CHAPTER 7

Marking Traffic

To service the growing numbers of customers and their needs, service provider networks have become more complex and often include both Layer 2 and Layer 3 network devices. With this continued growth, service providers must quickly identify the packets streaming across the network and apply the appropriate service behavior before sending them to their destinations.

A differentiated service (DiffServ) model enables you to classify packets based on traffic classes. In this model, traffic marking allows you to partition your network into multiple priority levels or classes of service. By marking traffic, other network devices along the forwarding path can quickly determine the proper class of service (CoS) to apply to a traffic flow.

An important aspect of DiffServ is that the markings must be consistently interpreted from end-to-end. All devices in the network path must understand the per-hop behavior to apply to a specific class of traffic. If one of the routers in the path does not act appropriately, the overall service for a particular packet might not be as desired.

This chapter describes the marking capabilities of the Cisco 10000 series router. It includes the following topics:

QoS Packet Marking

QoS packet marking is a QoS tool used to differentiate packets based on designated markings. Using marking, you can partition your network into multiple priority levels or classes of service. Marking simplifies the network Qos design and QoS tools configuration, and reduces the overhead of packet classification by other QoS tools.

You can configure QoS packet marking on a main interface, subinterface, or an individual virtual circuit (VC). Traffic marking involves setting bits inside frame, packet, or cell header fields that are specifically designed for QoS marking. Other devices can examine the marked bits and classify traffic based on the marked values.

Table 7-1 summarizes the mechanisms you can use to mark packets. The internal mechanisms affect only the Cisco 10000 series router's behavior; internal marks are not passed on to other routers.

Table 7-1 Traffic Marking Actions

Action	Description	Layer	Section Reference
atm-clp	Sets the ATM cell loss priority (CLP) bit to 1.	2	ATM Cell Loss Priority Marking, page 7-14
cos	Sets the IEEE 802.1Q class of service bits in the user priority field.	2	Class of Service Marking, page 7-10
discard-class	Marks a packet with the discard-class value that you specify, which indicates the drop eligibility of a packet.	Internal	Discard-Class Marking, page 7-16
dscp	Marks a packet with the differentiated services code point (DSCP) you specify.	3	IP Differentiated Services Code Point Marking, page 7-6
mpls experimental imposition	Sets the value of the MPLS experimental (EXP) field on all imposed label entries.	2	MPLS Experimental Marking, page 7-14
ip precedence	Marks a packet with the IP precedence level you specify.	3	IP Precedence Marking, page 7-4
qos-group	Marks a packet with the QoS group identifier you specify.	Internal	QoS Group Marking, page 7-13

Feature History for QoS Packet Marking

Cisco IOS Release	Description	Required PRE
Release 12.0(17)SL	The marking feature was introduced on the router.	PRE1
Release 12.0(22)S	This feature was enhanced to support MPLS experimental marking.	PRE1
Release 12.2(16)BX	This feature was introduced on the PRE2 and enhanced to support 802.1Q class of service marking.	PRE2
Release 12.3(7)XI1	This feature was enhanced on the PRE2 to support MPLS experimental marking on all imposed label entries and discard-class marking.	PRE2
Release 12.2(28)SB	This feature was integrated in Cisco IOS Release 12.2(28)SB for the PRE2.	PRE2
Release 12.2(31)SB2	This feature was introduced on the PRE3 for class of service marking. Enhancements to the modular QoS CLI allow you to mark the IP DSCP bits of traffic on the L2TP access concentrator (LAC). The Class-Based Frame Relay DE Bit Marking and Tunnel Header Marking features were also introduced on the PRE3.	PRE3
Release 12.2(33)SB	This feature was enhanced to support Class-Based Frame Relay DE Bit Marking on the PRE4.	PRE3, PRE4

Benefits of QoS Packet Marking

Network Partitioning and Categorizing

Packet marking allows you to partition your network into multiple priority levels or classes of service.

Layer 2 to Layer 3 Mapping

If a packet that needs to be marked to differentiate user-defined QoS services is leaving the router and entering a switch, the router can set the class of service (CoS) value of the packet because the switch can process the Layer 2 CoS header marking.

Weighted Random Early Detection Configuration

Weighted random early detection (WRED) uses IP precedence values or IP DSCP values to determine the drop probability of a packet. Therefore, you can use the IP precedence and IP DSCP markings with the WRED feature.

Improved Bandwidth Management in ATM Networks

The ability to set the ATM CLP bit allows you to extend your IP QoS policies into an ATM network. As congestion occurs in the ATM network, cells with the CLP bit set are more likely to be dropped, resulting in improved network performance for higher priority traffic and applications.

IP Precedence Marking

You can mark the importance of a packet by using the IP precedence marking mechanism. IP precedence marking helps to do the following:

- Manage congestion—IP precedence field is used to determine how to schedule packets.
- Avoid congestion—IP precedence field is used to determine how to handle packets when packet-dropping mechanisms, such as weighted random early detection (WRED), are configured.
- Police traffic—Networking devices within the network can use IP precedence values to determine how to handle inbound traffic based on the transmission rate.

Layer 2 media often changes as packets traverse from source to destination. A more ubiquitous marking can occur at Layer 3, using the IP type of service (ToS) byte. The ToS byte is the second byte in an IPv4 packet. The first three bits of the ToS byte are the IP precedence bits, which enable you to set eight IP precedence markings (0 through 7).

Table 7-2 lists the 8 different IP precedence markings defined in RFC 791. Notice that IP precedence 6 and 7 are used for network control. Do not use IP precedence 6 or 7 to mark packets, unless you are marking control packets.

Table 7-2 IP Precedence Values

Precedence Value	Precedence Name	Binary Value	Recommended Use
0	Routine	000	Default marking value
1	Priority	001	Data applications
2	Immediate	010	
3	Flash	011	Call signaling
4	Flash Override	100	Video conferencing and streaming video
5	Critic	101	Voice
6	Internetwork Control	110	Network control traffic (such as routing, which is typically precedence 6)
7	Network Control	111	

You can configure a QoS policy to include IP precedence marking for packets entering the network. Devices within your network can then use the newly marked IP precedence values to determine how to treat the packets. For example, class-based weighted random early detection (WRED) uses IP precedence values to determine the probability that a packet is dropped. You can also mark voice packets with a particular precedence. You can then configure low-latency queuing (LLQ) to place all packets of that precedence into the priority queue.

IP Precedence-Based Weighted Random Early Detection

When you configure IP precedence-based weighted random early detection (WRED) on an output policy map and the outgoing packets are MPLS packets, the router drops the MPLS packets based on the three experimental (EXP) bits in the MPLS label, instead of using the 3-bit IP precedence field in the underlying IP packets.

set ip precedence Command

To set the precedence value in a packet header, use the **set ip precedence** command in policy-map class configuration mode. To remove the precedence value, use the **no** form of this command. By default, this command is disabled.

set ip precedence *prec-value*

no set ip precedence *prec-value*

Syntax Description

ip	Specifies that the match is for IPv4 packets only. You must specify this keyword.
precedence *prec-value*	Sets the precedence value. Valid values are from 0 to 7.

set ip precedence Command History

Cisco IOS Release	Description
Release 12.0(17)SL	The **set ip precedence** command was introduced on the PRE1.
Release 12.2(16)BX	This command was introduced on the PRE2.
Release 12.2(28)SB	This command was integrated in Cisco IOS Release 12.2(28)SB for the PRE2.
Release 12.2(31)SB2	This command was introduced on the PRE3.
Release 12.2(33)SB	This command was introduced on the PRE4.

Usage Guidelines for the set ip precedence Command

Bit Settings

After the precedence bits are set, other quality of service (QoS) features such as weighted fair queuing (WFQ) and weighted random early detection (WRED) can then operate on the bit settings.

Precedence Value

The network can give priority (or some type of expedited handling) to marked traffic through the application of weighted fair queuing (WFQ) or weighted random early detection (WRED) at points downstream in the network. Typically, you set the precedence value at the edge of the network (or administrative domain); data then is queued according to the specified precedence. WFQ can speed up handling for certain precedence traffic at congestion points. WRED can ensure that certain precedence traffic has lower loss rates than other traffic during times of congestion.

In Cisco IOS Release 12.3(7)XI, the router accepts the **set precedence** command without specifying the **ip** keyword. However, you must specify the **set ip precedence** command to set the precedence value in a packet header.

IP Differentiated Services Code Point Marking

IP precedence marking might seem too restrictive and limiting because only eight classes are available for marking. You might choose instead to use the IP differentiated services code point (DSCP) marking model, which offers up to 64 different values (0 through 63).

The differentiated services (DiffServ) functionality of the Cisco IOS software is fully compliant with the Internet Engineering Task Force (IETF) standards defined in the following request for comments (RFCs) documents:

- RFC-2474
- RFC-2475
- RFC-2597
- RFC-2598

The router leverages the IETF definition of the IPv4 1-byte type of service (ToS) field in the IP packet header by using the six most significant bits of this field (the DSCP bits) to classify traffic into any of the 64 possible classes. After the router classifies packets, you can use the modular QoS CLI to implement IETF-defined per-hop behaviors (PHBs), including assured forwarding (AF) and expedited forwarding (EF).

The router also uses bits in the ToS field to prioritize packets using an IP precedence value. Because the IP precedence value is actually part of the DSCP value, you cannot simultaneously set both the IP precedence and DSCP values. If you attempt to, an error message displays.

Figure 7-1 shows the DSCP bits in the ToS field.

Figure 7-1 DSCP Bits in the IP ToS Byte

DSCP Per-Hop Behavior

You can enter DSCP values as numeric values or as special keyword names called *per-hop behaviors* (PHBs). For example, DSCP EF is the same as DSCP 46 and DSCP AF31 is the same as DSCP 26.

The router supports the following classes of DSCP PHBs:

- Best effort (BE)—DSCP 0
- Assured forwarding (AF)—AF classes 1 through 4
- Expedited forwarding (EF)—DSCP 46
- Class selector code points—CS1 through CS7

Again, vendor-specific mechanisms need to be configured to implement these PHBs. For more information about EF PHB, see RFC-2598. To implement the PHBs, you must configure vendor-specific mechanisms. For more information, see the appropriate RFC as indicated in Table 7-4 on page 7-8.

Assured Forwarding

There are four assured forwarding (AF) classes, AF1x through AF4x. The first number corresponds to the AF class and the second number (x) refers to the level of drop preference within each AF class. There are three drop probabilities, ranging from 1 (low drop) through 3 (high drop). Depending on a network policy, packets can be selected for a PHB based on required throughput, delay, jitter, loss, or according to the priority of access to network services. AF allows for a committed information rate between multiple classes in a network according to desired policies.

Table 7-3 provides the DSCP coding and drop probability for AF classes 1 through 4. Bits 0, 1, and 2 define the class; bits 3 and 4 specify the drop probability; bit 5 is always 0.

Table 7-3 Assured Forwarding DSCP Code Points

Drop Probability	Class 1	Class 2	Class 3	Class4
Low Drop	001010	010010	011010	100010
	AF11	AF21	AF31	AF41
	DSCP 10	DSCP 18	DSCP 26	DSCP 34
Medium Drop	001100	010100	011100	100100
	AF12	AF 22	AF32	AF42
	DSCP 12	DSCP 20	DSCP 28	DSCP 36
High Drop	001110	010110	011110	100110
	AF13	AF23	AF33	AF43
	DSCP 14	DSCP 22	DSCP 30	DSCP 38

Expedited Forwarding

The expedited forwarding (EF) PHB is used to build a low-loss, low-latency, low-jitter, assured bandwidth, end-to-end service through differentiated services (DiffServ) domains. This PHB appears to the endpoints like a point-to-point connection or a virtual leased line. EF PHB, also referred to as a *premium service*, is suitable for applications such as Voice over IP (VoIP).

The recommended code point for the EF PHB is 101110.

Class Selector Code Points

The router also supports class selector (CS) code points, which is a way of marking the six DSCP bits so that the code points are identical to IP precedence values. These code points can be used with systems that only support the IP precedence. The CS code points have the form *xyz*000, where *x*, *y*, and *z* represent a 1 or 0.

For more information, see the appropriate RFC as indicated in Table 7-4 on page 7-8.

DSCP Values

The following differentiated services (DiffServ) RFCs define DSCP values:

- RFC-2474, *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*
- RFC-2475, *An Architecture for Differentiated Services*
- RFC-2597, *Assured Forwarding PHB Group*
- RFC-2598, *An Expedited Forwarding PHB*

The RFCs do not dictate the way to implement PHBs; this is the responsibility of the vendor. Cisco implements queuing techniques that can base their PHB on the IP precedence or DSCP value in the IP header of a packet. Based on DSCP or IP precedence, traffic can be put into a particular service class. Packets within a service class are treated the same way.

Table 7-4 lists only the DSCP values suggested by the DiffServ RFCs.

Table 7-4 DSCP Values

DSCP Value	DSCP Name	Binary Value	Defined in RFC
0	Best Effort or Default	000000	2475
8	CS1	001000	
16	CS2	010000	
24	CS3	011000	
32	CS4	100000	
40	CS5	101000	
48	CS6	110000	
56	CS7	111000	
10	AF11	001010	2597
12	AF12	001100	
14	AF13	001110	
18	AF21	010010	
20	AF22	010100	
22	AF23	010110	
26	AF31	011010	
28	AF32	011100	
30	AF33	011110	
34	AF41	100010	
36	AF42	100100	
38	AF43	100110	
46	EF	101110	2598

You can configure a QoS policy to include an IP DSCP marking for packets entering the network. Devices within your network can then use the newly marked IP DSCP values to determine how to treat the packets. For example, class-based weighted random early detection (WRED) uses IP DSCP values to determine the probability that a packet is dropped. You can also mark voice packets with a particular DSCP value. You can then configure low-latency queuing (LLQ) to place all packets of that DSCP value into the priority queue.

DSCP-Based Weighted Random Early Detection

When you configure DSCP-based weighted random early detection (WRED) on an output policy map and the outgoing packets are MPLS packets, the router drops the MPLS packets based on the three experimental (EXP) bits in the MPLS label, instead of using the 6-bit DSCP field in the underlying IP packets. The router shifts the three EXP bits to the left to make it six bits. For example, if the value of the EXP bits is 5 (binary 101), the router left-shifts the bits to make them binary 101000, thus making it look like a 6-bit DSCP field. The router drops packets based on the shifted binary value.

set ip dscp Command

To mark a packet by setting the differentiated services code point (DSCP) value in the type of service (ToS) byte, use the **set ip dscp** command in policy-map class configuration mode. To remove a previously set DSCP value, use the **no** form of this command. By default, no packets are marked.

set ip dscp {*dscp-value* | **af***xy* | **cs***x* | **ef** | **default**}

no set ip dscp {*dscp-value* | **af***xy* | **cs***x* | **ef** | **default**}

Syntax Description

ip	Specifies that the match is for IPv4 packets only. You must specify this keyword.
dscp *dscp-value*	Sets the DSCP value. Valid values are from 0 to 63. Instead of specifying a numeric *dscp-value*, you can specify one of the following reserved keywords: • **af***xy* indicates assured forwarding. • **cs***x* indicates class selector code points that are backward-compatible with IP precedence. These code points (CS1 through CS7) are identical to IP precedence values 1 through 7. • **ef** indicates expedited forwarding. • **default** indicates best effort or DSCP 0. For more information, see Table 7-4 on page 7-8.

set ip dscp Command History

Cisco IOS Release	Description
Release 12.0(17)SL	This command was introduced on the PRE1.
Release 12.2(16)BX	This command was introduced on the PRE2.
Release 12.2(28)SB	This command was integrated in Cisco IOS Release 12.2(28)SB for the PRE2.
Release 12.2(31)SB2	This command was introduced on the PRE3 to allow you to mark the IP DSCP bits of traffic on the L2TP access concentrator (LAC).
Release 12.2(33)SB	This command was introduced on the PRE4.

Usage Guidelines for the set ip dscp Command

- After the DSCP bit is set, other quality of service (QoS) features can then operate on the bit settings.
- You cannot use the **set ip dscp** command with the **set ip precedence** command to mark the same packet. DSCP and precedence values are mutually exclusive. A packet can have one value or the other, but not both.
- The network can give priority (or some type of expedited handling) to marked traffic. Typically, you set the precedence value at the edge of the network (or administrative domain); data is then queued according to the precedence. Weighted fair queuing (WFQ) can speed up handling for high-precedence traffic at congestion points. Weighted random early detection (WRED) can ensure that high-precedence traffic has lower loss rates than other traffic during times of congestion.
- In Cisco IOS Release 12.3(7)XI, the router accepts the **set dscp** command without specifying the **ip** keyword. However, you must specify the **set ip dscp** command to set the DSCP value in a packet header. The **ip** keyword is required.

Class of Service Marking

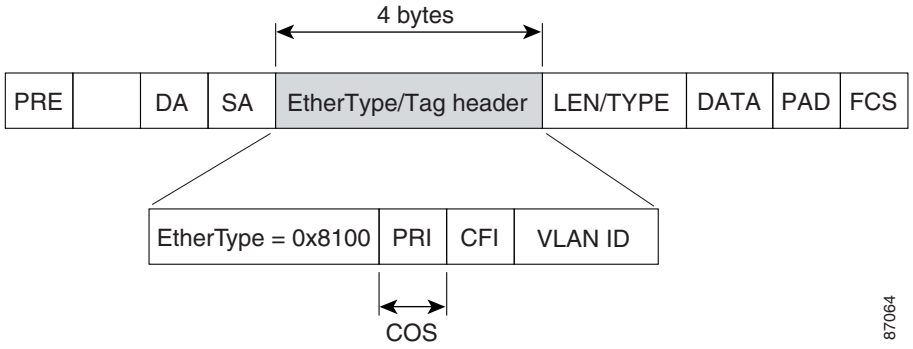
Class of service (CoS) marking enables the Cisco 10000 series router to interoperate with switches to deliver end-to-end QoS. The IEEE 802.1p standard enables the router to:

- Classify inbound Ethernet packets based on the value in the CoS field
- Set the value in the CoS field of outbound packets

For Layer 2 devices, you can assign priority-indexed IEEE 802.1p CoS values to Ethernet frames. Layer 2 IEEE 802.1Q frame headers have a 2-byte Tag Control Information field in the 802.1p portion of the header. The three most-significant bits of this field (the User Priority bits) make up the Layer 2 CoS field. This 3-bit field allows you to mark eight classes of service (0 through 7) on Layer 2 Ethernet frames. Other QoS tools can then use the CoS marking to classify traffic. For IEEE 802.1Q, the User Priority bits are set to zero (0) in the Ethernet header.

Figure 7-2 shows the PRI field containing the 3-bit User Priority field.

Figure 7-2 User Priority Bits in the IEEE 802.1p Header



For CoS-based QoS, the Cisco 10000 series router uses the IP precedence bits in the IP header to give preference to higher-priority traffic. Layer 3 IP headers have a 1-byte Type of Service (ToS) field. The router uses the six most significant bits of this field (the differentiated services code point (DSCP) bits) to prioritize traffic. Figure 5-3 shows the DSCP bits in the TOS field.

Figure 7-3 DSCP Bits in the IP ToS Byte

The router uses the CoS value to determine how to prioritize packets for transmission and can also use CoS marking to perform Layer 2 to Layer 3 mapping. Using the CoS field, you can differentiate user-defined QoS services for packets leaving a router and entering a switch. Switches already have the ability to match and set CoS values; therefore, a router can set the CoS value of a packet to enable Layer 2 to Layer 3 mapping. The switch can then process the Layer 2 CoS header marking.

To allow the Cisco 10000 series router to interoperate with Layer 2 devices, CoS-based QoS on the router allows the 802.1p User Priority bits to be mapped to the IP DSCP bits for packets received on inbound interfaces. The DSCP bits are mapped to the User Priority bits for packets forwarded from outbound interfaces.

In the inbound direction, you can configure the router to match on the CoS bits and then perform an action (such as setting the IP precedence or DSCP bits). By default, the router ignores the CoS field of inbound packets.

In the outbound direction, you can configure the router to set the CoS bits of outbound packets to a value that you specify. If you do not do this, by default, the router ignores the CoS field and leaves it set to a default value.

QinQ Class of Service Marking

For EXP-to-CoS mapping in QinQ configurations, the parallel express forwarding (PXF) engine marks both the inner and outer CoS bits.

For CoS-to-EXP mapping in QinQ configurations, the PXF engine looks at the CoS bits in the outer dot1q header to determine how to mark the EXP bits.

set cos Command

To set the Layer 2 class of service (CoS) value of an outgoing packet, use the **set cos** command in policy-map class configuration mode. To remove a specific CoS value setting, use the **no** form of this command. By default, this command is disabled.

set cos *cos-value*

no set cos *cos-value*

Syntax Description

cos-value	Is a specific IEEE 802.1Q CoS value from 0 to 7.

set cos Command History

Cisco IOS Release	Description
Release 12.0(16)BX	This command was introduced on the PRE2 only.
Release 12.2(28)SB	This command was integrated in Cisco IOS Release 12.2(28)SB for the PRE2.
Release 12.2(31)SB2	This command was integrated in Cisco IOS Release 12.2(31)SB2 for the PRE3.
Release 12.2(33)SB	This command was introduced on the PRE4.

Usage Guidelines for the set cos Command

The **set cos** command allows switches and routers to interoperate. By configuring the router to match packets based on the CoS value (using the **match cos** command) and to set CoS values, you can configure Layer 2 to Layer 3 mapping. If a packet that needs to be marked to differentiate user-defined QoS services is leaving a router and entering a switch, the router can set the CoS value of the packet because the switch can process the Layer 2 header.

Use the **set cos** command only in service policies that are attached in the output direction of an interface; packets entering an interface cannot be set with a CoS value. You can configure a CoS value on an Ethernet interface that is configured for 802.1Q or on a virtual access interface that is using an 802.1Q interface.

QoS Group Marking

You can use QoS group marking to assign packets to a QoS group. The QoS group field is an internal marking that exists only within the router. You can set this field as packets pass through the fabric of the router. The router uses the group ID marking to determine how to prioritize packets for transmission. QoS groups are used as part of QoS policy propagation through the Border Gateway Protocol (QPPB) and are useful in configurations that support MPLS QoS tunneling modes: short pipe, long pipe, and uniform pipe.

You can set up to 100 different QoS group markings.

set qos-group Command

To set a quality of service (QoS) group identifier (ID) that can be used later to classify packets, use the **set qos-group** command in policy-map class configuration mode. To remove the group ID, use the **no** form of this command. By default, this command is disabled; no group ID is specified.

set qos-group *group-id*

no set qos-group *group-id*

Syntax Description

group-id	Is the group identifier. Valid values are from 0 to 99.

set qos-group Command History

Cisco IOS Release	Description
Release 12.0(17)SL	This command was introduced on the PRE1.
Release 12.2(16)BX	This command was introduced on the PRE2.
Release 12.2(28)SB	This command was integrated in Cisco IOS Release 12.2(28)SB for the PRE2.

Usage Guidelines for the set qos-group Command

The **set qos-group** command allows you to associate a group ID with a packet. The group ID can be used later to classify packets into QoS groups as part of QoS policy propagation through the Border Gateway Protocol (QPPB). QoS groups are also useful in configurations supporting MPLS QoS tunneling modes: short pipe, long pipe, and uniform pipe.

A QoS group and discard class are required when the input per-hop behavior (PHB) marking is used for classifying packets on the output interface

ATM Cell Loss Priority Marking

You can change the cell loss priority (CLP) bit setting in an ATM header of a cell to control the discarding of cells in congested ATM environments. As congestion occurs in the ATM network, the ATM network switch can discard cells with the CLP bit set to 1 (discard) before discarding cells with a CLP bit setting of 0.

You can set ATM CLP marking only on outbound packets. The Cisco 10000 series router does not support CLP bit matching.

set atm-clp Command

To set the cell loss priority (CLP) bit to 1, use the **set atm-clp** command in policy-map class configuration mode. To change the CLP bit setting back to 0, use the **no** form of the command. By default, the CLP bit automatically sets to 0 when the router sends packets as ATM cells.

```
set atm-clp

no set atm-clp
```

set atm-clp Command History

Cisco IOS Release	Description
Release 12.0(17)SL	This command was introduced on the PRE1.
Release 12.2(28)SB	This command was integrated in Cisco IOS Release 12.2(28)SB for the PRE2.
Release 12.2(31)SB2	This command was introduced on the PRE3.
Release 12.2(33)SB	This command was introduced on the PRE4.

Usage Guidelines for the set atm-clp Command

You can attach a policy map containing the **set atm-clp** command only as an output policy. The **set atm-clp** command does not support packets that originate from the router.

To disable this command, remove the service policy from the interface by using the **no service-policy** command.

The router discards packets with the CLP bit set to 1 before it discards packets with the CLP bit set to 0.

MPLS Experimental Marking

The Multiprotocol Layer Switching (MPLS) experimental (EXP) field is a 3-bit field within the MPLS label that is used in QoS marking. By default, the IP precedence field in the underlying IP packet is copied to the MPLS EXP field during label imposition. Using the MPLS EXP field does not modify the DSCP or IP precedence markings in the packet IP header.

The MPLS EXP field allows up to eight different QoS markings that correspond to the eight possible IP precedence values. For more information, see Table 7-2 on page 7-4.

The value of the EXP bits determines the per-hop behavior (PHB) for MPLS nodes and is also used as transparency mechanisms when used with MPLS DiffServ tunneling modes such as pipe and uniform modes. IP marking does not modify an MPLS packet carrying IP data. You must configure MPLS marking on an input interface. MPLS marking takes effect only during label imposition. You can combine marking and policing to change the DSCP and MPLS EXP values of an IP packet during MPLS label imposition.

A provider edge (PE) router at the edge of the MPLS network can be configured to map the DSCP or IP precedence field to the MPLS EXP field. The router uses the value of the EXP field as the basis for IP QoS. As a result, MPLS routers can perform QoS features indirectly, based on the original IP precedence field inside the MPLS-encapsulated IP packet. The IP packet does not need to be opened to examine the IP precedence field. When a packet leaves the MPLS network, IP QoS is still based on the DSCP or IP precedence value in the IP header.

QinQ MPLS Experimental Marking

For CoS-to-EXP mapping in QinQ configurations, the parallel express forwarding (PXF) engine looks at the CoS bits in the outer dot1q header to determine how to mark the EXP bits.

For EXP-to-CoS mapping in QinQ configurations, the PXF marks both the inner and outer CoS bits.

set mpls experimental imposition Command

To set the value of the Multiprotocol Label Switching (MPLS) experimental (EXP) field on all imposed label entries, use the **set mpls experimental imposition** command in policy-map class configuration mode. To disable the setting, use the **no** form of the command. By default, no MPLS EXP value is set.

set mpls experimental imposition *mpls-exp-value*

no set mpls experimental imposition *mpls-exp-value*

Syntax Description

mpls-exp-value	Specifies the value used to set the MPLS EXP bits. Valid values are from 0 to 7.

set mpls experimental imposition Command History

Cisco IOS Release	Description
Release 12.0(22)S	The **set mpls experimental** command was introduced on the PRE1.
Release 12.3(7)XI1	The **set mpls experimental imposition** command was introduced on the PRE2.
Release 12.2(28)SB	This command was integrated in Cisco IOS Release 12.2(28)SB for the PRE2.

Note Cisco IOS software replaced the **set mpls experimental** command with the **set mpls experimental imposition** command. However, the Cisco 10000 series router continues to use the **set mpls experimental** command for PRE1. For PRE2, the command is **set mpls experimental imposition**.

Usage Guidelines for the set mpls experimental imposition Command

The **set mpls experimental imposition** command is supported only on input interfaces. Use this command during label imposition. This command sets the MPLS EXP field on all imposed label entries.

You can use the **set mpls experimental imposition** command on the input interface of a provider edge (PE) router connected to a customer edge (CE) router. In MPLS QoS differentiated services (DiffServ) tunneling modes, you can also use this command on the input interfaces of CE routers in pipe mode.

Note The Cisco 10000 series router does not support the **set mpls experimental topmost** command.

Discard-Class Marking

The discard-class is a 3-bit field that is used to set the per-hop behavior (PHB) for dropping traffic. The discard-class indicates the drop portion of the PHB. You can set the discard-class on the input interface to use as a matching criterion and to affect how packets are dropped on the output interface. You can use the discard-class with weighted random early detection (WRED) on the output interface to classify packets and determine packet drop probability. You can set up to eight discard-class values (0 through 7).

set discard-class Command

To mark a packet with a discard-class value or to drop a specific traffic type during congestion, use the **set discard-class** command in policy-map class configuration mode. To remove a discard-class value or to disable the discard-class value, use the **no** form of the command. By default, the discard-value is zero.

```
set discard-class value

no set discard-class value
```

Syntax Description

value	Is the priority of a type of traffic. Valid values are from 0 to 7. **Note** This command is available only on the PRE2.

set discard-class Command History

Cisco IOS Release	Description
Release 12.3(7)XI	This command was introduced on the PRE2 only.
Release 12.2(28)SB	This command was integrated in Cisco IOS Release 12.2(28)SB for the PRE2.

Usage Guidelines for the set discard-class Command

You can set the discard-class on the input interface to use as a matching criterion and to affect how packets are dropped on the output interface. You can use the discard-class with weighted random early detection (WRED) on the output interface to classify packets and determine packet drop probability.

The router supports the **set discard-class** command only on the PRE2.

Class-Based Frame Relay DE Bit Marking

The Class-Based Frame Relay DE Bit Marking feature provides the ability to prioritize frames in a Frame Relay network by setting the discard eligibility (DE) bit in the header of Frame Relay frames. As congestion occurs in the Frame Relay network, frames with the DE bit set are more likely to be dropped, resulting in improved network performance for higher priority traffic and applications.

This feature supports the classification of inbound Frame Relay traffic based on the DE bit setting and the marking of the DE bit of outbound Frame Relay traffic. During classification, the router matches the DE bit of inbound packets to previously configured traffic classes (created using a class map) and classifies each matching packet as belonging to a specific traffic class.

DE bit marking can occur either as a class-based shaping action or as a class-based policing action. The modular QoS command-line interface (MQC) commands used to mark the DE bit are the following:

- **set fr-de** command (class-based shaping)
- **set-frde-transmit** command (class-based policing)

The **set-frde-transmit** command is a policing action for conforming traffic and is used with the **police** command. When using the **conforming-action set-frde-transmit** command, the router sends the frames through the policer's token bucket mechanism for processing and sets the DE bit for all frames that conform to the committed rate.

The PRE3 and PRE4 support Frame Relay DE bit marking across packet fragments.

History for the Class-Based Frame Relay DE Bit Marking Feature

Cisco IOS Release	Description	Required PRE
Release 12.2(31)SB22	This feature was introduced on the PRE3.	PRE2, PRE3
Release 12.2(33)SB	This feature was introduced on the PRE4.	PRE2, PRE3, PRE4

Marking and Policing Traffic

When you simultaneously configure a class in a policy map to include both marking and policing commands (the **set** and **police** commands), the router processes the **set** command first and then processes the **police** command. As a result, the values set by the **police** command override the values of the **set** command. This occurs regardless of whether you attach a policy map to an inbound or outbound interface.

For example, if you use the **set** command to configure a value for the IP precedence field and you configure a value for the same field by using the **police** command, the IP precedence value you set for the **police** command overrides the IP precedence value you configured for the **set** command.

The **set** and **police** commands allow you to configure the following fields:

- IP precedence and IP DSCP
- QoS group
- MPLS experimental imposition
- Discard-class
- ATM cell loss priority

Tunnel Header Marking

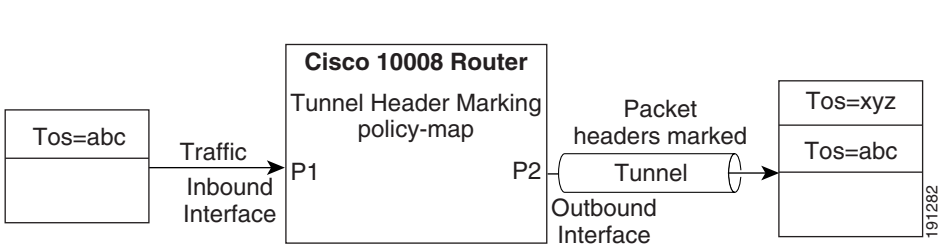
The Tunnel Header Marking (THM) feature allows you to mark the outer IP header's DSCP or precedence value during tunnel encapsulation of the packet.

The outer IP header type of service (ToS) field of a tunneled packet is typically exposed to a different QoS domain from that of the inner IP header. For example, for Multicast Virtual Private Network (MVPN) packets placed in Generic Routing Encapsulation (GRE) tunnels, the router processes the packet's outer ToS field based on the QoS services of a common core MPLS network. The router processes the packet's inner IP ToS field based on the QoS services of a particular VRF. Using tunnel header marking, different traffic streams that are aggregated into the same tunnel can mark their outer ToS field differently. This enables the streams to receive a different level of QoS processing at the outer ToS field's QoS domain.

A policy map is used to enable tunnel header marking and is applied to the inbound interface. If the outbound interface is a tunnel, the router marks the outer headers of packets as tunnel encapsulation occurs. If the outbound interface is not a tunnel, the policy map has no affect on the arriving packet headers.

As shown in Figure 7-4, the policy map named policy1 has tunnel header marking configured and is attached to inbound interface P1, and outbound interface P2 is a tunnel. As a result, the router classifies traffic as it enters the router through interface P1 and marks the traffic as it leaves through interface P2.

Figure 7-4 Tunnel Header Marking



Feature History for Tunnel Header Marking

Cisco IOS Release	Description	Required PRE
Release 12.2(31)SB2	This feature was introduced on the PRE2 to allow you to mark the outer IP header's DSCP or precedence value during tunnel encapsulation of the packet.	PRE2

Restrictions and Limitations for Marking

DSCP-Based and Precedence-Based Marking

- You cannot simultaneously configure both the **set ip dscp** command and the **set ip precedence** command in a policy map.
- Because IP precedence is actually part of the DSCP value, you cannot simultaneously set both the IP precedence and DSCP values for a traffic class. A packet can have one value or the other, but not both. If you do configure both values, the router marks the packet with the DSCP value.
- Because the router copies the IP precedence value to the MPLS EXP bits during label imposition, you cannot simultaneously set both IP precedence and MPLS experimental marking for a class.
- Marking has no preset scaling limit.
- In Cisco IOS Release 12.3(7)XI, the router accepts the **set precedence** and **set dscp** commands without specifying the **ip** keyword. However, you must specify the **set ip precedence** command to set the precedence value in a packet header and the **set ip dscp** command to set the DSCP value. The **ip** keyword is required.

Frame Relay DE Bit Marking Restrictions

- In Cisco IOS Release 12.3(7)XI, when you enter the **set ?** command, the context-sensitive help lists the **fr-de** keyword to allow you to set the Frame Relay discard eligibility (DE) bit. However, the router does not support setting the DE bit in Cisco IOS Release 12.3(7)XI and later releases.

Discard-Class-Based Marking Restrictions

- The router supports the **set discard-class** command only on the PRE2.
- When you use the input per-hop behavior (PHB) marking to classify packets on the output interface, you must configure the **set discard-class** command in the input policy.

CoS-Based Marking Restrictions

- The router supports CoS-based QoS only on Ethernet interfaces or PPPoE sessions associated with Ethernet interfaces.
- The router supports matching and marking for physical Ethernet interfaces and subinterfaces. The router supports CoS-based QoS for virtual access interfaces (VAIs) associated with PPPoE interfaces and it supports classification on the input policy and marking on the output policy.

Tunnel Header Marking Restrictions

- If the outbound interface is not a tunnel, a policy map with tunnel header marking has no effect on the packet headers.
- The router accepts only input service policies for tunnel header marking. You must apply a policy map with tunnel header marking to inbound interfaces. If you attempt to apply a service policy with tunnel header marking to an outbound interface, an error message displays.
- You may use the [**no**] **set ip** [**dscp** | **precedence**] **tunnel** *value* command in conjunction with other input set actions. However, if you specify tunnel header marking as a policer action, using the set-dscp-tunnel-transmit or set-prec-tunnel-transmit command, then you cannot specify any other policer action. The router only supports a single police action.
- The marking statistics for tunnel header marking are included in the statistical information for the class map.

Interfaces Supporting Marking

The following describes interface support for marking using the **set** commands:

Interfaces Supporting the set Command

- Physical
- Multilink PPP and multilink Frame Relay
- ATM unspecified bit rate (UBR) PVCs and point-to-point subinterfaces
- ATM variable bit rate (VBR) and constant bit rate (CBR) PVCs, and point-to-point subinterfaces
- Label-controlled ATM (LC-ATM) subinterfaces
- Frame Relay permanent virtual circuits (PVCs), point-to-point subinterfaces, and map classes
- Ethernet VLANs
- IP tunnel
- Virtual-access (See the "VAI QoS Inheritance" section on page 4-24.)

Note The router supports the **set** command on inbound and outbound interfaces.

Interfaces Not Supporting the set Command

- Fast Ethernet channel
- Frame Relay data link connection identifier (DLCI)

Classification and Marking Design Guidelines

The Cisco 10000 series router provides many tools for classifying and marking traffic. Your task is to determine how best to use these tools in your network environment. The following are guidelines to help you make good design choices for classification and marking tools:

- Classify and mark traffic as close to the ingress edge as possible.
- Consider the trust boundary in the network, making sure to mark or remark traffic after it reaches a trusted device in the network.
- Because the IP precedence and DSCP marking fields are part of the IP header and, therefore, are carried end-to-end, mark one of these fields to maximize the benefits of reducing classification overhead by the other QoS tools enabled in the network.
- If LAN switches connected to the router support only Layer 2 QoS (for example, the switch reacts to marked CoS bits, but not to marked IP precedence or DSCP bits), mark the CoS bits on the router before sending the frames onto the Ethernet.
- We suggest that you use the values indicated in Table 7-5 on page 7-21 for DSCP settings for voice and video payload, voice and video signaling, and data. Otherwise, follow the differentiated services (DiffServ) per-hop behavior (PHB) RFCs for DSCP settings as indicated in Table 7-4 on page 7-8.

Recommended Values for Traffic Marking

Table 7-5 lists the recommended values to use for traffic marking.

Table 7-5 Recommended Values for Traffic Marking

Traffic Type	IP Precedence	IP DSCP	Class of Service
Voice payload	5	EF	5
Video payload	4	AF41	4
Voice and video signaling	3	AF31	3
High priority data	2	AF21 AF22 AF23	2
Medium priority data	1	AF11 AF12 AF13	1
All other traffic	0	Default	0

Configuring Traffic Marking

To configure class-based traffic marking, perform any of the following optional tasks:

- Configuring IP Precedence Marking, page 7-22
- Configuring IP DSCP Marking, page 7-24
- Configuring Class of Service Marking, page 7-26
- Configuring QoS Group Marking, page 7-28
- Setting the ATM Cell Loss Priority Bit, page 7-29
- Configuring MPLS Experimental Marking, page 7-31
- Configuring Discard-Class Marking, page 7-33
- Configuring Tunnel Header Marking Using the set Command, page 7-35
- Configuring Tunnel Header Marking Using the police Command, page 7-36

For more information about classifying traffic and creating QoS service policies, see Chapter 2, "Classifying Traffic" and Chapter 3, "Configuring QoS Policy Actions and Rules."

Configuring IP Precedence Marking

To mark the IP precedence field of packets, enter the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# policy-map` *policy-map-name*	Specifies the name of the policy map and enters policy-map configuration mode. *policy-map-name* is the name of the policy map.
Step 2	`Router(config-pmap)# class` *class-map-name*	Assigns the traffic class you specify to the policy map. Enters policy-map class configuration mode. *class-map-name* is the name of a previously configured class map and is the traffic class for which you want to define QoS actions.
Step 3	`Router(config-pmap-c)# set ip precedence` *prec-value*	Specifies the IP precedence of packets within a traffic class. *prec-value* is the IP precedence value. Valid values are from 0 to 7. See Table 7-2 on page 7-4. **Note** Be sure you specify the **ip** keyword.

	Command	Purpose
Step 4	`Router(config-pmap-c)# exit`	Exits policy-map class configuration mode.
Step 5	`Router(config-pmap)# exit`	Exits policy-map configuration mode.
Step 6	`Router(config)# interface` *type number*	Specifies the interface to which you want to attach the service policy map. Enters interface configuration mode. *type* is the type of interface (for example, serial). *number* is the number of the interface (for example, 1/0/0).
Step 7	`Router(config-if)# service-policy {input | output}` *policy-map-name*	Attaches the policy map you specify to the interface. The router applies the service policy to packets on the interface in either the input or output direction. **input** indicates to apply the service policy to inbound packets. **output** indicates to apply the service policy to outbound packets. *policy-map-name* is the name of the policy map.

Configuration Examples for IP Precedence Marking and Classification

Example 7-1 shows how to configure IP precedence marking. In the example, a policy map named Bronze is created and the class map named Voice is associated with the Bronze policy. For all outbound packets on the Gigabit Ethernet 2/0/1 interface, the router sets the IP precedence bits to 5.

Example 7-1 Configuring IP Precedence Marking

```
Router(config)# class-map Voice
Router(config-cmap)# match access-group 110
Router(config-cmap)# exit
Router(config)# policy-map Bronze
Router(config-pmap)# class Voice
Router(config-pmap-c)# set ip precedence 5
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface GigabitEthernet 2/0/1
Router(config-if)# service-policy output Bronze
```

Example 7-2 shows how to configure IP precedence-based classification. In the example, a policy map named Second is created and the class map named ip-prec is associated with the Second policy. For all outbound packets on Gigabit Ethernet interface 2/0/1, the router classifies packets based on the setting of their IP precedence bits. If the bits are set to 3, the router assigns the packets to the ip-prec class and polices the traffic as indicated in the Second policy map.

Example 7-2 Configuring IP Precedence-Based Classification

```
Router(config)# class-map ip-prec
Router(config-cmap)# match ip precedence 3
Router(config-cmap)# exit
Router(config)# policy-map Second
Router(config-pmap)# class ip-prec
Router(config-pmap-c)# police 8000 4000 2000 conform-action transmit exceed-action drop
violate-action drop
Router(config-pmap-c)# exit
Router(config-pmap)# exit
```

```
Router(config)# interface GigabitEthernet 2/0/1
Router(config-if)# service-policy output Second
```

Configuring IP DSCP Marking

To mark the DSCP field of packets, enter the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# policy-map` *policy-map-name*	Specifies the name of the policy map and enters policy-map configuration mode. *policy-map-name* is the name of the policy map.
Step 2	`Router(config-pmap)# class` *class-map-name*	Assigns the traffic class you specify to the policy map. Enters policy-map class configuration mode. *class-map-name* is the name of a previously configured class map and is the traffic class for which you want to define QoS actions.
Step 3	`Router(config-pmap-c)# set ip dscp` {*dscp-value* | **af***xy* | **cs***x* | **ef** | **default**}	Sets the DSCP value in the ToS byte. **ip** specifies that the match is for IPv4 packets only. You must specify this keyword. **dscp** *dscp-value* sets the DSCP value. Valid values are from 0 to 63. Instead of specifying a numeric *dscp-value*, you can specify one of the following reserved keywords: • **af***xy* indicates assured forwarding points. The first number (*x*) indicates the AF class. Valid values are from 1 to 4. The second number (*y*) indicates the level of drop preference within each class. Valid values are from 1 (low drop) to 3 (high drop). • **cs** indicates class selector code points that are backward-compatible with IP precedence. Valid values for *x* are 1 through 7. The CS code points (CS1 through CS7) are identical to IP precedence values 1 through 7. • **ef** indicates expedited forwarding. • **default** indicates best effort or DSCP 0. For more information, see Table 7-4 on page 7-8.

	Command	Purpose
Step 4	`Router(config-pmap-c)# exit`	Exits policy-map class configuration mode.
Step 5	`Router(config-pmap)# exit`	Exits policy-map configuration mode.
Step 6	`Router(config)# interface` *type number*	Specifies the interface to which you want to attach the service policy map. Enters interface configuration mode. *type* is the type of interface (for example, serial). *number* is the number of the interface (for example, 1/0/0).
Step 7	`Router(config-if)# service-policy {input | output}` *policy-map-name*	Attaches the policy map you specify to the interface. The router applies the service policy to packets on the interface in either the input or output direction. **input** indicates to apply the service policy to inbound packets. **output** indicates to apply the service policy to outbound packets. *policy-map-name* is the name of the policy map.

Configuration Examples for IP DSCP Marking and Classification

Example 7-3 shows how to configure IP DSCP marking. In the example, the router assigns outbound traffic on the Gigabit Ethernet 1/0/0 interface to either class1 or class2. The router marks the packets by setting the DSCP bits of class1 packets to DSCP 5 and by setting the DSCP bits of class2 packets to DSCP 3 as indicated in the policy map named Silver.

Example 7-3 Configuring IP DSCP Marking

```
Router(config)# class-map class1
Router(config-cmap)# match qos-group 2
Router(config-cmap)# class class2
Router(config-cmap)# match access-group 108
Router(config-cmap)# exit
Router(config)# policy-map Silver
Router(config-pmap)# class class1
Router(config-pmap-c)# set ip dscp 5
Router(config-pmap-c)# class class2
Router(config-pmap-c)# set ip dscp 3
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface GigabitEthernet 1/0/0
Router(config-if)# service-policy output Silver
```

Example 7-4 shows how to configure IP DSCP-based classification. In the example, the router checks the DSCP bits of outbound packets on the GigabitEthernet interface 1/0/0. If the packet DSCP bits are set to 5, the router assigns the packet to the Voice class and gives the packet priority handling as indicated in the policy map named Platinum. All intermediate routers provide low-latency treatment to the Voice packets.

Example 7-4 Configuring IP DSCP-Based Classification

```
Router(config)# class-map Voice
Router(config-cmap)# match ip dscp 5
Router(config-cmap)# exit
Router(config)# policy-map Platinum
```

```
Router(config-pmap)# class Voice
Router(config-pmap-c)# priority
Router(config-pmap-c)# police 8000 600 400 conform-action transmit exceed-action drop
violate-action drop
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface GigabitEthernet 1/0/0
Router(config-if)# service-policy output Platinum
```

Configuring Class of Service Marking

To mark the Layer 2 class of service (CoS) field in the 802.1p header of outbound packets, enter the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# policy-map` *policy-map-name*	Specifies the name of the policy map and enters policy-map configuration mode. *policy-map-name* is the name of the policy map.
Step 2	`Router(config-pmap)# class` *class-map-name*	Assigns the traffic class you specify to the policy map. Enters policy-map class configuration mode. *class-map-name* is the name of a previously configured class map and is the traffic class for which you want to define QoS actions.
Step 3	`Router(config-pmap-c)# set cos` *cos-value*	Sets the Layer 2 class of service (CoS) value of an outbound packet. *cos-value* is a specific IEEE 802.1Q CoS value from 0 to 7.
Step 4	`Router(config-pmap-c)# exit`	Exits policy-map class configuration mode.
Step 5	`Router(config-pmap)# exit`	Exits policy-map configuration mode.
Step 6	`Router(config)# interface` *type number*	Specifies the interface to which you want to attach the service policy map. Enters interface configuration mode. *type* is the type of interface (for example, serial). *number* is the number of the interface (for example, 1/0/0).
Step 7	`Router(config-if)# service-policy output` *policy-map-name*	Attaches the policy map you specify to the interface. The router applies the service policy to packets on the interface in either the input or output direction. **output** indicates to apply the service policy to outbound packets. *policy-map-name* is the name of the policy map. **Note** You can attach a service policy containing the **set cos** command to only an outbound VLAN interface. The router cannot apply the **set cos** command to inbound packets.

Configuration Examples for CoS Marking and Classification

Example 7-5 shows how to configure CoS classification and marking on an interface, setting the Layer 2 CoS value in the 802.1p header. In the example, the router checks the DSCP bits of inbound packets on the Gigabit Ethernet interface 1/0/0. If the bits are set to DSCP AF11, the router assigns the packet to the class named Cos-Class and on the outbound interface marks the packet by setting the class of service bits to 5 as indicated in the policy map named Policy1.

Example 7-5 Configuring CoS Marking

```
Router(config)# class-map Cos-Class
Router(config-cmap)# match ip dscp AF11
Router(config-cmap)# exit
Router(config)# policy-map Policy1
Router(config-pmap)# class Cos-Class
Router(config-pmap-c)# set cos 5
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface GigabitEthernet 1/0/0
Router(config-if)# service-policy output Policy1
```

Example 7-6 shows how to configure CoS-based classification on outbound packets. In the example, the router checks the class of service bits of packets leaving on Gigabit Ethernet interface 4/0/0. If the bits are set to 3, the router assigns the packet to the class named Voice and marks the packet by setting the IP DSCP bits to 8 as indicated in the policy map named Policy1.

Note By default, the router maps the CoS field to the IP DSCP bits for packets received on inbound interfaces. The router maps IP precedence bits to the user priority bits for packets forwarded in the outbound direction. You can override this default behavior by creating a QoS policy that specifies the desired action.

Example 7-6 Configuring CoS-Based Classification

```
Router(config)# class-map Voice
Router(config-cmap)# match cos 3
Router(config-cmap)# exit
Router(config)# policy-map Policy1
Router(config-pmap)# class Voice
Router(config-pmap-c)# set ip dscp 8
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface GigabitEthernet 4/0/0
Router(config-if)# service-policy output Policy1
```

Configuring QoS Group Marking

To mark packets with a local QoS group ID, enter the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# policy-map policy-map-name`	Specifies the name of the policy map and enters policy-map configuration mode. *policy-map-name* is the name of the policy map.
Step 2	`Router(config-pmap)# class class-map-name`	Assigns the traffic class you specify to the policy map. Enters policy-map class configuration mode. *class-map-name* is the name of a previously configured class map and is the traffic class for which you want to define QoS actions.
Step 3	`Router(config-pmap-c)# set qos-group group-id`	Sets a QoS group identifier (ID) to use in classifying packets. *group-id* is the group identifier. Valid values are from 0 to 99.
Step 4	`Router(config-pmap-c)# exit`	Exits policy-map class configuration mode.
Step 5	`Router(config-pmap)# exit`	Exits policy-map configuration mode.
Step 6	`Router(config)# interface type number`	Specifies the interface to which you want to attach the service policy map. Enters interface configuration mode. *type* is the type of interface (for example, serial). *number* is the number of the interface (for example, 1/0/0).
Step 7	`Router(config-if)# service-policy {input | output} policy-map-name`	Attaches the policy map you specify to the interface. The router applies the service policy to packets on the interface in either the input or output direction. **input** indicates to apply the service policy to inbound packets. **output** indicates to apply the service policy to outbound packets. *policy-map-name* is the name of the policy map.

Configuration Examples for Configuring QoS Group Marking and Classification

Example 7-7 shows how to configure QoS group marking. In this example, the router classifies inbound packets on the Gigabit Ethernet interface 1/0/0 based on the class of service value. If the packet CoS value is 5, the router assigns the packet to the class named Group and sets the packet qos-group ID to 4 as indicated in the policy map named Policy1.

Example 7-7 Configuring QoS Group Marking

```
Router(config)# class-map Group
Router(config-cmap)# match cos 5
Router(config-cmap)# exit
Router(config)# policy-map Policy1
Router(config-pmap)# class Group
Router(config-pmap-c)# set qos-group 4
```

```
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface GigabitEthernet 1/0/0
Router(config-if)# service-policy input Policy1
```

Example 7-8 shows how to configure the router to classify packets based on the QoS group ID of the packet. In this example, the router checks outbound packets on Ethernet interface 1/0/0 for QoS group ID 5, assigns the matching packets to the traffic class named QoSGroup, defined in the policy map named Gold, and sets the packet DSCP bits to DSCP 0 (best effort).

Example 7-8 Configuring QoS Group-Based Classification

```
Router(config)# class-map QoSGroup
Router(config-cmap)# match qos-group 5
Router(config-cmap)# exit
Router(config)# policy-map Gold
Router(config-pmap)# class QoSGroup
Router(config-pmap-c)# set dscp 0
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface Ethernet 1/0/0
Router(config-if)# service-policy output Gold
```

Setting the ATM Cell Loss Priority Bit

To set the ATM cell loss priority (CLP) bit to 1, enter the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# policy-map` *policy-map-name*	Specifies the name of the policy map and enters policy-map configuration mode. *policy-map-name* is the name of the policy map.
Step 2	`Router(config-pmap)# class` *class-map-name*	Assigns the traffic class you specify to the policy map. Enters policy-map class configuration mode. *class-map-name* is the name of a previously configured class map and is the traffic class for which you want to define QoS actions.
Step 3	`Router(config-pmap-c)# set atm-clp`	Sets the cell loss priority bit to 1. The router discards packets with the CLP bit set to 1 before it discards packets with the CLP bit set to 0. **Note** To change the CLP bit back to 0, use the **no set atm-clp** command.

	Command	Purpose
Step 4	`Router(config-pmap-c)# exit`	Exits policy-map class configuration mode.
Step 5	`Router(config-pmap)# exit`	Exits policy-map configuration mode.
Step 6	`Router(config)# interface` *type number*	Specifies the interface to which you want to attach the service policy map. Enters interface configuration mode. *type* is the type of interface (for example, serial). *number* is the number of the interface (for example, 1/0/0).
Step 7	`Router(config-if)# service-policy {input | output}` *policy-map-name*	Attaches the policy map you specify to the interface. The router applies the service policy to packets on the interface in either the input or output direction. **input** indicates to apply the service policy to inbound packets. **output** indicates to apply the service policy to outbound packets. *policy-map-name* is the name of the policy map.

Configuration Example for Setting the ATM CLP Bit

Example 7-9 shows how to set the ATM CLP bit of packets. For all packets arriving on the ATM interface 1/0/1, the router assigns the packets that match access control list (ACL) 100 to the Class1 traffic class and sets the ATM CLP bit of each packet.

Example 7-9 Setting the ATM CLP Bit

```
Router(config)# class-map Class1
Router(config-cmap)# match access-group 100
Router(config-cmap)# exit
Router(config)# policy-map Premium
Router(config-pmap)# class Class1
Router(config-pmap-c)# set atm-clp
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface atm 1/0/1
Router(config-if)# service-policy output Premium
```

Configuring MPLS Experimental Marking

To copy the IP precedence or DSCP value to the MPLS experimental bits during label imposition, enter the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# policy-map policy-map-name`	Specifies the name of the policy map and enters policy-map configuration mode. *policy-map-name* is the name of the policy map.
Step 2	`Router(config-pmap)# class class-map-name`	Assigns the traffic class you specify to the policy map. Enters policy-map class configuration mode. *class-map-name* is the name of a previously configured class map and is the traffic class for which you want to define QoS actions.
Step 3	`Router(config-pmap-c)# set mpls experimental imposition mpls-exp-value`	Sets the value of the MPLS experimental (EXP) field on all imposed label entries. *mpls-exp-value* specifies the value used to set the MPLS EXP bits. Valid values are from 0 to 7.
Step 4	`Router(config-pmap-c)# exit`	Exits policy-map class configuration mode.
Step 5	`Router(config-pmap)# exit`	Exits policy-map configuration mode.
Step 6	`Router(config)# interface type number`	Specifies the interface to which you want to attach the service policy map. Enters interface configuration mode. *type* is the type of interface (for example, serial). *number* is the number of the interface (for example, 1/0/0).
Step 7	`Router(config-if)# service-policy {input | output} policy-map-name`	Attaches the policy map you specify to the interface. The router applies the service policy to packets on the interface in either the input or output direction. **input** indicates to apply the service policy to inbound packets. **output** indicates to apply the service policy to outbound packets. *policy-map-name* is the name of the policy map.

Configuration Examples for Configuring MPLS Experimental Marking and Classification

Example 7-10 shows how to configure MPLS Experimental (EXP) marking. In the example, for all packets on the inbound Gigabit Ethernet interface 1/0/0 that match class of service 3, the router sets the packet MPLS experimental bits to 5.

Example 7-10 Configuring MPLS EXP Marking

```
Router(config)# class-map voice
Router(config-cmap)# match cos 3
Router(config-cmap)# exit
Router(config)# policy-map Silver
Router(config-pmap)# class voice
Router(config-pmap-c)# set mpls experimental imposition 5
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface GigabitEthernet 1/0/0
Router(config-if)# mpls ip
Router(config-if)# service-policy input Silver
```

Example 7-11 shows how to configure MPLS EXP-based classification. In the example, the router checks the MPLS EXP bits of the packets arriving on the Gigabit Ethernet interface 1/0/0. The router assigns the packets whose bits have a setting of 5 to the mpls-exp class. As indicated in the policy map, the router provides low-latency priority handling of MPLS experimental traffic.

Example 7-11 Configuring MPLS EXP-Based Classification

```
Router(config)# class-map mpls-exp
Router(config-cmap)# match mpls experimental 5
Router(config-cmap)# exit
Router(config)# policy-map Platinum
Router(config-pmap)# class mpls-exp
Router(config-pmap-c)# priority
Router(config-pmap-c)# police percent 30 4000 2000 conform-action transmit exceed-action
drop
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface GigabitEthernet 1/0/0
Router(config-if)# mpls ip
Router(config-if)# service-policy output Platinum
```

Configuring Discard-Class Marking

To mark packets with a discard-class value, enter the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# policy-map policy-map-name`	Specifies the name of the policy map and enters policy-map configuration mode. *policy-map-name* is the name of the policy map.
Step 2	`Router(config-pmap)# class class-map-name`	Assigns the traffic class you specify to the policy map. Enters policy-map class configuration mode. *class-map-name* is the name of a previously configured class map and is the traffic class for which you want to define QoS actions.
Step 3	`Router(config-pmap-c)# set discard-class value`	Marks a packet with a discard eligibility value, setting the per-hop behavior (PHB) for dropping traffic. *value* is the priority of a type of traffic. Valid values are from 0 to 7. **Note** This command is only available on the PRE2.
Step 4	`Router(config-pmap-c)# exit`	Exits policy-map class configuration mode.
Step 5	`Router(config-pmap)# exit`	Exits policy-map configuration mode.
Step 6	`Router(config)# interface type number`	Specifies the interface to which you want to attach the service policy map. Enters interface configuration mode. *type* is the type of interface (for example, serial). *number* is the number of the interface (for example, 1/0/0).
Step 7	`Router(config-if)# service-policy {input | output} policy-map-name`	Attaches the policy map you specify to the interface. The router applies the service policy to packets on the interface in either the input or output direction. **input** indicates to apply the service policy to inbound packets. **output** indicates to apply the service policy to outbound packets. *policy-map-name* is the name of the policy map.

Configuration Examples for Configuring Discard-Class Marking and Classification

Example 7-12 shows how to configure the discard eligibility value for a traffic class. In the example, the router classifies inbound traffic on Ethernet interface 1/0/0 based on the class of service setting of the packets. If the CoS value matches 1, the router assigns the matching packets to the class named Class1 and sets the packet discard-class value to 4, as defined in the policy map named MyPolicy.

Example 7-12 Configuring Discard-Class Marking

```
Router(config)# class-map Class1
Router(config-cmap)# match cos 1
Router(config-cmap)# exit
Router(config)# policy-map MyPolicy
Router(config-pmap)# class Class1
Router(config-pmap-c)# set discard-class 4
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface Ethernet 1/0/0
Router(config-if)# service-policy input MyPolicy
```

Example 7-13 shows how to configure discard-class-based classification. In the example, the router classifies outbound traffic on Gigabit Ethernet interface 2/0/1 based on the discard-class setting of the packets. If the discard-class value matches 3, the router assigns the matching packets to the class named Group1 and provides a minimum bandwidth guarantee of 8000 kbps to Group1 traffic, as defined in the policy map named Manhattan.

Example 7-13 Configuring Discard-Class-Based Classification

```
Router(config)# class-map Group1
Router(config-cmap)# match discard-class 3
Router(config-cmap)# exit
Router(config)# policy-map Manhattan
Router(config-pmap)# class Group1
Router(config-pmap-c)# police 8000 600 400 conform-action transmit exceed-action drop
Router(config-pmap-c)# exit
Router (config-pmap)# exit
Router(config)# interface GigabitEthernet 2/0/1
Router(config-if)# service-policy output Manhattan
```

Configuring Tunnel Header Marking Using the set Command

To configure tunnel header marking using the **set** command, enter the following configuration commands beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# policy-map policy-map-name`	Specifies the name of the policy map and enters policy-map configuration mode. *policy-map-name* is the name of the policy map.
Step 2	`Router(config-pmap)# class class-map-name`	Assigns the traffic class you specify to the policy map. Enters policy-map class configuration mode. *class-map-name* is the name of a previously configured class map and is the traffic class for which you want to define QoS actions.
Step 3	`Router(config-pmap-c)# set ip [dscp | precedence] tunnel value`	Marks a packet by setting the differentiated services code point (DSCP) value or precedence level in the type of service (ToS) byte. (DSCP) **tunnel** *value* is a number from 0 to 63 or one of the following reserved keywords: • EF (expedited forwarding) • AF11 (assured forwarding class AF11) • AF12 (assured forwarding class AF12) (Precedence) **tunnel** *value* is a number from 0 to 7 that sets the precedence bit in the packet header.

Configuration Example for Tunnel Header Marking Using the set Command

The following example configuration shows how to configure tunnel header marking using the **set** command. In the example, marking is configured for the match_ip traffic class. For all packets belonging to that class, the router sets the DSCP bits to 3.

```
class-map match_ip
    match protocol ip

policy-map Tunnel_Marking
    class match_ip
    set ip dscp tunnel 3

class class-default
    shape 64000
```

Configuring Tunnel Header Marking Using the police Command

To configure tunnel header marking using the **police** command, enter the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# policy-map` *policy-map-name*	Specifies the name of the policy map and enters policy-map configuration mode. *policy-map-name* is the name of the policy map.
Step 2	`Router(config-pmap)# class` *class-map-name*	Assigns the traffic class you specify to the policy map. Enters policy-map class configuration mode. *class-map-name* is the name of a previously configured class map and is the traffic class for which you want to define QoS actions.
Step 3	`Router(config-pmap-c)# police [cir]` *bps* `[bc]` *burst-normal* `[pir]` *pir* `[be]` *burst-excess* `[conform-action {set-dscp-tunnel-transmit` *value* `| set-prec-tunnel-transmit` *value*`}] [exceed-action {set-dscp-tunnel-transmit` *value* `| set-prec-tunnel-transmit` *value*`}] [violate-action {set-dscp-tunnel-transmit` *value* `| set-prec-tunnel-transmit` *value*`}]`	Configures policing and uses the policer action to mark a packet's outer tunnel header. **set-dscp-tunnel-transmit** *value* is a number from 0 to 63 or one of the following reserved keywords: • EF (expedited forwarding) • AF11 (assured forwarding class AF11) • AF12 (assured forwarding class AF12) **set-prec-tunnel-transmit** *value* is a number from 0 to 7 that sets the precedence bit in the packet header. For more information, see the "police Command (Single-Rate)" section on page 6-6 or the "police Command (Two-Rate)" section on page 6-9.

Example Configuration for Tunnel Header Marking Using the police Command

The following example configuration shows how to mark the tunnel header of a packet using the **police** command. In the example, the policer sets the DSCP bits to 4 for all conforming traffic belonging to the match_ip class.

```
class-map match_ip
    match protocol ip

policy-map Tunnel_Marking
    class match_ip
    police 8000 conform-action set-dscp-tunnel-transmit 4

class class-default
    shape 64000
```

Verifying Traffic Marking

The Cisco 10000 series router collects statistical information about the number of packets and bytes marked.

To verify traffic marking, enter any of the following commands in privileged EXEC configuration mode:

Command	Purpose
`Router# show policy-map`	Displays configuration information for all configured policy maps.
`Router# show policy-map` *policy-map-name*	Displays configuration information for the policy map you specify.
`Router# show policy-map interface`	Displays configuration and statistical information for all of the input and output policies that are attached to an interface. For example, statistical information such as the incoming traffic rate, dropped packet rate, and the number of matched packets and bytes.
`Router# show policy-map interface` *interface*	Displays configuration and statistical information for the input and output policies attached to the interface you specify. *interface* is the name of the interface or subinterface whose policy configuration you want to display.
`Router# show policy-map interface` *interface* [**input** | **output**]	Displays the configuration of all classes configured for all inbound or outbound policy maps attached to the specified interface. *interface* is the name of the interface or subinterface whose policy configuration you want to display. **input** indicates to display the statistics for the attached inbound policy. **output** indicates to display the statistics for the attached outbound policy. **Note** If you do not specify **input** or **output**, the router displays information about all classes that are configured for all inbound and outbound policies attached to the interface you specified.
`Router# show policy-map` *policy-map-name* **class** *class-name*	Displays the configuration of the class you specify for the policy map you specify. *policy-map-name* is the name of the policy map that contains the class configuration you want to display. *class-name* is the name of the class whose configuration you want to display.

Verification Examples for Traffic Marking

Example 7-14 shows how to verify marking for the traffic classes in a policy map. In this example, traffic assigned to the Gold class has the precedence bits set to 5.

Example 7-14 Verifying Marking in a Policy Map

```
Router# show policy-map Child
  Policy Map Child
    Class Bronze
      police percent 30 6 ms 4 ms conform-action transmit exceed-action set-prep
    Class Gold
      police 8000 2000 4000 conform-action transmit exceed-action set-qos-transp
      set ip precedence 5
```

Example 7-15 shows how to verify marking on a specific interface. In this example, the QoS policy is a hierarchical policy that is attached to PVC 5/101 on the ATM 3/0/0.3 subinterface. In the Child policy, the Bronze class indicates to set the DSCP bits of Bronze packets to 3. The Gold class indicates to set the IP precedence bits of Gold packets to 5.

Example 7-15 Verifying Marking in a Hierarchical Policy

```
Router# show policy-map interface atm 3/0/0.3
 ATM3/0/0.3: VC 5/101 -

  Service-policy output: Parent

    Class-map: class-default (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
      Output queue: 0/64; 0/0 packets/bytes output, 0/0 drops
      Shape : 2000 kbps

      Service-policy : Child

        Class-map: Bronze (match-all)
          0 packets, 0 bytes
          5 minute offered rate 0 bps, drop rate 0 bps
          Match: ip precedence 3  5
          Police:
            600000 bps, 1536 limit, 1000 extended limit
            conformed 0 packets, 0 bytes; action: transmit
            exceeded 0 packets, 0 bytes; action: set-prec-transmit 2
            violated 0 packets, 0 bytes; action: drop
          QoS Set
            dscp 3
              Packets marked 0

        Class-map: Gold (match-all)
          0 packets, 0 bytes
          5 minute offered rate 0 bps, drop rate 0 bps
          Match: ip precedence 2
          Police:
            8000 bps, 2000 limit, 4000 extended limit
            conformed 0 packets, 0 bytes; action: transmit
            exceeded 0 packets, 0 bytes; action: set-qos-transmit 4
            violated 0 packets, 0 bytes; action: drop
          QoS Set
            precedence 5
```

```
        Packets marked 0

  Class-map: class-default (match-any)
    0 packets, 0 bytes
    5 minute offered rate 0 bps, drop rate 0 bps
    Match: any
Output queue: 0/64; 0/0 packets/bytes output, 0/0 drops
```

Related Documentation

This section provides hyperlinks to additional Cisco documentation for the features discussed in this chapter. To display the documentation, click the document title or a section of the document highlighted in blue. When appropriate, paths to applicable sections are listed below the documentation title.

Feature	Related Documentation
3-Color Marker for Traffic Policing (single rate)	*Release Notes for the Cisco 10000 Series ESR for Cisco IOS Release 12.0(23)SX* New Features in Cisco IOS Release 12.0(23)SX > Single Rate 3-Color Marker for Traffic Policing
ATM Cell Loss Priority Marking	*When Does a Router Set the CLP Bit in an ATM Cell?* *Cisco IOS Quality of Service Solutions Configuration Guide, Release 12.2* Part 1: Classification > Configuring Class-Based Packet Marking
Classification and Marking	*Cisco IOS Quality of Service Solutions Configuration Guide, Release 12.2* Part 1: Classification > Configuring Class-Based Packet Marking *Class-Based Marking, Release 12.0(26)S* feature module *Configuring Packet Marking on Frame Relay PVCs* *QoS Packet Marking, Implementing Quality of Service*
Class of Service Marking	*Service Provider Quality of Service Design Guide* *Cisco IOS Quality of Service Solutions Configuration Guide, Release 12.2* Part 1: Classification > Configuring Class-Based Packet Marking
DSCP Marking	*Service Provider Quality of Service Design Guide* *Cisco IOS Quality of Service Solutions Configuration Guide, Release 12.2* Part 1: Classification > Configuring Class-Based Packet Marking *QoS Packet Marking, Implementing Quality of Service Policies with DSCP*

Feature	Related Documentation
IP Precedence Marking	*Service Provider Quality of Service Design Guide* *Cisco IOS Quality of Service Solutions Configuration Guide, Release 12.2* Part 1: Classification > Configuring Class-Based Packet Marking
MPLS Experimental Marking	*Cisco IP Solution Center, 3.0: Quality of Service Management User Guide, Release 3.0* Quality of Service Concepts > MPLS Experimental Values *Service Provider Quality of Service Design Guide*
QoS Group Marking	*Cisco IOS Quality of Service Solutions Configuration Guide, Release 12.2* Part 1: Classification > Configuring Class-Based Packet Marking
QoS Policy Propagation through the Border Gateway Protocol (QPPB)	*Cisco IOS Quality of Service Solutions Configuration Guide, Release 12.2* Part 1: Classification > Classification Overview > QoS Policy Propagation via Border Gateway Protocol Part 1: Classification > Configuring QoS Policy Propagation via Border Gateway Protocol