CHAPTER 25

Configuring QoS

This chapter describes how to configure quality of service (QoS) using standard QoS commands. With QoS, you can provide preferential treatment to certain types of 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.

You can configure these basic QoS features on physical ports of the switch.

- IEEE 802.1p class of service (CoS)
- Four egress queues per port to enable differentiated management of different traffic types across the stack

Note For complete syntax and usage information for the commands used in this chapter, see the command reference this release.

This chapter consists of these sections:

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 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.

- Prioritization bits in Layer 2 frames:

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

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. 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 with this task.

Switches and routers along the path can use the class information to limit the amount of resources allocated per traffic class. The behavior of an individual device when handling traffic in the 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

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

Actions at the egress port include queueing and scheduling:

- Queueing evaluates the QoS packet label and the corresponding CoS value before selecting which of the four egress queues to use. For more information, see the "Configuring QoS" section on page 25-3.

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.

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

The QoS label is based on the CoS value in the packet and decides the queueing and scheduling actions to perform on the packet. The label is mapped according to the trust setting and the packet type.

For non-IP and IP traffic, you can configure the ports as trusted. Classification is performed on ingress packets by using the packet CoS value. The default CoS value is 0 which means best-effort traffic. The default port trust state is untrusted.

Configuring QoS

These sections contain this configuration information:

Default QoS Configuration

QoS is disabled. There is no concept of trusted or untrusted ports because the packets are not modified (the CoS value in the packet is not changed). Traffic is switched in pass-through mode (packets are switched without any rewrites and classified as best effort).

When QoS is enabled with the **mls qos** global configuration command and all other QoS settings are at their defaults, traffic is classified as best effort (the CoS value is set to 0. The default port trust state on all ports is untrusted. The default egress queue settings are described in the "Default Egress Queue Configuration" section on page 25-3.

Default Egress Queue Configuration

Table 25-1 shows the default egress queue configuration for each queue-set when QoS is enabled. All ports are mapped to queue-set 1. The port bandwidth limit is set to 100 percent and rate unlimited.

Table 25-1 Default Egress Queue Configuration

Feature	Queue 1	Queue 2	Queue 3	Queue 4
Buffer allocation	25 percent	25 percent	25 percent	25 percent
Threshold 1	100 percent	200 percent	100 percent	100 percent
Threshold 2	100 percent	200 percent	100 percent	100 percent
Reserved threshold	50 percent	50 percent	50 percent	50 percent
Maximum threshold	400 percent	400 percent	400 percent	400 percent

Table 25-2 shows the default CoS output queue threshold map when QoS is enabled.

Table 25-2 Default CoS Output Queue Threshold Map

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

Standard QoS Configuration Guidelines

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

- "Applying QoS on Interfaces" section on page 25-4
- "General QoS Guidelines" section on page 25-4

Applying QoS on Interfaces

These are the guidelines for configuring QoS on physical ports. This section also applies to SVIs:

- You can configure QoS on physical ports and SVIs.

General QoS Guidelines

These are general QoS guidelines:

- Control traffic (such as spanning-tree bridge protocol data units [BPDUs] and routing update packets) received by the switch are subject to all ingress QoS processing.
- You are likely to lose data when you change queue settings; therefore, try to make changes when traffic is at a minimum.

Enabling QoS Globally

By default, QoS is disabled on the switch.

Beginning in privileged EXEC mode, follow these steps to enable QoS. This procedure is required.

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**mls qos**	Enable QoS globally. QoS runs with the default settings described in the "Default QoS Configuration" section on page 25-3.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show mls qos**	Verify your entries.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

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

Configuring Classification Using Port Trust States

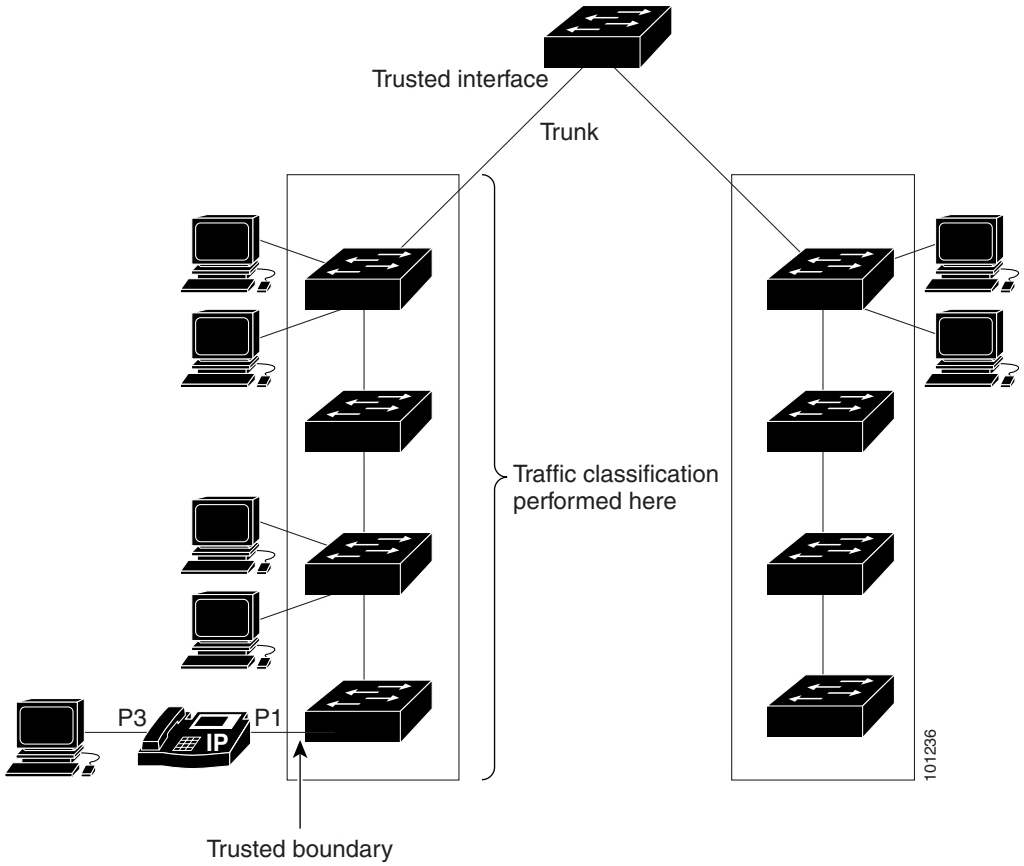
These sections describe how to classify incoming traffic by using port trust states. Depending on your network configuration, you must perform one or more of these tasks:

- Configuring the Trust State on Ports within the QoS Domain, page 25-5
- Configuring the CoS Value for an Interface, page 25-6
- Configuring a Trusted Boundary to Ensure Port Security, page 25-7

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 25-1 shows a sample network topology.

Figure 25-1 Port Trusted States within the QoS Domain



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

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Specify the port to be trusted, and enter interface configuration mode. Valid interfaces include physical ports.
Step 3	**mls qos trust** [**cos**]	Configure the port trust state. • **cos**—Classifies an ingress packet by using the packet CoS value. For an untagged packet, the port default CoS value is used. The default port CoS value is 0.

	Command	Purpose
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show mls qos interface**	Verify your entries.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To return 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 25-6.

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	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Specify the port to be configured, and enter interface configuration mode. Valid interfaces include physical ports.
Step 3	**mls qos cos** {*default-cos* | **override**}	Configure the default CoS value for the port. • For *default-cos,* specify a default CoS value to be assigned to a port. If the packet is untagged, the default CoS value becomes the packet CoS value. The CoS range is 0 to 7. The default is 0. • Use the **override** keyword to override the previously configured trust state of the incoming packet and to apply the default port CoS value to the port on all incoming packets. By default, CoS override is disabled. Use the **override** keyword when all incoming packets on specified ports deserve higher or lower priority than packets entering from other ports. Even if a port was previously set to trust CoS, this command overrides the previously configured trust state, and all the incoming CoS values are assigned the default CoS value configured with this command. If an incoming packet is tagged, the CoS value of the packet is modified with the default CoS of the port at the ingress port.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show mls qos interface**	Verify your entries.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

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

Configuring a Trusted Boundary to Ensure Port Security

In a typical network, you connect a device to a switch port, as shown in Figure 25-1 on page 25-5, and you can cascade other devices that generate data packets. The connected device guarantees the quality through a shared data link by marking the CoS level of some packets as high priority (CoS = 5) and by marking other packets as low priority (CoS = 0). Traffic sent from the device to the switch is typically marked with a tag that uses the 802.1Q header. The header contains the VLAN information and the class of service (CoS) 3-bit field, which is the priority of the packet.

For many configurations, the traffic sent from the device to the switch should be trusted to ensure that the traffic is properly prioritized over other types of traffic in the network. By using the **mls qos trust cos** interface configuration command, you configure the switch port to which the device is connected to trust the CoS labels of all traffic received on that port.

With the trusted setting, you also can use the trusted boundary feature to prevent misuse of a high-priority queue if a user bypasses the device and connects the PC directly to the switch. Without trusted boundary, the CoS labels generated by the PC are trusted by the switch (because of the trusted CoS setting). By contrast, trusted boundary uses CDP to detect the presence of other devices on a switch port. If the device is not detected, the trusted boundary feature disables the trusted setting on the switch port and prevents misuse of a high-priority queue.

In some situations, you can prevent a PC connected to the device from taking advantage of a high-priority data queue. You can use the **switchport priority extend cos** interface configuration command to configure the device through the switch CLI to override the priority of the traffic received from the PC.

Beginning in privileged EXEC mode, follow these steps to enable trusted boundary on a port:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**cdp run**	Enable CDP globally. By default, CDP is enabled.
Step 3	**interface** *interface-id*	Specify the port connected to a device, and enter interface configuration mode. Valid interfaces include physical ports.
Step 4	**cdp enable**	Enable CDP on the port. By default, CDP is enabled.
Step 5	**mls qos trust cos**	Configure the switch port to trust the CoS value in traffic received from the device. By default, the port is not trusted.
Step 6	**switchport priority extend** {**cos** *value* | **trust**}	Configure the device through the switch CLI to override the priority of the traffic received from the PC.
Step 7	**end**	Return to privileged EXEC mode.
Step 8	**show mls qos interface**	Verify your entries.
Step 9	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To disable the trusted boundary feature, use the **no mls qos trust device** interface configuration command.

Configuring the Egress Expedite Queue

You can ensure that certain packets have priority over all others by queuing them in the egress expedite queue.

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

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**mls qos**	Enable QoS on a switch.
Step 3	**interface** *interface-id*	Specify the egress port, and enter interface configuration mode.
Step 4	**priority-queue out**	Enable the egress expedite queue, which is disabled by default.
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**show running-config**	Verify your entries.
Step 7	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

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

Displaying QoS Information

To display QoS information, use one or more of the privileged EXEC commands in Table 25-3:

Table 25-3 Commands for Displaying Standard QoS Information

Command	Purpose
show mls qos	Display global QoS configuration information.
show mls qos interface [*interface-id*] [**buffers** |**queueing** | **statistics**]	Display QoS information at the port level, including the buffer allocation, the queueing strategy, and the ingress and egress statistics.
show mls qos queue-set [*qset-id*]	Display QoS settings for the egress queues.