Queues

Beginning in privileged EXEC mode, follow these steps to map CoS ingress values to select one of the egress queues:

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>mls qos</b>	Enable QoS on the switch.
Step 3	<b>interface</b> <i>interface-id</i>	Enter interface configuration mode, and specify the egress 10/100 Ethernet interface.
Step 4	<b>wrr-queue cos-map</b> <i>queue-id cos1 ... cos8</i>	Map assigned CoS values to select one of the egress queues.  These are the default map values: CoS value 0, 1 selects queue 1. CoS value 2, 3 selects queue 2. CoS value 4, 5 selects queue 3. CoS value 6, 7 selects queue 4.  <ul style="list-style-type: none"> <li>• For <i>queue-id</i>, specify the ID of the egress queue. The range is 1 to 4, where 4 can be configured as the expedite queue. For more information, see the <a href="#">“Configuring the Egress Expedite Queue” section on page 27-54</a>.</li> <li>• For <i>cos1 ... cos8</i>, specify the CoS values that select a queue. Enter up to eight CoS values. Separate each value with a space. The range is 0 to 7.</li> </ul>
Step 5	<b>end</b>	Return to privileged EXEC mode.
Step 6	<b>show mls qos interface queueing</b>	Verify your entries.
Step 7	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

To return to the default CoS-to-egress-queue map, use the **no wrr-queue cos-map** [*queue-id*] interface configuration command.

This example shows how to map CoS values 6 and 7 to queue 1, 4 and 5 to queue 2, 2 and 3 to queue 3, and 0 and 1 to queue 4.

```
Switch(config)# interface fastethernet0/1
Switch(config-if)# wrr-queue cos-map 1 6 7
Switch(config-if)# wrr-queue cos-map 2 4 5
Switch(config-if)# wrr-queue cos-map 3 2 3
Switch(config-if)# wrr-queue cos-map 4 0 1
```

## Configuring the Minimum-Reserve Levels

You can configure the buffer size of the minimum-reserve levels on all 10/100 ports and assign the minimum-reserve level to an egress queue on a 10/100 Ethernet port.

Beginning in privileged EXEC mode, follow these steps to configure the egress queue sizes:

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>mls qos</b>	Enable QoS on the switch.
Step 3	<b>mls qos min-reserve</b> <i>min-reserve-level</i> <i>min-reserve-buffersize</i>	Configure the buffer size of the minimum-reserve level, if necessary, for all the 10/100 Ethernet ports.  By default, the buffer size for all eight minimum-reserve levels is set to 100 packets. <ul style="list-style-type: none"> <li>For <i>min-reserve-level</i>, specify the minimum-reserve level number. The range is 1 to 8.</li> <li>For <i>min-reserve-buffersize</i>, specify the buffer size. The range is 10 to 170 packets.</li> </ul>
Step 4	<b>interface</b> <i>interface-id</i>	Enter interface configuration mode, and specify the egress 10/100 Ethernet interface.
Step 5	<b>wrr-queue min-reserve</b> <i>queue-id</i> <i>min-reserve-level</i>	Assign a minimum-reserve level number to a particular egress queue.  By default, queue 1 selects minimum-reserve level 1, queue 2 selects minimum-reserve level 2, queue 3 selects minimum-reserve level 3, and queue 4 selects minimum-reserve level 4. <ul style="list-style-type: none"> <li>For <i>queue-id</i>, specify the ID of the egress queue. The range is 1 to 4, where 4 can be configured as the expedite queue. For more information, see the <a href="#">“Configuring the Egress Expedite Queue” section on page 27-54</a>.</li> <li>For <i>min-reserve-level</i>, specify the minimum-reserve level configured in Step 3.</li> </ul>
Step 6	<b>end</b>	Return to privileged EXEC mode.
Step 7	<b>show mls qos interface buffers</b>	Verify your entries.
Step 8	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

To return to the default minimum-reserve buffer size, use the **no mls qos min-reserve** *min-reserve-level* global configuration command. To return to the default queue selection of the minimum-reserve level, use the **no wrr-queue min-reserve** *queue-id* interface configuration command.

This example shows how to configure minimum-reserve level 5 to 20 packets and to assign minimum-reserve level 5 to egress queue 1 on the Fast Ethernet 0/1 interface 0/1:

```
Switch(config)# mls qos min-reserve 5 20
Switch(config)# interface fastethernet0/1
Switch(config-if)# wrr-queue min-reserve 1 5
```

## Configuring the Egress Expedite Queue

You can ensure that certain packets have priority over all others by queuing them in the egress expedite queue. This queue is serviced until it is empty and before the other queues are serviced.

Beginning in privileged EXEC mode, follow these steps to enable the egress expedite queue:

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>mls qos</b>	Enable QoS on the switch.
Step 3	<b>interface</b> <i>interface-id</i>	Enter interface configuration mode, and specify the egress 10/100 Ethernet interface.
Step 4	<b>priority-queue out</b>	Enable the egress expedite queue, which is disabled by default.  When you configure this command, the WRR weight is affected because there is one fewer queue participating in WRR. This means that <i>weight4</i> in the <b>wrr-queue bandwidth</b> command is ignored (not used in the ratio calculation).
Step 5	<b>end</b>	Return to privileged EXEC mode.
Step 6	<b>show running-config</b>	Verify your entries.
Step 7	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

To disable the egress expedite queue, use the **no priority-queue out** interface configuration command.

## Allocating Bandwidth among Egress Queues

You need to 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 WRR scheduler drops packets from each queue.

Beginning in privileged EXEC mode, follow these steps to allocate bandwidth to each queue:

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>mls qos</b>	Enable QoS on the switch.
Step 3	<b>interface</b> <i>interface-id</i>	Enter interface configuration mode, and specify the egress 10/100 Ethernet interface.

	Command	Purpose
Step 4	<b>wrr-queue bandwidth</b> <i>weight1 weight2 weight3 weight4</i>	<p>Assign WRR weights to the egress queues.</p> <p>By default, all the weights are set to 25 (1/4 of the bandwidth is allocated to each queue).</p> <p>For <i>weight1 weight2 weight3 weight4</i>, enter the ratio, which determines the ratio of the frequency in which the WRR scheduler drops packets. Separate each value with a space. The range is 0 to 65536.</p> <p>All four queues participate in the WRR unless the expedite queue (queue 4) is enabled, in which case <i>weight4</i> is ignored (not used in the ratio calculation). The expedite queue is a strict-priority queue, and it is serviced until empty before the other queues are serviced.</p> <p>A weight of 0 means no bandwidth is allocated for that queue, and the available bandwidth is shared among the remaining queues.</p>
Step 5	<b>end</b>	Return to privileged EXEC mode.
Step 6	<b>show mls qos interface queueing</b>	Verify your entries.
Step 7	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

To return to the default bandwidth setting, use the **no wrr-queue bandwidth** interface configuration command.

This example shows how to configure the weight ratio of the WRR scheduler running on the egress queues. In this example, four queues are used (no expedite queue), and the ratio of the bandwidth allocated for each queue is  $1/(1+2+3+4)$ ,  $2/(1+2+3+4)$ ,  $3/(1+2+3+4)$ , and  $4/(1+2+3+4)$ , which is 1/10, 2/10, 3/10, and 4/10 for queues 1, 2, 3, and 4.

```
Switch(config)# interface fastethernet0/1
Switch(config-if)# wrr-queue bandwidth 1 2 3 4
```

# Displaying QoS Information

To display QoS information, use one or more of the privileged EXEC commands in [Table 27-6](#):

**Table 27-6** Commands for Displaying QoS Information

Command	Purpose
<code>show class-map [class-map-name]</code>	Display QoS class maps, which define the match criteria to classify traffic.
<code>show policy-map [policy-map-name [class class-name]   interface interface-id]</code>	Display QoS policy maps, which define classification criteria for incoming traffic.
<code>show mls qos aggregate-policer [aggregate-policer-name]</code>	Display the aggregate policer configuration.
<code>show mls qos maps [cos-dscp   dscp-cos   dscp-mutation   ip-prec-dscp   policed-dscp]</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] [buffers   policers   queueing   statistics]</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). <sup>1</sup>

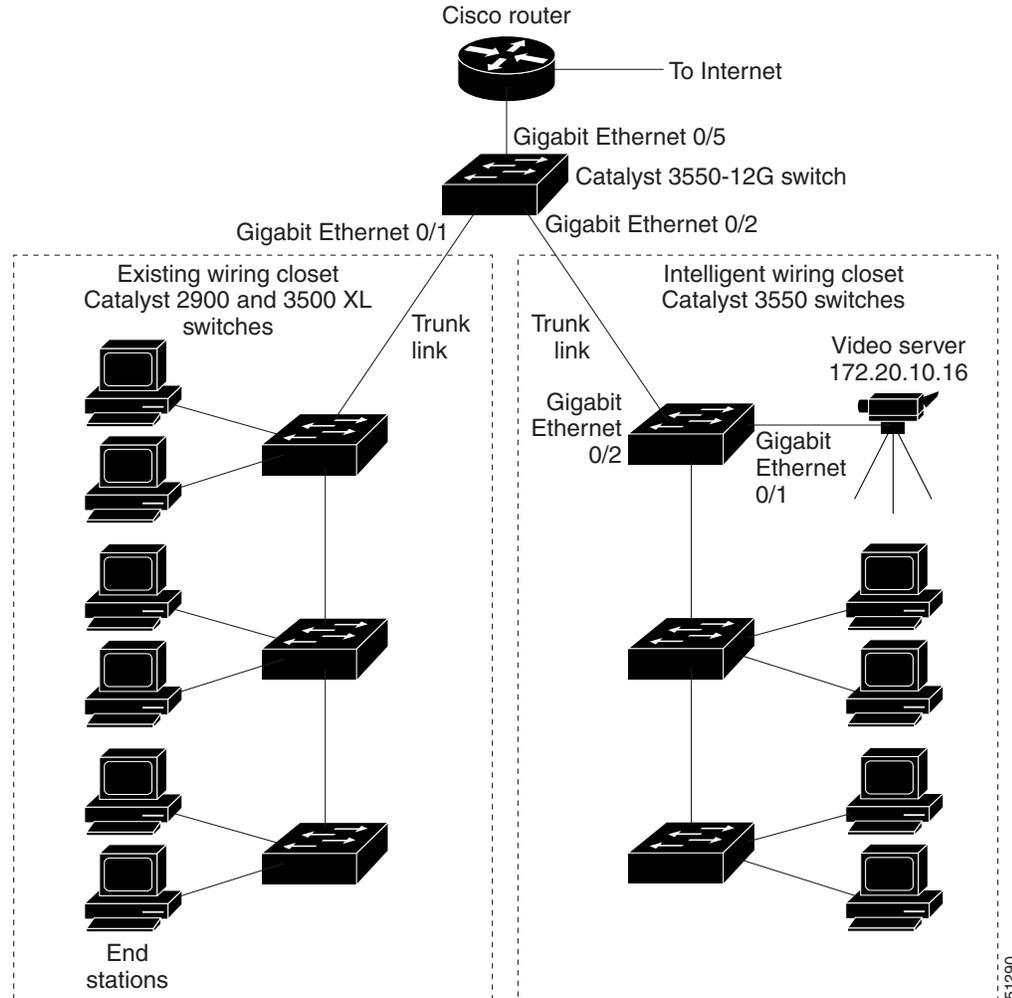
1. You can define up to 16 DSCP values for which byte or packet statistics are gathered by hardware by using the `mls qos monitor {bytes | dscp dscp1 ... dscp8 | packets}` interface configuration command and the `show mls qos interface statistics` privileged EXEC command.

## QoS Configuration Examples

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 27-10](#). It contains this information:

- [QoS Configuration for the Common Wiring Closet, page 27-57](#)
- [QoS Configuration for the Intelligent Wiring Closet, page 27-58](#)
- [QoS Configuration for the Distribution Layer, page 27-59](#)

Figure 27-10 QoS Configuration Example Network



## QoS Configuration for the Common Wiring Closet

The common wiring closet in [Figure 27-10](#) consists of existing Catalyst 3500 XL and 2900 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 3500 XL and 2900 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 ISL or 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 3500 XL, 2950, other 2900 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 3500 XL and 2900 XL switches, CoS configures each 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 whereas 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 27-10](#) is composed of Catalyst 3550 multilayer 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 56 is assigned to the video traffic. This traffic is stored in the expedite queue (queue 4), which is serviced until empty before the other queues are serviced. The appropriate CoS value selects queue 4 in the CoS-to-egress-queue map.

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

	Command	Purpose
Step 1	<code>configure terminal</code>	Enter global configuration mode.
Step 2	<code>access-list 1 permit 172.20.10.16</code>	Define an IP standard ACL, and permit traffic from the video server at 172.20.10.16.
Step 3	<code>class-map videoclass</code>	Create a class map called <i>videoclass</i> , and enter class-map configuration mode.
Step 4	<code>match access-group 1</code>	Define the match criterion by matching the traffic specified by access list 1.
Step 5	<code>exit</code>	Return to global configuration mode.
Step 6	<code>policy-map videopolicy</code>	Create a policy map called <i>videopolicy</i> , and enter policy-map configuration mode.
Step 7	<code>class videoclass</code>	Specify the class on which to act, and enter policy-map class configuration mode.
Step 8	<code>set ip dscp 56</code>	For traffic matching ACL 1, set the DSCP of incoming packets to 56.
Step 9	<code>police 5000000 2000000 exceed-action drop</code>	Define a policer for the classified video traffic to drop traffic that exceeds 5-Mbps average traffic rate with a 2-MB burst size.
Step 10	<code>exit</code>	Return to policy-map configuration mode.
Step 11	<code>exit</code>	Return to global configuration mode.
Step 12	<code>interface gigabitethernet0/1</code>	Enter interface configuration mode, and specify the ingress interface.
Step 13	<code>service-policy input videopolicy</code>	Apply the policy to the ingress interface.
Step 14	<code>exit</code>	Return to global configuration mode.
Step 15	<code>interface gigabitethernet0/2</code>	Enter interface configuration mode, and specify the egress interface (to configure the queues).
Step 16	<code>priority-queue out</code>	Enable the expedite queue.

	Command	Purpose
Step 17	<b>wrr-queue cos-map 4 6 7</b>	Configure the CoS-to-egress-queue map so that CoS values 6 and 7 select queue 4 (this is the default setting).  Because the default DSCP-to-CoS map has DSCP values 56 to 63 mapped to CoS value 7, the matched traffic that is set to DSCP 56 goes to the queue 4, the priority queue.
Step 18	<b>end</b>	Return to privileged EXEC mode.
Step 19	<b>show class-map videoclass</b> <b>show policy-map videopolicy</b> <b>show mls qos maps [cos-dscp   dscp-cos]</b> <b>show mls qos interface queueing</b>	Verify your entries.
Step 20	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

## QoS Configuration for the Distribution Layer

This example focuses on the configuration steps for the Catalyst 3550-12G multilayer switch at the distribution layer (see [Figure 27-10](#)). Because the classification was performed by the switches at the edge of the network, fewer classification steps are needed at the distribution layer switch.

For the connection to the common wiring closet, Gigabit Ethernet interface 0/1 on the multilayer switch is configured to trust the received CoS value. In this situation, the default CoS-to-DSCP map on the multilayer switch is sufficient. For information on the default map settings, see the [“Configuring the CoS-to-DSCP Map”](#) section on page 27-39.

For the connection to the intelligent wiring closet, Gigabit Ethernet interface 0/2 on the multilayer switch is configured to trust the received DSCP value. The DSCP-to-threshold map also needs to be configured on this ingress interface so that on the egress interface, WRED can provide congestion avoidance control. By default, all DSCP values are mapped to threshold 1.

You need to configure several of the switch maps from their default settings. The object of the configuration is to have only DSCP value 56 sent to the expedite queue (queue 4). The default CoS-to-egress-queue map is sufficient; however, you need to configure the DSCP-to-CoS map so that DSCP values 57 to 63 map to CoS 5.

For the egress interface, Gigabit Ethernet interface 0/5, WRR weights need to be configured by using the **wrr-queue bandwidth** interface configuration command. WRED needs to be enabled and the threshold percentages configured for each queue. The bandwidth allocated to each queue must be configured to determine the ratio of the frequency at which packets are dropped from the queue.

Beginning in privileged EXEC mode, follow these steps to configure the multilayer switch at the distribution layer:

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>mls qos</b>	Enable QoS on the switch.
Step 3	<b>interface gigabitethernet0/1</b>	Enter interface configuration mode, and specify the ingress interface that is connected to the common wiring closet.
Step 4	<b>mls qos trust cos</b>	Classify incoming packets on this port by using the packet CoS value.

	Command	Purpose
Step 5	<b>switchport mode trunk</b>	Configure this port as a trunk port.
Step 6	<b>exit</b>	Return to global configuration mode.
Step 7	<b>interface gigabitethernet0/2</b>	Enter interface configuration mode, and specify the ingress interface connected to the intelligent wiring closet.
Step 8	<b>mls qos trust dscp</b>	Classify incoming packets on this port by using the packet DSCP value.
Step 9	<b>wrr-queue dscp-map</b> <i>threshold-id</i> <i>dscp1 ... dscp8</i>	Map the ingress DSCP values to the WRED thresholds of the egress queues.  In the default DSCP-to-threshold map, all DSCP values are mapped to threshold 1. <ul style="list-style-type: none"> <li>For <i>threshold-id</i>, specify the threshold ID of the queue. The range is 1 to 2.</li> <li>For <i>dscp1 ... dscp8</i>, specify the DSCP values that are mapped to a threshold ID. Enter up to eight DSCP values per command. Separate each value with a space. The DSCP range is 0 to 63.</li> </ul>
Step 10	<b>switchport mode trunk</b>	Configure this port as a trunk port.
Step 11	<b>exit</b>	Return to global configuration mode.
Step 12	<b>mls qos map dscp-cos</b> <i>dscp-list to cos</i>	Modify the DSCP-to-CoS map. You can enter up to eight DSCP values separated by spaces in the DSCP-to-CoS map.  For example, to map DSCP values 57 to 63 to CoS 5, enter: <b>mls qos map dscp-cos 57 58 59 60 61 62 63 to 5</b>
Step 13	<b>interface gigabitethernet0/5</b>	Enter interface configuration mode, and specify the egress interface to configure.
Step 14	<b>priority-queue out</b>	Enable the expedite queue.
Step 15	<b>wrr-queue bandwidth</b> <i>weight1 weight2</i> <i>weight3 weight4</i>	Configure WRR weights to the egress queues to determine the ratio of the frequency at which packets are dropped. Separate each value with a space. The weight range is 0 to 65536.  In this example, to configure the weights so that queue 4 is serviced more frequently than the other queues, enter: <b>wrr-queue bandwidth 1 2 3 4</b>  Because the expedite queue is enabled, only the first three weights are used in the ratio calculation.
Step 16	<b>wrr-queue random-detect</b> <b>max-threshold</b> <i>queue-id</i> <i>threshold-percentage1</i> <i>threshold-percentage2</i>	Enable WRED and assign two WRED threshold values to an egress queue of a Gigabit-capable Ethernet port. <ul style="list-style-type: none"> <li>For <i>queue-id</i>, the range is 1 to 4.</li> <li>For <i>threshold-percentage1 threshold-percentage2</i>, the range is 1 to 100 percent.</li> </ul> In this example, to configure the thresholds, enter: <b>wrr-queue random-detect max-threshold 1 20 100</b> <b>wrr-queue random-detect max-threshold 2 40 100</b> <b>wrr-queue random-detect max-threshold 3 60 100</b> <b>wrr-queue random-detect max-threshold 4 80 100</b>

	<b>Command</b>	<b>Purpose</b>
<b>Step 17</b>	<b>end</b>	Return to privileged EXEC mode.
<b>Step 18</b>	<b>show mls qos interface</b> and <b>show interfaces</b>	Verify your entries.
<b>Step 19</b>	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

