

Configuring MPLS QoS

This chapter describes how to configure Multiprotocol Label Switching (MPLS) quality of service (QoS) in Cisco IOS Software Release 12.2SX.

**Note**

- For complete syntax and usage information for the commands used in this chapter, see the Cisco IOS Software Releases 12.2SX Command References at this URL:
http://www.cisco.com/en/US/docs/ios/mcl/122sx_mcl.html
- MPLS QoS extends to MPLS traffic the PFC QoS features described in [Chapter 36, “Configuring PFC QoS.”](#)
- This chapter provides supplemental information on MPLS QoS features. Be sure that you understand the PFC QoS features before you read this chapter.
- All policing and marking available for MPLS QoS are managed from the modular QoS command-line interface (CLI). The modular QoS CLI (MQC) is a command-line interface that allows you to define traffic classes, create and configure traffic policies (policy maps), and then attach those traffic policies to interfaces. A detailed description of the modular QoS CLI can be found in the *Cisco IOS Quality of Service Solutions Configuration Guide, Release 12.2* at this URL:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fqos_c/qcfbook.pdf

This chapter contains these sections:

- [Terminology, page 38-2](#)
- [MPLS QoS Features, page 38-3](#)
- [MPLS QoS Overview, page 38-4](#)
- [MPLS QoS, page 38-5](#)
- [Understanding MPLS QoS, page 38-7](#)
- [MPLS QoS Default Configuration, page 38-15](#)
- [MPLS QoS Commands, page 38-16](#)
- [MPLS QoS Restrictions and Guidelines, page 38-17](#)
- [Configuring MPLS QoS, page 38-17](#)
- [MPLS DiffServ Tunneling Modes, page 38-31](#)
- [Configuring Short Pipe Mode, page 38-34](#)
- [Configuring Uniform Mode, page 38-39](#)

Terminology

This section defines some MPLS QoS terminology:

- *Class of Service* (CoS) refers to three bits in either an Inter-Switch Link (ISL) header or an 802.1Q header that are used to indicate the priority of the Ethernet frame as it passes through a switched network. The CoS bits in the 802.1Q header are commonly referred to as the 802.1p bits. To maintain QoS when a packet traverses both Layer 2 and Layer 3 domains, the type of service (ToS) and CoS values can be mapped to each other.
- *Classification* is the process used for selecting traffic to be marked for QoS.
- *Differentiated Services Code Point* (DSCP) is the first six bits of the ToS byte in the IP header. DSCP is only present in an IP packet.
- *E-LSP* is a label switched path (LSP) on which nodes infer the QoS treatment for MPLS packets exclusively from the experimental (EXP) bits in the MPLS header. Because the QoS treatment is inferred from the EXP (both class and drop precedence), several classes of traffic can be multiplexed onto a single LSP (use the same label). A single LSP can support up to eight classes of traffic because the EXP field is a 3-bit field. The maximum number of classes would be less after reserving some values for control plane traffic or if some of the classes have a drop precedence associated with them.
- *EXP bits* define the QoS treatment (per-hop behavior) that a node should give to a packet. It is the equivalent of the DiffServ Code Point (DSCP) in the IP network. A DSCP defines a class and drop precedence. The EXP bits are generally used to carry all the information encoded in the IP DSCP. In some cases, however, the EXP bits are used exclusively to encode the dropping precedence.
- *Frames* carry traffic at Layer 2. Layer 2 frames carry Layer 3 packets.
- *IP precedence* is the three most significant bits of the ToS byte in the IP header.
- *QoS tags* are prioritization values carried in Layer 3 packets and Layer 2 frames. A Layer 2 CoS label can have a value ranging between zero for low priority and seven for high priority. A Layer 3 IP precedence label can have a value ranging between zero for low priority and seven for high priority. IP precedence values are defined by the three most significant bits of the 1-byte ToS byte. A Layer 3 DSCP label can have a value between 0 and 63. DSCP values are defined by the six most significant bits of the 1-byte IP ToS field.
- *LERs* (label edge routers) are devices that impose and dispose of labels upon packets; also referred to as Provider Edge (PE) routers.
- *LSRs* (label switching routers) are devices that forward traffic based upon labels present in a packet; also referred to as Provider (P) routers.
- *Marking* is the process of setting a Layer 3 DSCP value in a packet. Marking is also the process of choosing different values for the MPLS EXP field to mark packets so that they have the priority that they require during periods of congestion.
- *Packets* carry traffic at Layer 3.
- *Policing* is limiting bandwidth used by a flow of traffic. Policing can mark or drop traffic.

MPLS QoS Features

QoS enables a network to provide improved service to selected network traffic. This section explains the following MPLS QoS features, which are supported in an MPLS network:

- [MPLS Experimental Field, page 38-3](#)
- [Trust, page 38-3](#)
- [Classification, page 38-3](#)
- [Policing and Marking, page 38-4](#)
- [Preserving IP ToS, page 38-4](#)
- [EXP Mutation, page 38-4](#)
- [MPLS DiffServ Tunneling Modes, page 38-4](#)

MPLS Experimental Field

Setting the MPLS experimental (EXP) field value satisfies the requirement of service providers who do not want the value of the IP precedence field modified within IP packets transported through their networks.

By choosing different values for the MPLS EXP field, you can mark packets so that packets have the priority that they require during periods of congestion.

By default, the IP precedence value is copied into the MPLS EXP field during imposition. You can mark the MPLS EXP bits with an MPLS QoS policy.

Trust

For received Layer 3 MPLS packets, the PFC usually trusts the EXP value in the received topmost label. None of the following have any effect on MPLS packets:

- Interface trust state
- Port CoS value
- Policy-map **trust** command

For received Layer 2 MPLS packets, the PFC can either trust the EXP value in the received topmost label or apply port trust or policy trust to the MPLS packets for CoS and egress queueing purposes.

Classification

Classification is the process that selects the traffic to be marked. Classification accomplishes this by partitioning traffic into multiple priority levels, or classes of service. Traffic classification is the primary component of class-based QoS provisioning. The PFC makes classification decisions based on the EXP bits in the received topmost label of received MPLS packets (after a policy is installed). See the [“Configuring a Class Map to Classify MPLS Packets”](#) section on page 38-20 for information.

Policing and Marking

Policing causes traffic that exceeds the configured rate to be discarded or marked down to a higher drop precedence. Marking is a way to identify packet flows to differentiate them. Packet marking allows you to partition your network into multiple priority levels or classes of service.

The MPLS QoS policing and marking features that you can implement depend on the received traffic type and the forwarding operation applied to the traffic. See [“Configuring a Policy Map” section on page 38-23](#) for information.

Preserving IP ToS

The PFC automatically preserves the IP ToS during all MPLS operations including imposition, swapping, and disposition. You do not need to enter a command to save the IP ToS.

EXP Mutation

You can configure up to eight egress EXP mutation maps to mutate the internal EXP value before it is written as the egress EXP value. You can attach egress EXP mutation maps to these interface types:

- LAN port subinterfaces
- Layer 3 VLAN interfaces
- Layer 3 LAN ports

You cannot attach EXP mutation maps to these interface types:

- Layer 2 LAN ports (ports configured with the **switchport** command)
- FlexWAN ports or subinterfaces

For configuration information, see the [“Configuring MPLS QoS Egress EXP Mutation” section on page 38-29](#).

MPLS DiffServ Tunneling Modes

The PFC uses MPLS DiffServ tunneling modes. Tunneling provides QoS transparency from one edge of a network to the other edge of the network. See the [“MPLS DiffServ Tunneling Modes” section on page 38-31](#) for information.

MPLS QoS Overview

MPLS QoS enables network administrators to provide differentiated types of service across an MPLS network. Differentiated service satisfies a range of requirements by supplying for each transmitted packet the service specified for that packet by its QoS. Service can be specified in different ways, for example, using the IP precedence bit settings in IP packets.

Specifying the QoS in the IP Precedence Field

When you send IP packets from one site to another, the IP precedence field (the first three bits of the DSCP field in the header of an IP packet) specifies the QoS. Based on the IP precedence marking, the packet is given the treatment configured for that quality of service. If the service provider network is an MPLS network, then the IP precedence bits are copied into the MPLS EXP field at the edge of the network. However, the service provider might want to set QoS for an MPLS packet to a different value determined by the service offering.

In that case, the service provider can set the MPLS EXP field. The IP header remains available for the customer's use; the QoS of an IP packet is not changed as the packet travels through the MPLS network.

For more information, see the [“MPLS DiffServ Tunneling Modes”](#) section on page 38-31.

MPLS QoS

This section describes how MPLS QoS works.

[Figure 38-1](#) shows an MPLS network of a service provider that connects two sites of a customer network.

Figure 38-1 *MPLS Network Connecting Two Sites of a Customer's IP Network*



The network is bidirectional, but for the purpose of this document the packets move left to right.

In [Figure 38-1](#), the symbols have the following meanings:

- CE1—Customer equipment 1
- PE1—Service provider ingress label edge router (LER)
- P1—Label switch router (LSR) within the core of the network of the service provider
- P2—LSR within the core of the network of the service provider
- PE2—service provider egress LER
- CE2—Customer equipment 2

**Note**

PE1 and PE2 are at the boundaries between the MPLS network and the IP network.

These sections describe LER and LSR operation in an MPLS network.

- [LERs at the Input Edge of an MPLS Network, page 38-6](#)
- [LSRs in the Core of an MPLS Network, page 38-6](#)
- [LERs at the Output Edge of an MPLS Network, page 38-7](#)

**Note**

The QoS capabilities at the input interface differ depending on whether the input interface is a LAN port or a port adapter on a FlexWAN or Enhanced FlexWAN module. This section is for LAN ports. For information on a FlexWAN or Enhanced FlexWAN module, see the *FlexWAN and Enhanced FlexWAN Installation and Configuration Note*.

LERs at the Input Edge of an MPLS Network

**Note**

Incoming labels are aggregate or nonaggregate. The aggregate label indicates that the arriving MPLS or MPLS VPN packet must be switched through an IP lookup to find the next hop and the outgoing interface. The nonaggregate label indicates that the packet contains the IP next hop information.

This section describes how edge LERs can operate at either the ingress or the egress side of an MPLS network.

At the ingress side of an MPLS network, LERs process packets as follows:

1. Layer 2 or Layer 3 traffic enters the edge of the MPLS network at the edge LER (PE1).
2. The PFC receives the traffic from the input interface and uses the 802.1p bits or the IP ToS bits to determine the EXP bits and to perform any classification, marking, and policing. For classification of incoming IP packets, the input service policy can also use access control lists (ACLs).
3. For each incoming packet, the PFC performs a lookup on the IP address to determine the next-hop router.
4. The appropriate label is pushed (imposition) into the packet, and the EXP value resulting from the QoS decision is copied into the MPLS EXP field in the label header.
5. The PFC forwards the labeled packets to the appropriate output interface for processing.
6. The PFC also forwards the 802.1p bits or the IP ToS bits to the output interface.
7. At the output interface, the labeled packets are differentiated by class for marking or policing. For LAN interfaces, egress classification is still based on IP, not on MPLS.
8. The labeled packets (marked by EXP) are sent to the core MPLS network.

LSRs in the Core of an MPLS Network

This section describes how LSRs used at the core of an MPLS network process packets:

1. Incoming MPLS-labeled packets (and 802.1p bits or IP ToS bits) from an edge LER (or other core device) arrive at the core LSR.
2. The PFC receives the traffic from the input interface and uses the EXP bits to perform classification, marking, and policing.
3. The PFC3 performs a table lookup to determine the next-hop LSR.

4. An appropriate label is placed (swapped) into the packet and the MPLS EXP bits are copied into the label header.
5. The PFC forwards the labeled packets to the appropriate output interface for processing.
6. The PFC also forwards the 802.1p bits or the IP ToS bits to the output interface.
7. The outbound packet is differentiated by the MPLS EXP field for marking or policing.
8. The labeled packets (marked with EXP) are sent to another LSR in the core MPLS network or to an LER at the output edge.

**Note**

Within the service provider network, there is no IP precedence field for the queuing algorithm to use because the packets are MPLS packets. The packets remain MPLS packets until they arrive at PE2, the provider edge router.

LERs at the Output Edge of an MPLS Network

At the egress side of an MPLS network, LERs process packets as follows:

1. MPLS-labeled packets (and 802.1p bits or IP ToS bits) from a core LSR arrive at the egress LER (PE2) from the MPLS network backbone.
2. The PFC pops the MPLS labels (disposition) from the packets. Aggregate labels are classified using the original 802.1p bits or the IP ToS bits. Nonaggregate labels are classified with the EXP value by default.
3. For aggregate labels, the PFC performs a lookup on the IP address to determine the packet's destination; the PFC then forwards the packet to the appropriate output interface for processing. For non-aggregate labels, forwarding is based on the label. By default, non-aggregate labels are popped at the penultimate-hop router (next to last), not the egress PE router.
4. The PFC also forwards the 802.1p bits or the IP ToS bits to the output interface.
5. The packets are differentiated according to the 802.1p bits or the IP ToS bits and treated accordingly.

**Note**

The MPLS EXP bits allow you to specify the QoS for an MPLS packet. The IP precedence and DSCP bits allow you to specify the QoS for an IP packet.

Understanding MPLS QoS

MPLS QoS supports IP QoS. For MPLS packets, the EXP value is mapped into an internal DSCP so that the PFC can apply non-MPLS QoS marking and policing.

For both the ingress and egress policies, MPLS QoS marking and policing decisions are made on a per-interface basis at an ingress PFC. The ingress interfaces are physical ports, subinterfaces, or VLANs.

The QoS policy ACLs are programmed in QoS TCAM separately for ingress and egress lookup. The ternary content addressable memory (TCAM) egress lookup takes place after the IP forwarding table (FIB) and NetFlow lookups are completed.

The results of each QoS TCAM lookup yield an index into RAM that contains policer configuration and policing counters. Additional RAM contains the microflow policer configuration; the microflow policing counters are maintained in the respective NetFlow entries that match the QoS ACL.

The results of ingress and egress aggregate and microflow policing are combined into a final policing decision. The out-of-profile packets can be either dropped or marked down in the DSCP.

This section describes MPLS QoS for the following:

- [LERs at the EoMPLS Edge, page 38-8](#)
- [LERs at the IP Edge \(MPLS, MPLS VPN\), page 38-9](#)
- [LSRs at the MPLS Core, page 38-13](#)

**Note**

The following sections see QoS features for LAN ports and FlexWAN ports. For details about how the different features work, see the appropriate documentation.

LERs at the EoMPLS Edge

This section summarizes the Ethernet over MPLS (EoMPLS) QoS features that function on the LERs. EoMPLS QoS support is similar to IP-to-MPLS QoS:

- For EoMPLS, if the port is untrusted, the CoS trust state is automatically configured for VC type 4 (VLAN mode), not for VC type 5 (port mode). 802.1q CoS preservation across the tunnel is similar.
- Packets received on tunnel ingress are treated as untrusted for EoMPLS interfaces, except for VC Type 4 where trust CoS is automatically configured on the ingress port and policy marking is not applied.
- If the ingress port is configured as trusted, packets received on an EoMPLS interface are never marked by QoS policy in the original IP packet header (marking by IP policy works on untrusted ports).
- 802.1p CoS is preserved from entrance to exit, if available through the 802.1q header.
- After exiting the tunnel egress, queuing is based on preserved 802.1p CoS if 1p tag has been tunnelled in the EoMPLS header (VC type 4); otherwise, queuing is based on the CoS derived from the QoS decision.

Ethernet to MPLS

For Ethernet to MPLS, the ingress interface, MPLS QoS, and egress interface features are similar to corresponding features for IP to MPLS. For more information, see these sections:

- [Classification for IP-to-MPLS, page 38-9](#)
- [Classification for IP-to-MPLS Mode MPLS QoS, page 38-10](#)
- [Classification at IP-to-MPLS Ingress Port, page 38-10](#)
- [Classification at IP-to-MPLS Egress Port, page 38-10](#)

MPLS to Ethernet

For MPLS to Ethernet, the ingress interface, MPLS QoS, and egress interface features are similar to corresponding features for MPLS to IP except for the case of EoMPLS decapsulation where egress IP policy cannot be applied (packets can be classified as MPLS only).

For more information, see these sections:

- [Classification for MPLS-to-IP, page 38-11](#)
- [Classification for MPLS-to-IP MPLS QoS, page 38-11](#)
- [Classification at MPLS-to-IP Ingress Port, page 38-11](#)
- [Classification at MPLS-to-IP Egress Port, page 38-12.](#)

LERs at the IP Edge (MPLS, MPLS VPN)

This section provides information about QoS features for LERs at the ingress (CE-to-PE) and egress (PE-to-CE) edges for MPLS and MPLS VPN networks. Both MPLS and MPLS VPN support general MPLS QoS features. See the “[MPLS VPN](#)” section on [page 38-12](#) for additional MPLS VPN-specific QoS information.

IP to MPLS

The PFC provides the following MPLS QoS capabilities at the IP-to-MPLS edge:

- Assigning an EXP value based on the **mls qos trust** or **policy-map** command
- Marking an EXP value using a policy
- Policing traffic using a policy

This section provides information about the MPLS QoS classification that the PFC supports at the IP-to-MPLS edge. Additionally, this section provides information about the capabilities provided by the ingress and egress interface modules.

Classification for IP-to-MPLS

The PFC ingress and egress policies for IP traffic classify traffic on the original received IP using **match** commands for IP precedence, IP DSCP, and IP ACLs. Egress policies do not classify traffic on the imposed EXP value nor on a marking done by an ingress policy.

After the PFC applies the port trust and QoS policies, it assigns the internal DSCP. The PFC then assigns the EXP value based on the internal DSCP-to-EXP global map for the labels that it imposes. If more than one label is imposed, the EXP value is the same in each label. The PFC preserves the original IP ToS when the MPLS labels are imposed.

The PFC assigns the egress CoS based on the internal DSCP-to-CoS global map. If the default internal DSCP-to-EXP and the internal DSCP-to-CoS maps are consistent, then the egress CoS has the same value as the imposed EXP.

If the ingress port receives both IP-to-IP and IP-to-MPLS traffic, classification should be used to separate the two types of traffic. For example, if the IP-to-IP and IP-to-MPLS traffic have different destination address ranges, you can classify traffic on the destination address, and then apply IP ToS policies to the IP-to-IP traffic and apply a policy (that marks or sets the EXP value in the imposed MPLS header) to the IP-to-MPLS traffic. See the following two examples:

- A PFC policy to mark IP ToS sets the internal DSCP—If it is applied to all traffic, then for IP-to-IP traffic, the egress port will rewrite the CoS (derived from the internal DSCP) to the IP ToS byte in the egress packet. For IP-to-MPLS traffic, the PFC will map the internal DSCP to the imposed EXP value.
- A PFC policy to mark MPLS EXP sets the internal DSCP—If it is applied to all traffic, then for IP-to-IP traffic, the egress port rewrites the IP ToS according to the ingress IP policy (or trust). The CoS is mapped from the ToS. For IP-to-MPLS traffic, the PFC will map the internal DSCP to the imposed EXP value.

Classification for IP-to-MPLS Mode MPLS QoS

MPLS QoS at the ingress to PE1 supports:

- Matching on IP precedence or DSCP values or filtering with an access group
- The **set mpls experimental imposition** and **police** commands

MPLS QoS at the egress of PE1 supports the **mpls experimental topmost** command.

Classification at IP-to-MPLS Ingress Port

Classification for IP- to- MPLS is the same as for IP-to-IP. LAN port classification is based on the received Layer 2 802.1Q CoS value. FlexWAN interfaces classify based on information in the received Layer 3 IP header.

Classification at IP-to-MPLS Egress Port

LAN port classification is based on the received EXP value and the egress CoS values is mapped from that value.

FlexWAN interfaces classify traffic when you use the **match mpls experimental** command to match on the egress CoS as a proxy for the EXP value. The **match mpls experimental** command does not match on the EXP value in the topmost label.

If the egress port is a trunk, the LAN ports copy the egress CoS into the egress 802.1Q field.

MPLS to IP

MPLS QoS supports these capabilities at the MPLS-to-IP edge:

- Option to propagate EXP value into IP DSCP on exit from an MPLS domain per egress interface
- Option to use IP service policy on the MPLS-to-IP egress interface

This section provides information about the MPLS-to-IP MPLS QoS classification. Additionally, this section provides information about the capabilities provided by the ingress and egress modules.

Classification for MPLS-to-IP

The PFC assigns the internal DSCP (internal priority that the PFC assigns to each frame) based on the QoS result. The QoS result is affected by the following:

- Default trust EXP value
- Label type (per-prefix or aggregate)
- Number of VPNs
- Explicit NULL use
- QoS policy

There are three different classification modes:

- Regular MPLS classification—For nonaggregate labels, in the absence of MPLS recirculation, the PFC classifies the packet based on MPLS EXP ingress or egress policy. The PFC queues the packet based on COS derived from EXP-to-DSCP-to-CoS mapping. The underlying IP DSCP is either preserved after egress decapsulation, or overwritten from the EXP (through the EXP-to-DSCP map).
- IP classification for aggregate label hits in VPN CAM—The PFC does one of the following:
 - Preserves the underlying IP ToS
 - Rewrites the IP ToS by a value derived from the EXP-to-DSCP global map
 - Changes the IP ToS to any value derived from the egress IP policy

In all cases, egress queueing is based on the final IP ToS from the DSCP-to-CoS map.

- IP classification with aggregate labels not in VPN CAM—After recirculation, the PFC differentiates the MPLS-to-IP packets from the regular IP-to-IP packets based on the ingress reserved VLAN specified in the MPLS decapsulation adjacency. The reserved VLAN is allocated per VRF both for VPN and non-VPN cases. The ingress ToS after recirculation can be either the original IP ToS value, or derived from the original EXP value. The egress IP policy can overwrite this ingress ToS to an arbitrary value.



Note

For information about recirculation, see the [“Recirculation” section on page 26-4](#).

For incoming MPLS packets on the PE-to-CE ingress, the PFC supports MPLS classification only. Ingress IP policies are not supported. PE-to-CE traffic from the MPLS core is classified or policed on egress as IP.

Classification for MPLS-to-IP MPLS QoS

MPLS QoS at the ingress to PE2 supports matching on the EXP value and the **police** command.

MPLS QoS at the egress of PE2 supports matching on IP precedence or DSCP values or filtering with an access group and the **police** command.

Classification at MPLS-to-IP Ingress Port

LAN port classification is based on the EXP value. FlexWAN interfaces classify traffic using the **match mpls experimental** command. The **match mpls experimental** command matches on the EXP value in the received topmost label.

Classification at MPLS-to-IP Egress Port

**Note**

The egress classification queuing is different for LAN and WAN ports.

Classification for MPLS-to-IP is the same as it is for IP-to-IP.

The LAN interface classification is based on the egress CoS. The FlexWAN interfaces classify traffic on information in the transmitted IP header.

If the egress port is a trunk, the LAN ports copy the egress CoS into the egress 802.1Q field.

**Note**

For MPLS to IP, egress IP ACL or QoS is not effective on the egress interface if the egress interface has MPLS IP (or tag IP) enabled. The exception is a VPN CAM hit, in which case the packet is classified on egress as IP.

MPLS VPN

The information in this section also applies to an MPLS VPN network.

The following PE MPLS QoS features are supported for MPLS VPN:

- Classification, policing, or marking of CE-to-PE IP traffic through the VPN subinterface
- Per-VPN QoS (per-port, per-VLAN, or per-subinterface)

For customer edge (CE)-to-PE traffic, or for CE-to-PE-to-CE traffic, the subinterface support allows you to apply IP QoS ingress or egress policies to subinterfaces and to physical interfaces. Per-VPN policing is also provided for a specific interface or subinterface associated with a given VPN on the CE side.

In situations when there are multiple interfaces belonging to the same VPN, you can perform per-VPN policing aggregation using the same shared policer in the ingress or egress service policies for all similar interfaces associated with the same PFC.

For aggregate VPN labels, the EXP propagation in recirculation case may not be supported because MPLS adjacency does not know which egress interface the final packet will use.

**Note**

For information on recirculation, see the [“Recirculation” section on page 26-4](#).

The PFC propagates the EXP value if all interfaces in the VPN have EXP propagation enabled.

The following PE MPLS QoS features are supported:

- General MPLS QoS features for IP packets
- Classification, policing, or marking of CE-to-PE IP traffic through the VPN subinterface
- Per-VPN QoS (per-port, per-VLAN, or per-subinterface)

LSRs at the MPLS Core

This section provides information about MPLS QoS features for LSRs at the core (MPLS-to-MPLS) for MPLS and MPLS VPN networks. Ingress features, egress interface, and PFC features for Carrier Supporting Carrier (CsC) QoS features are similar to those used with MPLS to MPLS described in the next section. A difference between CsC and MPLS to MPLS is that with CsC labels can be imposed inside the MPLS domain.

MPLS to MPLS

MPLS QoS at the MPLS core supports the following:

- Per-EXP policing based on a service policy
- Copying the input topmost EXP value into the newly imposed EXP value
- Optional EXP mutation (changing of EXP values on an interface edge between two neighboring MPLS domains) on the egress boundary between MPLS domains
- Microflow policing based on individual label flows for a particular EXP value
- Optional propagation of topmost EXP value into the underlying EXP value when popping the topmost label from a multi-label stack.

The following section provides information about MPLS-to-MPLS MPLS QoS classification. Additionally, the section provides information about the capabilities provided by the ingress and egress modules.

Classification for MPLS-to-MPLS

For received MPLS packets, the PFC ignores the port trust state, the ingress CoS, and any policy-map **trust** commands. Instead, the PFC trusts the EXP value in the topmost label.

**Note**

The MPLS QoS ingress and egress policies for MPLS traffic classify traffic on the EXP value in the received topmost label when you enter the **match mpls experimental** command.

MPLS QoS maps the EXP value to the internal DSCP using the EXP-to-DSCP global map. What the PFC does next depends on whether it is swapping labels, imposing a new label, or popping a label:

- Swapping labels—When swapping labels, the PFC preserves the EXP value in the received topmost label and copies it to the EXP value in the outgoing topmost label. The PFC assigns the egress CoS using the internal DSCP-to-CoS global map. If the DSCP global maps are consistent, then the egress CoS is based on the EXP in the outgoing topmost label.

The PFC can mark down out-of-profile traffic using the **police** command's **exceed** and **violate** actions. It does not mark in-profile traffic, so the **conform** action must be transmitted and the **set** command cannot be used. If the PFC is performing a markdown, it uses the internal DSCP as an index into the internal DSCP markdown map. The PFC maps the result of the internal DSCP markdown to an EXP value using the internal DSCP-to-EXP global map. The PFC rewrites the new EXP value to the topmost outgoing label and does not copy the new EXP value to the other labels in the stack. The PFC assigns the egress CoS using the internal DSCP-to-CoS global map. If the DSCP maps are consistent, then the egress CoS is based on the EXP value in the topmost outgoing label.

- Imposing an additional label—When imposing a new label onto an existing label stack, the PFC maps the internal DSCP to the EXP value in the imposed label using the internal DSCP-to-EXP map. It then copies the EXP value in the imposed label to the underlying swapped label. The PFC assigns the egress CoS using the internal DSCP-to-CoS global map. If the DSCP maps are consistent, the egress CoS is based on the EXP value in the imposed label.

The PFC can mark in-profile and mark down out-of-profile traffic. After it marks the internal DSCP, the PFC uses the internal DSCP-to-EXP global map to map the internal DSCP to the EXP value in the newly imposed label. The PFC then copies the EXP in the imposed label to the underlying swapped label. The PFC assigns the egress CoS using the internal DSCP-to-CoS global map. Therefore, the egress CoS is based on the EXP in the imposed label.

- Popping a label—When popping a label from a multi-label stack, the PFC preserves the EXP value in the exposed label. The PFC assigns the egress CoS using the internal DSCP-to-CoS global map. If the DSCP maps are consistent, then the egress CoS is based on the EXP value in the popped label.
- If EXP propagation is configured for the egress interface, the PFC maps the internal DSCP to the EXP value in the exposed label using the DSCP-to-EXP global map. The PFC assigns the egress CoS using the internal DSCP-to-CoS global map. If the DSCP maps are consistent, the egress CoS is based on the EXP value in the exposed label.

Classification for MPLS-to-MPLS MPLS QoS

MPLS QoS at the ingress to P1 or P2 supports the following:

- Matching with the **mpls experimental topmost** command
- The **set mpls experimental imposition**, **police**, and **police** with **set imposition** commands

MPLS QoS at the egress of P1 or P2 supports matching with the **mpls experimental topmost** command.

Classification at MPLS-to-MPLS Ingress Port

LAN port classification is based on the egress CoS from the PFC. FlexWAN interfaces classify traffic using the **match mpls experimental** command. The **match mpls experimental** command matches on the EXP value in the received topmost label.

Classification at MPLS-to-MPLS Egress Port

LAN port classification is based on the egress CoS value from the PFC. FlexWAN interfaces classify traffic using the **match mpls experimental** command. The **match mpls experimental** command matches on the egress CoS; it does not match on the EXP in the topmost label.

If the egress port is a trunk, the LAN ports copy the egress CoS into the egress 802.1Q field.

MPLS QoS Default Configuration

This section describes the MPLS QoS default configuration. The following global MPLS QoS settings apply:

Feature	Default Value
PFC QoS global enable state	<p>Note With PFC QoS disabled and all other PFC QoS parameters at default values, default EXP is mapped from IP precedence.</p> <p>Note With PFC QoS enabled and all other PFC QoS parameters at default values, PFC QoS sets Layer 3 DSCP to zero (untrusted ports only), Layer 2 CoS to zero, the imposed EXP to zero in all traffic transmitted from LAN ports (default is untrusted). For trust CoS, the default EXP value is mapped from COS; for trust DSCP, the default EXP value is mapped from IP precedence.</p>
PFC QoS port enable state	Enabled when PFC QoS is globally enabled
Port CoS value	0
Microflow policing	Enabled
IntraVLAN microflow policing	Disabled
Port-based or VLAN-based PFC QoS	Port-based
EXP to DSCP map (DSCP set from EXP values)	EXP 0 = DSCP 0 EXP 1 = DSCP 8 EXP 2 = DSCP 16 EXP 3 = DSCP 24 EXP 4 = DSCP 32 EXP 5 = DSCP 40 EXP 6 = DSCP 48 EXP 7 = DSCP 56
IP precedence to DSCP map (DSCP set from IP precedence values)	IP precedence 0 = DSCP 0 IP precedence 1 = DSCP 8 IP precedence 2 = DSCP 16 IP precedence 3 = DSCP 24 IP precedence 4 = DSCP 32 IP precedence 5 = DSCP 40 IP precedence 6 = DSCP 48 IP precedence 7 = DSCP 56
DSCP to EXP map (EXP set from DSCP values)	DSCP 0–7 = EXP 0 DSCP 8–15 = EXP 1 DSCP 16–23 = EXP 2 DSCP 24–31 = EXP 3 DSCP 32–39 = EXP 4 DSCP 40–47 = EXP 5 DSCP 48–55 = EXP 6 DSCP 56–63 = EXP 7

Feature	Default Value
Marked-down DSCP from DSCP map	Marked-down DSCP value equals original DSCP value (no mark down)
EXP mutation map	No mutation map by default
Policers	None
Policy maps	None
MPLS flow mask in NetFlow table	Label + EXP value
MPLS core QoS	<p>There are four possibilities at the MPLS core QoS:</p> <ul style="list-style-type: none"> Swapping—Incoming EXP field is copied to outgoing EXP field. Swapping + imposition—Incoming EXP field is copied to both the swapped EXP field and the imposed EXP field. <p>Note If there is a service policy with a set for EXP field, its EXP field will be placed into the imposed label and also into the swapped label.</p> <ul style="list-style-type: none"> Disposition of topmost label—Exposed EXP field is preserved. Disposition of only label—Exposed IP DSCP is preserved.
MPLS to IP edge QoS	Preserve the exposed IP DSCP

MPLS QoS Commands

MPLS QoS supports the following MPLS QoS commands:

- **match mpls experimental topmost**
- **set mpls experimental imposition**
- **police**
- **mls qos map exp-dscp**
- **mls qos map dscp-exp**
- **mls qos map exp-mutation**
- **mls qos exp-mutation**
- **show mls qos mpls**
- **no mls qos mpls trust exp**



Note

For information about supported non-MPLS QoS commands, see [“Configuring PFC QoS” section on page 36-53](#).

The following commands are not supported:

- **set qos-group**
- **set discard-class**

MPLS QoS Restrictions and Guidelines

When configuring MPLS QoS, follow these guidelines and restrictions:

- For IP-to-MPLS or EoMPLS imposition when the received packet is an IP packet:
 - When QoS is disabled, the EXP value is based on the received IP ToS.
 - When QoS is queuing only, the EXP value is based on the received IP ToS.
- For EoMPLS imposition when the received packet is a non-IP packet:
 - When QoS is disabled, the EXP value is based on the ingress CoS.
 - When QoS is queuing only, the EXP value is based on the received IP ToS.
- For MPLS-to-MPLS operations:
 - Swapping when QoS is disabled, the EXP value is based on the original EXP value (in the absence of EXP mutation).
 - Swapping when QoS is queuing only, the EXP value is based on the original EXP value (in the absence of EXP mutation).
 - Imposing additional label when QoS is disabled, the EXP value is based on the original EXP value (in the absence of EXP mutation).
 - Imposing an additional label when QoS is queuing only, the EXP value is based on the original EXP value (in the absence of EXP mutation).
 - Popping one label when QoS is disabled, the EXP value is based on the underlying EXP value.
 - Popping one label when QoS is queuing only, the EXP value is based on the underlying EXP value.
- EXP value is irrelevant to MPLS-to-IP disposition.
- The **no mls qos rewrite ip dscp** command is incompatible with MPLS. The default **mls qos rewrite ip dscp** command must remain enabled in order for the PFC to assign the correct EXP value for the labels that it imposes.
- The **no mls qos mpls trust exp** command allows you to treat MPLS packets similarly to Layer 2 packets for CoS and egress queuing purposes by applying port trust or policy trust instead of the default EXP value.

Configuring MPLS QoS

These sections describe how to configure MPLS QoS:

- [Enabling QoS Globally, page 38-18](#)
- [Enabling Queueing-Only Mode, page 38-19](#)
- [Configuring a Class Map to Classify MPLS Packets, page 38-20](#)
- [Configuring the MPLS Packet Trust State on Ingress Ports, page 38-22](#)

- [Configuring a Policy Map, page 38-23](#)
- [Displaying a Policy Map, page 38-27](#)
- [Configuring MPLS QoS Egress EXP Mutation, page 38-29](#)
- [Configuring EXP Value Maps, page 38-30](#)

Enabling QoS Globally

Before you can configure QoS on the PFC, you must enable the QoS functionality globally using the **mls qos** command. This command enables default QoS conditioning of traffic.

When the **mls qos** command is enabled, the PFC assigns a priority value to each frame. This value is the internal DSCP. The internal DSCP is assigned based on the contents of the received frame and the QoS configuration. This value is rewritten to the egress frame's CoS and ToS fields.

To enable QoS globally, perform this task:

	Command	Purpose
Step 1	Router(config)# mls qos	Enables PFC QoS globally on the switch.
	Router(config)# no mls qos	Disables PFC QoS globally on the switch.
Step 2	Router(config)# end	Exits configuration mode.
Step 3	Router# show mls qos	Verifies the configuration.

This example shows how to enable QoS globally:

```
Router(config)# mls qos
Router(config)# end
Router#
```

This example shows how to verify the configuration:

```
Router# show mls qos
QoS is enabled globally
  Microflow policing is enabled globally
  QoS ip packet dscp rewrite enabled globally

QoS trust state is DSCP on the following interfaces:
  Gi4/1 Gi4/1.12

QoS trust state is IP Precedence on the following interfaces:
  Gi4/2 Gi4/2.42
Vlan or Portchannel(Multi-Earl) policies supported: Yes
Egress policies supported: Yes

----- Module [5] -----
QoS global counters:
  Total packets: 5957870
  IP shortcut packets: 0
  Packets dropped by policing: 0
  IP packets with TOS changed by policing: 6
  IP packets with COS changed by policing: 0
  Non-IP packets with COS changed by policing: 3
  MPLS packets with EXP changed by policing: 0
```

Enabling Queueing-Only Mode

To enable queueing-only mode, perform this task:

	Command	Purpose
Step 1	Router(config)# mls qos queueing-only	Enables queueing-only mode.
	Router(config)# no mls qos queueing-only	Disables PFC QoS globally. Note You cannot disable queueing-only mode separately.
Step 2	Router(config)# end	Exits configuration mode.
Step 3	Router# show mls qos	Verifies the configuration.

When you enable queueing-only mode, the router does the following:

- Disables marking and policing globally
- Configures all ports to trust Layer 2 CoS



Note The switch applies the port CoS value to untagged ingress traffic and to traffic that is received through ports that cannot be configured to trust CoS.

This example shows how to enable queueing-only mode:

```
Router# configure terminal
Router(config)# mls qos queueing-only
Router(config)# end
Router#
```

Restrictions and Usage Guidelines

If QoS is disabled (**no mls qos**) for the PFC, the EXP value is determined as follows:

- For IP-to-MPLS or EoMPLS imposition when the received packet is an IP packet:
 - When QoS is disabled (**no mls qos**), the EXP value is based on the received IP ToS.
 - When QoS is queuing only (**mls qos queueing-only**), the EXP value is based on the received IP ToS.
- For EoMPLS imposition when the received packet is a non-IP packet:
 - When QoS is disabled, the EXP value is based on the ingress CoS.
 - When QoS is queuing only, the EXP value is based on the received IP ToS.
- For MPLS-to-MPLS operations:
 - Swapping when QoS is disabled, the EXP value is based on the original EXP value (in the absence of EXP mutation).
 - Swapping when QoS is queuing only, the EXP value is based on the original EXP value (in the absence of EXP mutation).
 - Imposing an additional label when QoS is disabled, the EXP value is based on the original EXP value (in the absence of EXP mutation).

- Imposing additional label when QoS is queuing only, the EXP value is based on the original EXP value (in the absence of EXP mutation).
 - Popping one label when QoS is disabled, the EXP value is based on the underlying EXP value.
 - Popping one label when QoS is queuing only, the EXP value is based on the underlying EXP value.
- EXP value is irrelevant to MPLS-to-IP disposition.

Configuring a Class Map to Classify MPLS Packets

You can use the **match mpls experimental topmost** command to define traffic classes inside the MPLS domain by packet EXP values. This allows you to define service policies to police the EXP traffic on a per-interface basis by using the **police** command.

To configure a class map, perform this task beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# class-map <i>class_name</i>	Specifies the class map to which packets will be matched.
Step 2	Router(config-cmap)# match mpls experimental topmost <i>value</i>	Specifies the packet characteristics that will be matched to the class.
Step 3	Router(config-cmap)# exit	Exits class-map configuration mode.

This example shows that all packets that contain MPLS experimental value 3 are matched by the traffic class named exp3:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# class-map exp3
Router(config-cmap)# match mpls experimental topmost 3
Router(config-cmap)# exit
Router(config)# policy-map exp3
Router(config-pmap)# class exp3
Router(config-pmap-c)# police 1000000 8000000 conform-action transmit exceed-action drop
Router(config-pmap-c)# exit
Router(config-pmap)# end
Router# show class exp3
Class Map match-all exp3 (id 61)
  Match mpls experimental topmost 3
Router# show policy-map exp3
Policy Map exp3
  Class exp3
    police cir 1000000 bc 8000000 be 8000000 conform-action transmit exceed-action drop
Router# show running-config interface fastethernet 3/27
Building configuration...

Current configuration : 173 bytes
!
interface FastEthernet3/27
 ip address 47.0.0.1 255.0.0.0
 tag-switching ip
end

Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
```

```

Router(config)# interface fastethernet 3/27
Router(config-if)# service-policy input exp3
Router(config-if)#
Router#
Enter configuration commands, one per line. End with CNTL/Z.
Router# show running-config interface fastethernet 3/27
Building configuration...

Current configuration : 173 bytes
!
interface FastEthernet3/27
 ip address 47.0.0.1 255.0.0.0
 tag-switching ip
 service-policy input exp3
end

Router#
1w4d: %SYS-5-CONFIG_I: Configured from console by console
Router# show mls qos mpls
QoS Summary [MPLS]: (* - shared aggregates, Mod - switch module)

      Int Mod Dir  Class-map DSCP  Agg  Trust Fl  AgForward-By  AgPoliced-By
-----
      Fa3/27  5  In      exp3    0    2   dscp  0           0           0

      All  5  -      Default  0    0*   No   0       3466140423      0
Router# show policy-map interface fastethernet 3/27
FastEthernet3/27

Service-policy input: exp3

class-map: exp3 (match-all)
 Match: mpls experimental topmost 3
 police :
  1000000 bps 8000000 limit 8000000 extended limit
Earl in slot 5 :
  0 bytes
  5 minute offered rate 0 bps
 aggregate-forwarded 0 bytes action: transmit
 exceeded 0 bytes action: drop
 aggregate-forward 0 bps exceed 0 bps

Class-map: class-default (match-any)
  0 packets, 0 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
 Match: any

Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface fastethernet 3/27
Router(config-if)# service-policy output ip2tag
Router(config-if)# end
Router# show mls qos ip
QoS Summary [IPv4]: (* - shared aggregates, Mod - switch module)

      Int Mod Dir  Class-map DSCP  Agg  Trust Fl  AgForward-By  AgPoliced-By
-----
      Vl300  5  In      x      44    1   No   0           0           0
      Fa3/27  5  Out     iptcp  24    2   --   0           0           0

      All  5  -      Default  0    0*   No   0       3466610741      0

```

Restrictions and Usage Guidelines

The following restrictions and guidelines apply when classifying MPLS packets:

- The **match mpls experimental** command specifies the name of an EXP field value to be used as the match criterion against which packets are checked to determine if they belong to the class specified by the class map.
- To use the **match mpls experimental** command, you must first enter the **class-map** command to specify the name of the class whose match criteria you want to establish. After you identify the class, you can use the **match mpls experimental** command to configure its match criteria.
- If you specify more than one command in a class map, only the last command entered applies. The last command overrides the previously entered commands.

Configuring the MPLS Packet Trust State on Ingress Ports

You can use the **no mls qos mpls trust exp** command to apply port or policy trust to MPLS packets in the same way that you apply them to Layer 2 packets.

To configure the MPLS packet trust state of an ingress port, perform this task:

	Command	Purpose
Step 1	Router(config)# interface {{type slot/port} {port-channel number}}	Selects the interface to configure.
Step 2	Router(config-if)# no mls qos mpls trust exp	Sets the trust state of an MPLS packet so that all trusted cases (trust cos, trust dscp, trust ip-precedence) are treated as trust-cos.
	Router(config-if)# mls qos mpls trust exp	Reverts to the default trust state where only the EXP value in the incoming packet is trusted.
Step 3	Router(config-if)# end	Exits interface configuration mode.
Step 4	Router# show mls qos	Verifies the configuration.

This example shows how to set the trusted state of MPLS packets to untrusted so that the incoming MPLS packets operate like incoming Layer 2 packets.

```
Router(config)# interface fastethernet 3/27
Router(config-if)# no mls qos mpls trust exp
Router(config-if)#
```

Restrictions and Usage Guidelines

The following restrictions and guidelines apply when using the **no mls qos mpls trust exp** command to configure the MPLS packet trust state on input ports:

- This command affects both Layer 2 and Layer 3 packets; use this command only on interfaces with Layer 2 switched packets.
- The **no mls qos mpls trust exp** command affects ingress marking; it does not affect classification.

Configuring a Policy Map

You can attach only one policy map to an interface. Policy maps can contain one or more policy map classes, each with different policy map commands.

Configure a separate policy map class in the policy map for each type of traffic that an interface receives. Put all commands for each type of traffic in the same policy map class. MPLS QoS does not attempt to apply commands from more than one policy map class to matched traffic.

Configuring a Policy Map to Set the EXP Value on All Imposed Labels

To set the value of the MPLS EXP field on all imposed label entries, use the **set mpls experimental imposition** command in QoS policy-map class configuration mode. To disable the setting, use the no form of this command.



Note The **set mpls experimental imposition** command replaces the **set mpls experimental** command.

	Command	Purpose
Step 1	Router(config)# policy-map <i>policy_name</i>	Creates a policy map.
Step 2	Router(config-pmap)# class-map <i>name</i> [match-all match-any]	Accesses the QoS class-map configuration mode to configure QoS class maps.
Step 3	Router(config-pmap-c)# set mpls experimental imposition { <i>mpls-exp-value</i> <i>from-field</i> [table <i>table-map-name</i>]}	Sets the value of the MPLS experimental (EXP) field on all imposed label entries.
Step 4	Router(config-pmap-c)# exit	Exits class-map configuration mode.

The following example sets the MPLS EXP imposition value according to the DSCP value defined in the MPLS EXP value 3:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# access-1 101 p tcp any any
Router(config)# class-map iptcp
Router(config-cmap)# match acc 101
Router(config-cmap)# exit
Router(config)#
Router(config-cmap)# policy-map ip2tag
Router(config-pmap)# class iptcp
Router(config-pmap-c)# set mpls exp imposition 3
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)#
Router#
1w4d: %SYS-5-CONFIG_I: Configured from console by console
Router#
Router# show policy-map ip2tag
  Policy Map ip2tag
    Class iptcp
      set mpls experimental imposition 3
Router# show class iptcp
  Class Map match-all iptcp (id 62)
    Match access-group101
```

```

Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface fastethernet 3/27
Router(config-if)# ser in ip2tag
Router(config-if)#
Routers
1w4d: %SYS-5-CONFIG_I: Configured from console by console
Router# show pol ip2tag
  Policy Map ip2tag
    Class iptcp
      set mpls experimental imposition 3
Router# show class-map iptcp
  Class Map match-all iptcp (id 62)
    Match access-group 101

Router# show access-l 101
Extended IP access list 101
  10 permit tcp any any
Router# show mls qos ip
QoS Summary [IPv4]:          (* - shared aggregates, Mod - switch module)

      Int Mod Dir  Class-map DSCP  Agg  Trust Fl  AgForward-By  AgPoliced-By
      -----
      Fa3/27  5  In    iptcp   24   2    No  0           0             0
      Vl300   5  In     x     44   1    No  0           0             0

      All 5 -   Default  0   0*   No  0   3466448105  0

Router#
Router# show policy-map interface fastethernet 3/27
FastEthernet3/27

Service-policy input: ip2tag

class-map: iptcp (match-all)
  Match: access-group 101
  set mpls experimental 3:
  Earl in slot 5 :
    0 bytes
    5 minute offered rate 0 bps
    aggregate-forwarded 0 bytes

class-map: class-default (match-any)
  Match: any

Class-map: class-default (match-any)
  0 packets, 0 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
  Match: any

```

This example shows how to verify the configuration:

```

Router# show policy map ip2tag
  Policy Map ip2tag
    Class iptcp
      set mpls experimental imposition 3

```


EXP Value Imposition Guidelines and Restrictions

When setting the EXP value on all imposed labels, follow these guidelines and restrictions:

- Use the **set mpls experimental imposition** command during label imposition. This command sets the MPLS EXP field on all imposed label entries.
- The **set mpls experimental imposition** command is supported only on input interfaces (imposition).
- The **set mpls experimental imposition** command does not mark the EXP value directly; instead, it marks the internal DSCP that is mapped to EXP through the internal DSCP-to-EXP global map.
- It is important to note that classification (based on the original received IP header) and marking (done to the internal DSCP) do not distinguish between IP-to-IP traffic and IP-to-MPLS traffic. The commands that you use to mark IP ToS and mark EXP have the same result as when you mark the internal DSCP.
- To set the pushed label entry value to a value different from the default value during label imposition, use the **set mpls experimental imposition** command.
- You optionally can use the **set mpls experimental imposition** command with the IP precedence, DSCP field, or QoS IP ACL to set the value of the MPLS EXP field on all imposed label entries.
- When imposing labels onto the received IP traffic with the PFC, you can mark the EXP field using the **set mpls experimental imposition** command.

For more information on this command, see the *Cisco IOS Switching Services Command Reference, Release 12.3* located at this URL:

http://www.cisco.com/en/US/products/sw/iosswrel/ps5187/products_command_reference_chapter09186a008017cf44.html#wp1092877

Configuring a Policy Map Using the Police Command

Policing is a function in the PFC hardware that provides the ability to rate limit a particular traffic class to a specific rate. The PFC supports aggregate policing and microflow policing.

Aggregate policing meters all traffic that ingresses into a port, regardless of different source, destination, protocol, source port, or destination port. Microflow policing meters all traffic that ingresses into a port, on a per flow (per source, destination, protocol, source port, and destination port). For additional information on aggregate and microflow policing, see the “Policers” section on page 36-17.

To configure traffic policing, use the **police** command. For information on this command, see the Cisco IOS Software Releases 12.2SX Command References.

	Command	Purpose
Step 1	Router(config)# policy-map <i>policy_name</i>	Creates a policy map.
Step 2	Router(config-pmap)# class-map <i>name</i> [match-all match-any]	Accesses the QoS class map configuration mode to configure QoS class maps.
Step 3	Router(config-pmap-c)# police { aggregate <i>name</i> }	Adds the class to a shared aggregate policer.
Step 4	Router(config-pmap-c)# police <i>bps burst_normal burst_max conform-action action exceed-action action violate-action action</i>	Creates a per-class-per-interface policer.

	Command	Purpose
Step 5	Router(config-pmap-c)# police flow {bps [burst_normal] [conform-action action] [exceed-action action]}	Creates an ingress flow policer. (Not supported in egress policy.)
Step 6	Router(config-pmap-c)# exit	Exits class-map configuration mode.

This is an example of creating a policy map with a policer:

```
Router(config)# policy-map ip2tag
Router(config-pmap)# class iptcp
Router(config-pmap-c)# no set mpls exp topmost 3
Router(config-pmap-c)# police 1000000 1000000 c set-mpls-exp?
set-mpls-exp-imposition-transmit

Router(config-pmap-c)# police 1000000 1000000 c set-mpls-exp-imposit 3 e d
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface fastethernet 3/27
Router(config-if)# ser in ip2tag
Router(config-if)#
```

This is an example of verifying the configuration:

```
Router# show pol ip2tag
Policy Map ip2tag
Class iptcp
  police cir 1000000 bc 1000000 be 1000000 conform-action
set-mpls-exp-imposition-transmit 3 exceed-action drop
Router# show running-config interface fastethernet 3/27
Building configuration...
```

```
Current configuration : 202 bytes
!
interface FastEthernet3/27
  logging event link-status
  service-policy input ip2tag
end
```

```
Router# show mls qos ip
QoS Summary [IPv4]:          (* - shared aggregates, Mod - switch module)

      Int Mod Dir  Class-map DSCP  Agg  Trust Fl  AgForward-By  AgPoliced-By
      -----
      Fa3/27  5  In    iptcp   24   2    No  0           0             0
      Vl300   5  In     x     44   1    No  0           0             0

      All 5 -   Default  0   0*   No  0           3468105262    0
```

```
Router# show policy interface fastethernet 3/27
FastEthernet3/27

Service-policy input: ip2tag

class-map: iptcp (match-all)
Match: access-group 101
police :
  1000000 bps 1000000 limit 1000000 extended limit
Earl in slot 5 :
  0 bytes
  5 minute offered rate 0 bps
  aggregate-forwarded 0 bytes action: set-mpls-exp-imposition-transmit
  exceeded 0 bytes action: drop
```

```

aggregate-forward 0 bps exceed 0 bps

class-map: class-default (match-any)
  Match: any

Class-map: class-default (match-any)
  0 packets, 0 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
  Match: any
R7# show mls qos ip
QoS Summary [IPv4]:          (* - shared aggregates, Mod - switch module)

      Int Mod Dir  Class-map DSCP  Agg  Trust Fl  AgForward-By  AgPoliced-By
      -----
      Fa3/27  5  In    iptcp   24   2   No  0           0             0
      Vl300   5  In     x     44   1   No  0           0             0

      All  5  -    Default  0   0*  No  0       3468161522    0

```

Restrictions and Usage Guidelines

The following restrictions and guidelines apply when using the **police** command to configure a policy map:

- With MPLS, the **exceed-action** *action* command and the **violate-action** *action* command work similarly to IP usage. The packet may get dropped or the EXP value is marked down. For information on how these actions affect IP-to-IP traffic, see the [“Configuring a Policy Map”](#) section on page 36-69.
- With MPLS, the **set-dscp transmit** *action* command and the **set-prec-transmit** *action* command set the internal DSCP that is mapped into the CoS bits, which affects queuing, however, they do not change the EXP value, except for imposition.
- When swapping labels for received MPLS traffic with the PFC, you can mark down out-of-profile traffic using the **police** command **exceed-action policed-dscp-transmit** and **violate-action policed-dscp-transmit** keywords. The PFC does not mark in-profile traffic; when marking down out-of-profile traffic, the PFC marks the outgoing topmost label. The PFC does not propagate the marking down through the label stack.
- With MPLS, the flow key is based on the label and EXP value; there is no flowmask option. Otherwise, flow key operation is similar to IP-to-IP. See the [“Configuring a Policy Map”](#) section on page 36-69.
- You can use the **police** command to set the pushed label entry value to a value different from the default value during label imposition.
- When imposing labels onto the received IP traffic with the PFC, you can mark the EXP field using the **conform-action set-mpls-exp-imposition-transmit** keywords.
- During IP-to-MPLS imposition, IP ToS marking is not supported. If you configure a policy to mark IP ToS, the PFC marks the EXP value.

Displaying a Policy Map

You can display a policy map with an interface summary for MPLS QoS classes or with the configuration of all classes configured for all service policies on the specified interface.

Displaying an MPLS QoS Policy Map Class Summary

To display an MPLS QoS policy map class summary, perform this task:

Command	Purpose
Router# show mls qos mpls [{ interface <i>interface_type</i> <i>interface_number</i> } { module <i>slot</i> }]	Displays an MPLS QoS policy map class summary.

This example shows how to display an MPLS QoS policy map class summary:

```
Router# show mls qos mpls
QoS Summary [MPLS]:      (* - shared aggregates, Mod - switch module)
  Int Mod Dir  Class-map DSCP  Agg  Trust Fl  AgForward-By  AgPoliced-By
                               Id      Id
-----
  Fa3/27  5  In    exp3    0    2  dscp  0           0           0
        All  5  -    Default  0    0*  No   0           3466140423  0
```

Displaying the Configuration of All Classes

To display the configuration of all classes configured for all service policies on the specified interface, perform this task:

Command	Purpose
Router# show policy interface <i>interface_type</i> <i>interface_number</i>	Displays the configuration of all classes configured for all policy maps on the specified interface.

This example shows the configurations for all classes on Fast Ethernet interface 3/27:

```
Router# show policy interface fastethernet 3/27
FastEthernet3/27

Service-policy input: ip2tag

  class-map: iptcp (match-all)
    Match: access-group 101
    police :
      1000000 bps 1000000 limit 1000000 extended limit
    Earl in slot 5 :
      0 bytes
      5 minute offered rate 0 bps
      aggregate-forwarded 0 bytes action: set-mls-exp-imposition-transmit
      exceeded 0 bytes action: drop
      aggregate-forward 0 bps exceed 0 bps

  class-map: class-default (match-any)
    Match: any

  Class-map: class-default (match-any)
    0 packets, 0 bytes
    5 minute offered rate 0 bps, drop rate 0 bps
    Match: any
```

Configuring MPLS QoS Egress EXP Mutation

These sections describe how to configure MPLS QoS egress EXP mutation:

- [Configuring Named EXP Mutation Maps, page 38-29](#)
- [Attaching an Egress EXP Mutation Map to an Interface, page 38-29](#)

Configuring Named EXP Mutation Maps

To configure a named EXP mutation map, perform this task:

	Command	Purpose
Step 1	<pre>Router(config)# mls qos map exp-mutation name mutated_exp1 mutated_exp2 mutated_exp3 mutated_exp4 mutated_exp5 mutated_exp6 mutated_exp7 mutated_exp8 Router(config)# no mls qos map exp-mutation name</pre>	<p>Configures a named EXP mutation map.</p> <p>Reverts to the default map.</p>
Step 2	<pre>Router(config)# end</pre>	Exits configuration mode.
Step 3	<pre>Router# show mls qos maps</pre>	Verifies the configuration.

When configuring a named EXP mutation map, note the following information:

- You can enter up to eight input EXP values that map to a mutated EXP value.
- You can enter multiple commands to map additional EXP values to a mutated EXP value.
- You can enter a separate command for each mutated EXP value.
- You can configure 15 ingress EXP mutation maps to mutate the internal EXP value before it is written as the ingress EXP value. You can attach ingress EXP mutation maps to any interface that PFC QoS supports.
- PFC QoS derives the egress EXP value from the internal DSCP value. If you configure ingress EXP mutation, PFC QoS does not derive the ingress EXP value from the mutated EXP value.

Attaching an Egress EXP Mutation Map to an Interface

To attach an egress EXP mutation map to an interface, perform this task:

	Command	Purpose
Step 1	<pre>Router(config)# interface {{vlan vlan_ID} {type¹ slot/port[.subinterface]} {port-channel number[.subinterface]}}</pre>	Selects the interface to configure.
Step 2	<pre>Router(config-if)# mls qos exp-mutation exp-mutation-table-name Router(config-if)# no mls qos exp-mutation</pre>	<p>Attaches an egress EXP mutation map to the interface.</p> <p>Removes the egress DSCP mutation map from the interface.</p>
Step 3	<pre>Router(config-if)# end</pre>	Exits configuration mode.
Step 4	<pre>Router# show running-config interface {{vlan vlan_ID} {type slot/port} {port-channel number}}</pre>	Verifies the configuration.

1. *type* = fastethernet, gigabitethernet, or tengigabitethernet

This example shows how to attach the egress EXP mutation map named mutemap2:

```
Router(config)# interface fastethernet 3/26
Router(config-if)# mls qos exp-mutation mutemap2
Router(config-if)# end
```

Configuring EXP Value Maps

These sections describe how EXP values are mapped to other values:

- [Configuring an Ingress-EXP to Internal-DSCP Map, page 38-30](#)
- [Configuring a Named Egress-DSCP to Egress-EXP Map, page 38-30](#)

Configuring an Ingress-EXP to Internal-DSCP Map

To configure an ingress-EXP to internal-DSCP map, perform this task:

	Command	Purpose
Step 1	Router(config)# mls qos map exp-dscp values	Configures the ingress-EXP value to internal-DSCP map. You must enter eight DSCP values corresponding to the EXP values. Valid values are 0 through 63.
	Router(config)# no mls qos map exp-dscp	Reverts to the default map.
Step 2	Router(config)# end	Exits configuration mode.
Step 3	Router# show mls qos maps	Verifies the configuration.

This example shows how to configure an ingress-EXP to internal-DSCP map:

```
Router(config)# mls qos map exp-dscp 43 43 43 43 43 43 43 43
Router(config)#
```

This example shows how to verify the configuration:

```
Router(config)# show mls qos map exp-dscp
Exp-dscp map:
  exp:  0  1  2  3  4  5  6  7
-----
  dscp: 43 43 43 43 43 43 43 43
```

Configuring a Named Egress-DSCP to Egress-EXP Map

To configure a named egress-DSCP to egress-EXP map, perform this task:

	Command	Purpose
Step 1	Router(config)# mls qos map dscp-exp dscp_values to exp_values	Configures a named egress-DSCP to egress-EXP map. You can enter up to eight DSCP values at one time to a single EXP value. Valid values are 0 through 7.
	Router(config)# no mls qos map dscp-exp	Reverts to the default map.

	Command	Purpose
Step 2	Router(config)# end	Exits configuration mode.
Step 3	Router# show mls qos maps	Verifies the configuration.

This example shows how to configure a named egress-DSCP to egress-EXP map:

```
Router(config)# mls qos map dscp-exp 20 25 to 3
Router(config)#
```

MPLS DiffServ Tunneling Modes

Tunneling provides QoS the ability to be transparent from one edge of a network to the other edge of the network. A tunnel starts where there is label imposition. A tunnel ends where there is label disposition; that is, where the label is removed from the stack, and the packet goes out as an MPLS packet with a different per-hop behavior (PHB) layer underneath or as an IP packet with the IP PHB layer.

For the PFC, there are two ways to forward packets through a network:

- **Short Pipe mode**—In Short Pipe mode, the egress PE router uses the original packet marking instead of the marking used by the intermediate provider (P) routers. EXP marking does not propagate to the packet ToS byte.

For a description of this mode, see the “[Short Pipe Mode](#)” section on page 38-31.

For the configuration information, see the “[Configuring Short Pipe Mode](#)” section on page 38-34.

- **Uniform mode**—In Uniform mode, the marking in the IP packet may be manipulated to reflect the service provider’s QoS marking in the core. This mode provides consistent QoS classification and marking throughout the network including CE and core routers. EXP marking is propagated to the underlying ToS byte.

For a description, see the “[Uniform Mode](#)” section on page 38-33.

For the configuration procedure, see the “[Configuring Uniform Mode](#)” section on page 38-39.

Both tunneling modes affect the behavior of edge and penultimate label switching routers (LSRs) where labels are put onto packets and removed from packets. They do not affect label swapping at intermediate routers. A service provider can choose different types of tunneling modes for each customer.

For additional information, see “MPLS DiffServ Tunneling Modes” at this URL:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_feature_guide09186a0080110bd5.html.

Short Pipe Mode

Short pipe mode is used when the customer and service provider are in different DiffServ domains. It allows the service provider to enforce its own DiffServ policy while preserving customer DiffServ information, which provides a DiffServ transparency through the service provider network.

QoS policies implemented in the core do not propagate to the packet ToS byte. The classification based on MPLS EXP value ends at the customer-facing egress PE interface; classification at the customer-facing egress PE interface is based on the original IP packet header and not the MPLS header.

**Note**

The presence of an egress IP policy (based on the customer's PHB marking and not on the provider's PHB marking) automatically implies the Short Pipe mode.

Figure 38-2 Short Pipe Mode Operation with VPNs



Short Pipe mode functions as follows:

1. CE1 transmits an IP packet to PE1 with an IP DSCP value of 1.
2. PE1 sets the MPLS EXP field to 5 in the imposed label entries.
3. PE1 transmits the packet to P1.
4. P1 sets the MPLS EXP field value to 5 in the swapped label entry.
5. P1 transmits the packet to P2.
6. P2 pops the IGP label entry.
7. P2 transmits the packet to PE2.
8. PE2 pops the BGP label.
9. PE2 transmits the packet to CE2, but does QoS based on the IP DSCP value.

For additional information, see “MPLS DiffServ Tunneling Modes” at this URL:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_feature_guide09186a0080110bd5.html

Short Pipe Mode Restrictions and Guidelines

The following restriction applies to Short Pipe mode:

Short Pipe mode is not supported if the MPLS-to-IP egress interface is EoMPLS (the adjacency has the end of marker (EOM) bit set).

Uniform Mode

In Uniform mode, packets are treated uniformly in the IP and MPLS networks; that is, the IP precedence value and the MPLS EXP bits always correspond to the same PHB. Whenever a router changes or recolors the PHB of a packet, that change must be propagated to all encapsulation markings. The propagation is performed by a router only when a PHB is added or exposed due to label imposition or disposition on any router in the packet's path. The color must be reflected everywhere at all levels. For example, if a packet's QoS marking is changed in the MPLS network, the IP QoS marking reflects that change.

Figure 38-3 Uniform Mode Operation



The procedure varies according to whether IP precedence bit markings or DSCP markings are present.

The following actions occur if there are IP precedence bit markings:

1. IP packets arrive in the MPLS network at PE1, the service provider edge router.
2. A label is copied onto the packet.
3. If the MPLS EXP field value is recolors (for example, if the packet becomes out-of-rate because too many packets are being transmitted), that value is copied to the IGP label. The value of the BGP label is not changed.
4. At the penultimate hop, the IGP label is removed. That value is copied into the next lower level label.
5. When all MPLS labels have been removed from the packet that is sent out as an IP packet, the IP precedence or DSCP value is set to the last changed EXP value in the core.

The following is an example when there are IP precedence bit markings:

1. At CE1 (customer equipment 1), the IP packet has an IP precedence value of 3.
2. When the packet arrives in the MPLS network at PE1 (the service provider edge router), the IP precedence value of 3 is copied to the imposed label entries of the packet.

3. The MPLS EXP field in the IGP label header might be changed within the MPLS core (for example, at P1) by a mark down.

**Note**

Because the IP precedence bits are 3, the BGP label and the IGP label also contain 3 because in Uniform mode, the labels always are identical. The packet is treated uniformly in the IP and MPLS networks.

Uniform Mode Restrictions and Guidelines

The following restriction applies to the Uniform mode:

If the egress IP ACLs or service policies are configured on the MPLS-to-IP exit point, the Uniform mode is always enforced because of recirculation.

MPLS DiffServ Tunneling Restrictions and Usage Guidelines

The MPLS DiffServ tunneling restrictions and usage guidelines are as follows:

- One label-switched path (LSP) can support up to eight classes of traffic (that is, eight PHBs) because the MPLS EXP field is a 3-bit field.
- MPLS DiffServ tunneling modes support E-LSPs. An E-LSP is an LSP on which nodes determine the QoS treatment for MPLS packet exclusively from the EXP bits in the MPLS header.

The following features are supported with the MPLS differentiated service (DiffServ) tunneling modes:

- MPLS per-hop behavior (PHB) layer management. (Layer management is the ability to provide an additional layer of PHB marking to a packet.)
- Improved scalability of the MPLS layer management by control on managed customer edge (CE) routers.
- MPLS can tunnel a packet's QoS (that is, the QoS is transparent from edge to edge). With QoS transparency, the IP marking in the IP packet is preserved across the MPLS network.
- The MPLS EXP field can be marked differently and separately from the PHB marked in the IP precedence or DSCP field.

Configuring Short Pipe Mode

The following sections describe how to configure the Short Pipe mode:

- [Ingress PE Router—Customer Facing Interface, page 38-35](#)
- [Configuring Ingress PE Router—P Facing Interface, page 38-36](#)
- [Configuring the P Router—Output Interface, page 38-37](#)
- [Configuring the Egress PE Router—Customer Facing Interface, page 38-38](#)

**Note**

-
- The steps that follow show one way, but not the only way, to configure Short Pipe mode.
 - The Short Pipe mode on the egress PE (or PHP) is automatically configured when you attach to the interface an egress service policy that includes an IP class.
-

Ingress PE Router—Customer Facing Interface

This procedure configures a policy map to set the MPLS EXP field in the imposed label entries.

To set the EXP value, the ingress LAN port must be untrusted. FlexWAN ports do not have the trust concept, but, as with traditional Cisco IOS routers, the ingress ToS is not changed (unless a marking policy is configured).

For MPLS and VPN, the ingress PE supports all ingress PFC IP policies. For information about the classification for PFC IP policies based on IP ACL/DSCP/precedence, see <http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/software/122sx/swcg/qos.htm>.

To configure a policy map to set the MPLS EXP field in the imposed label entries, perform this task:

	Command	Purpose
Step 1	Router(config)# mls qos	Enables PFC QoS globally.
Step 2	Router(config)# access-list <i>ipv4_acl_number_or_name</i> permit any	Creates an IPv4 access list.
Step 3	Router(config)# class-map <i>class_name</i>	Creates a class map.
Step 4	Router(config-cmap)# match access-group <i>ipv4_acl_number_or_name</i>	Configures the class map to filter with the ACL created in step 2.
Step 5	Router(config)# policy-map <i>policy_map_name</i>	Creates a named QoS policy.
Step 6	Router(config-pmap)# class <i>class_name</i>	Configures the policy to use the class map created in step 3.
Step 7	Router(config-pmap-c) # police <i>bits_per_second</i> [<i>normal_burst_bytes</i>] conform-action set-mpls-exp-transmit <i>exp_value</i> exceed-action drop	Configures policing, including the following: <ul style="list-style-type: none"> Action to take on packets that conform to the rate limit specified in the service level agreement (SLA). Action to take on packets that exceed the rate limit specified in the SLA. <p>The <i>exp_value</i> sets the MPLS EXP field.</p>
Step 8	Router(config)# interface <i>type slot/port</i>	Selects an interface to configure.
Step 9	Router(config-if)# no mls qos trust	Configures the interface as untrusted.
Step 10	Router(config-if)# service-policy input <i>policy_map_name</i>	Attaches the policy map created in step 5 to the interface as an input service policy.

Configuration Example

This example shows how to configure a policy map to set the MPLS EXP field in the imposed label entries:

```
Router(config)# mls qos
Router(config)# access-list 1 permit any
Router(config)# class-map CUSTOMER-A
Router(config-cmap)# match access-group 1
Router(config)# policy-map set-MPLS-PHB
Router(config-pmap)# class CUSTOMER-A
Router(config-pmap-c)# police 50000000 conform-action set-mpls-exp-transmit 4
exceed-action drop
Router(config)# interface GE-WAN 3/1
Router(config-if)# no mls qos trust
Router(config)# interface GE-WAN 3/1.31
Router(config-if)# service-policy input set-MPLS-PHB
```

Configuring Ingress PE Router—P Facing Interface

This procedure classifies packets based on their MPLS EXP field and provides appropriate discard and scheduling treatments.


Note

QoS features shown here are available only with FlexWAN and Enhanced FlexWAN modules.

To classify packets based on their MPLS EXP field and provide appropriate discard and scheduling treatments, perform this task:

	Command	Purpose
Step 1	Router(config)# mls qos	Enables PFC QoS globally.
Step 2	Router(config)# class-map <i>class_name</i>	Specifies the class map to which packets will be mapped (matched). Creates a traffic class.
Step 3	Router(config-c-map)# match mpls experimental <i>exp_list</i>	Specifies the MPLS EXP field values used as a match criteria against which packets are checked to determine if they belong to the class.
Step 4	Router(config)# policy-map <i>name</i>	Configures the QoS policy for packets that match the class or classes.
Step 5	Router(config-p-map)# class <i>class_name</i>	Associates the traffic class with the service policy.
Step 6	Router(config-p-map-c)# bandwidth { <i>bandwidth_kbps</i> percent <i>percent</i> }	Specifies the minimum bandwidth guarantee to a traffic class. You can specify the minimum bandwidth guarantee in kilobits per second or by percent of the overall bandwidth.
Step 7	Router(config-p-map)# class class-default	Specifies the default class so that you can configure or modify its policy.
Step 8	Router(config-p-map-c)# random-detect	Enables a WRED drop policy for a traffic class that has a bandwidth guarantee.
Step 9	Router(config)# interface <i>type slot/port</i>	Selects an interface to configure.
Step 10	Router(config-if)# service-policy output <i>name</i>	Attaches a QoS policy to an interface and specifies that policies should be applied on packets leaving the interface.


Note

The **bandwidth** command and **random-detect** command are not supported on LAN ports.

Configuration Example

This example shows how to classify packets based on their MPLS EXP field and provide appropriate discard and scheduling treatments:

```
Router(config)# mls qos
Router(config)# class-map MPLS-EXP-4
Router(config-c-map)# match mpls experimental 4
Router(config)# policy-map output-qos
Router(config-p-map)# class MPLS-EXP-4
Router(config-p-map-c)# bandwidth percent 40
Router(config-p-map)# class class-default
Router(config-p-map-c)# random-detect
```

```
Router(config)# interface pos 4/1
Router(config-if)# service-policy output output-qos
```

Configuring the P Router—Output Interface



Note QoS features shown here are available only with FlexWAN and Enhanced FlexWAN modules.

To classify packets based on their MPLS EXP field and provide appropriate discard and scheduling treatments, perform this task:

	Command	Purpose
Step 1	Router(config)# mls qos	Enables PFC QoS globally.
Step 2	Router(config)# class-map <i>class_name</i>	Specifies the class map to which packets will be mapped (matched). Creates a traffic class.
Step 3	Router(config-c-map)# match mpls experimental <i>exp_list</i>	Specifies the MPLS EXP field values used as a match criteria against which packets are checked to determine if they belong to the class.
Step 4	Router(config)# policy-map <i>name</i>	Configures the QoS policy for packets that match the class or classes.
Step 5	Router(config-p-map)# class <i>class_name</i>	Associates the traffic class with the service policy.
Step 6	Router(config-p-map-c)# bandwidth { <i>bandwidth_kbps</i> percent <i>percent</i> }	Specifies the minimum bandwidth guarantee to a traffic class. You can specify the minimum bandwidth guarantee in kilobits per second or by percent of the overall bandwidth.
Step 7	Router(config-p-map)# class class-default	Specifies the default class so that you can configure or modify its policy.
Step 8	Router(config-p-map-c)# random-detect	Applies WRED to the policy based on the IP precedence or the MPLS EXP field value.
Step 9	Router(config)# interface <i>type slot/port</i>	Selects an interface to configure.
Step 10	Router(config-if)# service-policy output <i>name</i>	Attaches a QoS policy to an interface and specifies that policies should be applied on packets leaving the interface.



Note The **bandwidth** command and **random-detect** command are not supported on LAN ports.

Configuration Example

This example shows how to classify packets based on their MPLS EXP field and provide appropriate discard and scheduling treatments:

```
Router(config)# mls qos
Router(config)# class-map MPLS-EXP-4
Router(config-c-map)# match mpls experimental 4
Router(config)# policy-map output-qos
Router(config-p-map)# class MPLS-EXP-4
Router(config-p-map-c)# bandwidth percent 40
Router(config-p-map)# class class-default
```

```
Router(config-p-map-c)# random-detect
Router(config)# interface pos 2/1
Router(config-if)# service-policy output output-qos
```

Configuring the Egress PE Router—Customer Facing Interface



Note QoS features shown here are available only with FlexWAN and Enhanced FlexWAN modules.

To classify a packet based on its IP DSCP value and provide appropriate discard and scheduling treatments, perform this task:

	Command	Purpose
Step 1	Router(config)# mls qos	Enables PFC QoS globally.
Step 2	Router(config)# class-map <i>class_name</i>	Specifies the class map to which packets will be mapped (matched). Creates a traffic class.
Step 3	Router(config-c-map)# match ip dscp <i>dscp_values</i>	Uses the DSCP values as the match criteria.
Step 4	Router(config)# policy-map <i>name</i>	Configures the QoS policy for packets that match the class or classes.
Step 5	Router(config-p-map)# class <i>class_name</i>	Associates the traffic class with the service policy.
Step 6	Router(config-p-map-c)# bandwidth { <i>bandwidth_kbps</i> percent <i>percent</i> }	Specifies the minimum bandwidth guarantee to a traffic class. You can specify the minimum bandwidth guarantee in kilobits per second or by percent of the overall bandwidth.
Step 7	Router(config-p-map)# class class-default	Specifies the default class so that you can configure or modify its policy.
Step 8	Router(config-p-map-c)# random-detect dscp-based	Enables a WRED drop policy for a traffic class that has a bandwidth guarantee.
Step 9	Router(config)# interface <i>type slot/port</i>	Selects an interface to configure.
Step 10	Router(config-if)# service-policy output <i>name</i>	Attaches a QoS policy to an interface and specifies that policies should be applied on packets leaving the interface.



Note The **bandwidth** command and **random-detect** command are not supported on LAN ports.

Configuration Example

This example shows how to classify a packet based on its IP DSCP value and provide appropriate discard and scheduling treatments:

```
Router(config)# mls qos
Router(config)# class-map IP-PREC-4
Router(config-c-map)# match ip precedence 4
Router(config)# policy-map output-qos
Router(config-p-map)# class IP-PREC-4
Router(config-p-map-c)# bandwidth percent 40
Router(config-p-map)# class class-default
Router(config-p-map-c)# random-detect
```

```
Router(config)# interface GE-WAN 3/2.32
Router(config-if)# service-policy output output-qos
```

Configuring Uniform Mode

This section describes how to configure the following:

- [Configuring the Ingress PE Router—Customer Facing Interface](#), page 38-39
- [Configuring the Ingress PE Router—P Facing Interface](#), page 38-40
- [Configuring the Egress PE Router—Customer Facing Interface](#), page 38-41



Note

The steps that follow show one way, but not the only way, to configure the Uniform mode.

Configuring the Ingress PE Router—Customer Facing Interface

For Uniform mode, setting the trust state to IP precedence or IP DSCP allows the PFC to copy the IP PHB into the MPLS PHB.



Note

This description applies to PFC QoS for LAN ports. For information about FlexWAN and Enhanced FlexWAN QoS, see the *FlexWAN and Enhanced FlexWAN Modules Installation and Configuration Guide* at this URL:

<http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/cfgnotes/flexport/combo/index.htm>.

To configure a policy map to set the MPLS EXP field in imposed label entries, perform this task:

	Command	Purpose
Step 1	Router(config)# mls qos	Enables PFC QoS globally.
Step 2	Router(config)# access-list <i>ipv4_acl_number_or_name</i> permit any	Creates an IPv4 access list.
Step 3	Router(config)# class-map <i>class_name</i>	Creates a class map.
Step 4	Router(config-cmap)# match access-group <i>ipv4_acl_number_or_name</i>	Configures the class map to filter with the ACL created in Step 2.
Step 5	Router(config)# policy-map <i>policy_map_name</i>	Creates a named QoS policy.
Step 6	Router(config-pmap)# class <i>class_name</i>	Configures the policy to use the class map created in step 3.
Step 7	Router(config-pmap-c)# police <i>bits_per_second</i> <i>[normal_burst_bytes]</i> conform-action transmit exceed-action drop	Configures policing, including the following: <ul style="list-style-type: none"> • Action to take on packets that conform to the rate limit specified in the SLA. • Action to take on packets that exceed the rate limit specified in the SLA.
Step 8	Router(config)# interface <i>type slot/port</i>	Selects an interface to configure.

	Command	Purpose
Step 9	Router(config-if)# mls qos trust dscp	Configures received DSCP as the basis of the internal DSCP for all the port's ingress traffic.
Step 10	Router(config-if)# service-policy input <i>policy_map_name</i>	Attaches the policy map created in step 5 to the interface as an input service policy.

Configuration Example

This example shows how to configure a policy map to set the MPLS EXP field in imposed label entries:

```
Router(config)# mls qos
Router(config)# access-list 1 permit any
Router(config)# class-map CUSTOMER-A
Router(config-cmap)# match access-group 1
Router(config)# policy-map SLA-A
Router(config-pmap)# class CUSTOMER-A
Router(config-pmap-c)# police 50000000 conform-action transmit exceed-action drop
Router(config)# interface GE-WAN 3/1
Router(config-if)# mls qos trust dscp
Router(config)# interface GE-WAN 3/1.31
Router(config-if)# service-policy input SLA-A
```

Configuring the Ingress PE Router—P Facing Interface

To classify packets based on their MPLS EXP field and provide appropriate discard and scheduling treatments, perform this task:

	Command	Purpose
Step 1	Router(config)# mls qos	Enables PFC QoS globally.
Step 2	Router(config)# class-map <i>class_name</i>	Specifies the class map to which packets will be mapped (matched). Creates a traffic class.
Step 3	Router(config-c-map)# match mpls experimental <i>exp_list</i>	Specifies the MPLS EXP field values used as a match criteria against which packets are checked to determine if they belong to the class.
Step 4	Router(config)# policy-map <i>name</i>	Configures the QoS policy for packets that match the class or classes.
Step 5	Router(config-p-map)# class <i>class_name</i>	Associates the traffic class with the service policy.
Step 6	Router(config-p-map-c)# bandwidth { <i>bandwidth_kbps</i> percent <i>percent</i> }	Specifies the minimum bandwidth guarantee to a traffic class. You can specify the minimum bandwidth guarantee in kilobits per second or by percent of the overall bandwidth.
Step 7	Router(config-p-map)# class class-default	Specifies the default class so that you can configure or modify its policy.
Step 8	Router(config-p-map-c)# random-detect	Enables a WRED drop policy for a traffic class that has a bandwidth guarantee.
Step 9	Router(config)# interface <i>type slot/port</i>	Selects an interface to configure.
Step 10	Router(config-if)# service-policy output <i>name</i>	Attaches a QoS policy to an interface and specifies that policies should be applied on packets leaving the interface.

**Note**

The **bandwidth** command and **random-detect** command are not supported on LAN ports.

Configuration Example

This example shows how to classify packets based on their MPLS EXP field and provide appropriate discard and scheduling treatments:

```
Router(config)# mls qos
Router(config)# class-map MPLS-EXP-3
Router(config-c-map)# match mpls experimental 3
Router(config)# policy-map output-qos
Router(config-p-map)# class MPLS-EXP-3
Router(config-p-map-c)# bandwidth percent 40
Router(config-p-map)# class class-default
Router(config-p-map-c)# random-detect
Router(config)# interface pos 4/1
Router(config-if)# service-policy output output-qos
```

Configuring the Egress PE Router—Customer Facing Interface

To configure the egress PE router at the customer-facing interface, perform this task:

	Command	Purpose
Step 1	Router(config)# mls qos	Enables PFC QoS globally.
Step 2	Router(config)# class-map <i>class_name</i>	Specifies the class map to which packets will be mapped (matched). Creates a traffic class.
Step 3	Router(config-c-map)# match ip precedence precedence-value	Identifies IP precedence values as match criteria.
Step 4	Router(config)# policy-map <i>name</i>	Configures the QoS policy for packets that match the class or classes.
Step 5	Router(config-p-map)# class <i>class_name</i>	Associates the traffic class with the service policy.
Step 6	Router(config-p-map-c)# bandwidth { <i>bandwidth_kbps</i> percent <i>percent</i> }	Specifies the minimum bandwidth guarantee to a traffic class. You can specify the minimum bandwidth guarantee in kilobits per second or by percent of the overall bandwidth.
Step 7	Router(config-p-map)# class class-default	Specifies the default class so that you can configure or modify its policy.
Step 8	Router(config-p-map-c)# random-detect	Applies WRED to the policy based on the IP precedence or the MPLS EXP field value.
Step 9	Router(config)# interface <i>type slot/port</i>	Selects an interface to configure.
Step 10	Router(config-if) mpls propagate-cos	Enables propagation of EXP value into the underlying IP DSCP at the MPLS domain exit LER egress port.
Step 11	Router(config-if)# service-policy output <i>name</i>	Attaches a QoS policy to an interface and specifies that policies should be applied on packets coming into the interface.

**Note**

The **bandwidth** command and **random-detect** command are not supported on LAN ports.

Configuration Example

This example shows how to configure the egress PE router at the customer-facing interface:

```
Router(config)# mls qos
Router(config)# class-map IP-PREC-4
Router(config-c-map)# match ip precedence 4
Router(config)# policy-map output-qos
Router(config-p-map)# class IP-PREC-4
Router(config-p-map-c)# bandwidth percent 40
Router(config-p-map)# class class-default
Router(config-p-map-c)# random-detect
Router(config)# interface GE-WAN 3/2.32
Router(config-if) mpls propagate-cos
Router(config-if)# service-policy output output-qos
```