Packet Marking for Priority Differentiation

This chapter describes how QoS packet marking enables differentiated traffic treatment by assigning priority values—such as IP precedence, DSCP, CoS, and MPLS EXP bits—to packets, ensuring consistent handling of traffic classes across interfaces and network domains.

Packet marking

Packet marking is a QoS traffic differentiation model that

- assigns a priority value to each packet to indicate its relative importance in the network
- embeds this priority value into header fields such as IP precedence, Differentiated Services Code Point (DSCP), Class of Service (CoS), or MPLS Experimental (EXP) bits, and
- enables consistent forwarding treatment and queuing decisions across interfaces and network domains.

You can use packet marking in input policy maps to set or modify the attributes for traffic belonging to a specific class. For example, you can change the CoS value in a class or set DSCP or IP precedence values for a specific type of traffic. These new values are then used to determine how the traffic should be treated.

Types of packet marking

QoS uses packet and frame markings at different layers of the network stack to identify traffic classes, assign priorities, and influence queuing or drop behavior.

The primary marking categories are organized by the protocol layer at which they operate.

Layer 3 QoS markings

- Differentiated Services Code Point (DSCP): a six-bit field that defines per-hop behavior for traffic classes.
- IP Precedence: a three-bit field in the IP header that represents eight levels of priority.

- MPLS Experimental (EXP) bits: a three-bit field in the MPLS header that conveys packet priority across MPLS networks.

Layer 2 QoS markings

- Class of Service (CoS): a three-bit field in the 802.1Q VLAN tag that specifies a priority level (0-7) for a Layer 2 Ethernet frame.
- Priority Code Point (PCP): a three-bit field in the 802.1Q VLAN tag that indicates frame priority at Layer 2.
- Drop Eligibility Indicator (DEI): a one-bit field in the 802.1Q VLAN tag that indicates frame drop precedence.

For more information on the different types of packet marking, refer to the *Types of packet classification* section in the *Classify Packets to Identify Specific Traffic* chapter.

ECN—a system-controlled marking mechanism

Explicit Congestion Notification (ECN) is not to be confused with QoS packet marking mechanisms such as DSCP, CoS, or MPLS EXP, because ECN does not classify or prioritize traffic. Instead of defining how packets are queued or forwarded, ECN signals network congestion between devices by using two bits in the IP header. Routers and switches set or clear these bits dynamically when congestion is detected, allowing end hosts to reduce transmission rates without dropping packets.

Unlike DSCP or CoS markings, which administrators configure through Modular QoS CLI (MQC) policies to define per-hop behavior and resource allocation, ECN is system-controlled and not user-configurable.

Packet marking commands

The table lists the packet marking commands available in Modular QoS CLI (MQC) and shows their applicability for ingress and egress traffic directions, supported value ranges, and conditional or unconditional usage.

Table 1: Packet marking commands for egress and ingress interfaces

QoS marking command	Range	Unconditional marking—applicable direction	Conditional marking—availability
set ip encapsulation	0-63	ingress	No
set discard-class	0-1	ingress	No
set dscp	0-63	ingress, egress	No
set mpls experimental topmost	0-7	ingress, egress	No
set precedence	0-7	ingress, egress	No
set qos-group	0-31	ingress	No
set cos	0-7	ingress, egress	No
set dei	0-1	ingress, egress	No

Default QoS marking behavior for VLAN and MPLS encapsulations

When a packet enters or leaves a router, additional encapsulations such as VLAN tags or MPLS labels may be added to the frame. To maintain consistent QoS behavior, the router applies default marking profiles that specify which CoS or EXP values are written into those encapsulations. These profiles define how unclassified or unmarked traffic is treated, allowing the device to maintain a predictable baseline for scheduling, shaping, and congestion management operations.

During initialization, the system automatically creates one ingress default QoS mapping profile and one egress default QoS mapping profile for each device. These mappings determine the default CoS and EXP field values for all tagged or labeled traffic when no explicit class-based policy overrides them.

Unconditional QoS packet marking

Unconditional QoS packet marking is a QoS traffic differentiation feature that

- overwrites the packet's existing marking with the value configured in the policy map
- operates independently of policer conformance state or the packet's current header markings, and
- applies through MQC set-actions (for example, setting DSCP, CoS, MPLS EXP, or qos-group) at the configured interface and direction.

Conditional QoS packet marking is a QoS traffic differentiation feature that

- modifies the packet's marking based on specific traffic conditions such as policer conformance results (for example, conform, exceed, or violate actions), and
- allows differentiated treatment of packets depending on whether they meet defined rate or threshold criteria.

QoS marking modes for MPLS traffic

QoS marking modes for MPLS traffic is a QoS traffic differentiation feature for MPLS traffic that

- determines how the network preserves or rewrites packet priority markings as traffic moves between network domains
- applies to MPLS networks that carry IPv4 or IPv6 packets, defining how DSCP or Class of Service (CoS) values are mapped to or restored from MPLS Experimental (EXP) bits, and
- uses uniform mode to preserve ingress markings across domains and pipe mode to apply domain-specific QoS policies.

Table 2: Feature History Table

Feature Name	Release Information	Feature Description
Packet Marking for IPv4 and IPv6 Traffic	Release 26.3.1	Introduced in this release on: Fixed Systems (8700 [ASIC: K100])(select variants only*) *This feature is supported on Cisco 8711-28H8F-M routers.

Feature Name	Release Information	Feature Description
Packet Marking for IPv4 and IPv6 Traffic	Release 26.3.1	Introduced in this release on: Modular Systems (8800 [LC ASIC: K100])(select variants only*) *This feature is supported on Cisco 88-LC1-16H16F-EM line cards.
Packet Marking for IPv4 and IPv6 Traffic	Release 26.1.1	Introduced in this release on: Centralized Systems (8400 [ASIC: K100]) (select variants only*) *This feature is now supported on the Cisco 8404-SYS-D routers.
Packet Marking for IPv4 and IPv6 Traffic	Release 25.4.1	Introduced in this release on: Fixed Systems (8700 [ASIC: K100], 8010 [ASIC: A100])(select variants only*) *This feature is supported on: • 8711-48Z-M • 8011-32Y8L2H2FH • 8011-12G12X4Y-A/D
Packet Marking for IPv4 and IPv6 Traffic	Release 25.1.1	Introduced in this release on: Fixed Systems (8010 [ASIC: A100])(select variants only*) *This feature is supported on Cisco 8011-4G24Y4H-I routers.
Packet Marking for IPv4 and IPv6 Traffic	Release 24.4.1	Introduced in this release on: Fixed Systems (8700) (select variants only*) You can use uniform or pipe modes to implement QoS for IPv4 and IPv6 traffic. *This functionality is now extended to the Cisco 8712-MOD-M routers.

Feature Name	Release Information	Feature Description
Packet Marking for IPv4 and IPv6 Traffic	Release 24.3.1	Introduced in this release on: Modular Systems (8800 [LC ASIC: P100]) (select variants only*), Fixed Systems (8200) (select variants only*), Fixed Systems (8700 (P100, K100)) (select variants only*) You can use uniform or pipe modes to implement QoS for IPv4 and IPv6 traffic. *This feature is supported on: • 88-LC1-12TH24FH-E • 88-LC1-52Y8H-EM • 8212-48FH-M • 8711-32FH-M
Packet Marking for IPv4 and IPv6 Traffic	Release 24.2.11	Introduced in this release on: Modular Systems (8800 [LC ASIC: P100])(select variants only*) Using uniform or pipe modes, you can implement QoS for IPv4 and IPv6 traffic. Uniform mode maintains DSCP marking for packets across different network segments and is useful where the network policy requires consistent treatment of packets across multiple domains. Pipe mode separates QoS policies between network segments. In this mode, ingress DSCP markings classify and queue the packets, but the packets can remarked before they egress. Such treatment is beneficial when you need to apply one set of QoS policies within your network and a different set when packets exit the network towards your customer. *This feature is supported on 88-LC1-36EH.

MPLS QoS marking modes

You can apply QoS marking on IPv4 and IPv6 packets that traverse an MPLS network using uniform or pipe modes.

Uniform mode: It's a DiffServ-aware MPLS marking mode that preserves the incoming IP header's DSCP or CoS values throughout the MPLS domain. When packets are label-imposed and later disposed, the same DSCP values are copied into and out of the MPLS EXP field. This approach ensures consistent, end-to-end QoS treatment across provider and customer networks, making it suitable where network domains share a common QoS policy.

Pipe mode: It's a DiffServ-aware MPLS marking mode that isolates QoS policies between domains. In this mode, the MPLS domain applies its own EXP-based treatment that may differ from the IP DSCP values

received at ingress. The original IP markings are restored (or re-applied) when packets egress, enabling independent QoS control within the MPLS provider network.

This table shows the details for uniform and pipe modes.

Table 3: Differences between uniform mode and pipe mode

Uniform mode	Pipe mode
Preserves ingress DSCP or CoS markings across the MPLS domain.	Applies new MPLS EXP markings based on provider QoS policy.
Provides consistent end-to-end QoS treatment across interconnected network domains.	Enables independent QoS enforcement within the MPLS provider network.
DSCP values are copied into and out of MPLS EXP fields during label imposition and disposition.	DSCP values are used only at ingress for classification; packets may be remarked at egress.
Suitable when customer and provider networks share a common QoS model.	Suitable when customer and provider networks maintain distinct QoS models to enable policy separation and administrative autonomy.

QoS marking for IP-to-MPLS traffic

QoS marking for IP-to-MPLS traffic is a QoS traffic differentiation feature that

- transfers the DSCP value into the MPLS experimental (EXP) field when IP packets are encapsulated into MPLS
- maintains end-to-end service differentiation across the IP and MPLS domains by aligning per-hop behaviors between IP and label-switched segments, and
- enables consistent QoS treatment for customer traffic traversing MPLS networks through DSCP-to-EXP mapping configured in QoS policies.

This feature ensures that traffic classified at the IP layer retains its intended QoS behavior as it transits an MPLS-enabled core, preserving prioritization and congestion-handling characteristics across heterogeneous domains.

Table 4: Feature History Table

Feature Name	Release Information	Feature Description
Mark IP DSCP and MPLS EXP Values for IP to MPLS Traffic	Release 7.5.4	We've provided you with more granular control for IP to MPLS traffic, so you can collect billing information for your customers upstream at the MPLS core and correlate them with subsequent next-hop IP nodes. This helps you accurately bill your customers as they pay for specific services based on their network requirements. Such control is possible because we've enabled the remarking of IP DSCP values in the inner IP header—that remain even after the POP tag removes the outer header—along with the existing ability to remark MPLS EXP values on the outer MPLS header. There's no action required for you to enable this functionality, and there are no changes to command options.

QoS behavior for DSCP and EXP marking in IP-to-MPLS encapsulation

In earlier software releases, remarking the DSCP value in an ingress QoS policy for IP-to-MPLS traffic resulted in incomplete propagation of the marked value.

- The inner IP header retained its original DSCP value, preventing the intended QoS action from being applied across the network.
- The outer MPLS header, however, received the remarked value through the EXP bits that reflected the QoS policy action.

Starting from Cisco IOS XR Release 7.5.4, the QoS marking behavior for IP packets transiting an MPLS core has been enhanced.

- During MPLS imposition, the inner IP header now receives the remarked DSCP value from the ingress QoS policy, ensuring that the IP packet carries consistent QoS intent across the network.
- The top MPLS label continues to receive the remarked EXP value, derived from the three most significant bits of the DSCP field.

Benefits of QoS marking for IP-to-MPLS traffic

The ability to remark IP DSCP and MPLS EXP values at the ingress provides:

- Granular QoS control across multiple hops, ensuring consistent per-hop behavior and prioritization across both IP and MPLS domains.
- Improved service visibility, enabling correlation between traffic treatment in the IP edge and forwarding performance in the MPLS core.
- Enhanced operational efficiency, allowing service providers to collect and align customer-specific billing or usage data with the QoS policies applied at different network layers.

Limitations for configuring QoS marking for IP-to-MPLS traffic

- This feature is supported only on Cisco Silicon One Q200–based ASICs, available in both fixed and distributed systems.
- In distributed systems, you can use a Cisco Silicon One Q100–based ASIC line card for ingress classification; however, the egress line card must be equipped with a Q200 ASIC.

Configure QoS marking for IP-to-MPLS encapsulated traffic

Before you begin

Complete these prerequisites before you begin:

- Ensure MPLS forwarding and label imposition are enabled on the PE router interfaces.
- Verify that class maps and policy maps required for ingress DSCP remarking and egress classification are defined in your configuration plan.
- Confirm that the platform uses Cisco Silicon One Q200–based ASICs for egress functionality.

Procedure

Step 1 Create an ingress class map and policy map to remark DSCP values for IP packets before MPLS encapsulation.

This configuration sets the DSCP value to AF41 for traffic originally marked as AF31 to define a higher assured forwarding PHB.

Example:

```
Router(config)#class-map AF31
Router(config-cmap)#match dscp AF31
Router(config-cmap)#end-class-map
Router(config)#
Router(config)#policy-map INGRESS_REMARK
Router(config-pmap)#class AF31
Router(config-pmap-c)#set dscp AF41
Router(config-pmap-c)#end-policy-map
Router(config)#
Router(config)#interface FourHundredGigE0/0/0/0
Router(config-if)#service-policy input INGRESS_REMARK
Router(config-if)#commit
```

Step 2 Create an egress class map and policy map to classify packets based on remarked DSCP values.

This configuration classifies incoming traffic as AF31 or AF41 and maps it to the appropriate traffic-class values for forwarding decisions.

Example:

```
Router(config)#class-map AF31
Router(config-cmap)#match dscp AF31
Router(config-cmap)#end-class-map
Router(config)#
Router(config)#class-map AF41
Router(config-cmap)#match dscp AF41
Router#end-class-map
Router(config)#
Router(config)#policy-map INGRESS_CLASSIFY
Router(config-pmap)#class AF31
Router(config-pmap-c)#set traffic-class 3
Router(config-pmap-c)#exit
Router(config-pmap)#
Router(config-pmap)#class AF41
Router(config-pmap-c)#set traffic-class 4
Router(config-pmap-c)#exit
Router(config-pmap)#end-policy-map
Router(config)#
Router(config)#int FourHundredGigE0/0/0/1
Router(config-if)#service-policy input INGRESS_CLASSIFY
Router(config-if)#commit
```

Step 3 Verify DSCP remarking and classification at the egress PE router.

Use the `show policy-map interface` command to verify that traffic marked as AF41 at ingress is now being classified and counted correctly at egress.

Example:

```
Router#show policy-map interface FourHundredGigE0/0/0/1 input

FourHundredGigE0/0/0/1 input: INGRESS_CLASSIFY

Class AF31
  Classification statistics          (packets/bytes)     (rate - kbps)
    Matched             :                  0/0                   0
    Transmitted         :                  0/0                   0
    Total Dropped       :                  0/0                   0
Class AF41
  Classification statistics          (packets/bytes)     (rate - kbps)
    Matched             :           9813350/13738690000          936847
    Transmitted         :           9813350/13738690000          936847
    Total Dropped       :                  0/0                   0
Class class-default
  Classification statistics          (packets/bytes)     (rate - kbps)
    Matched             :                  0/0                   0
    Transmitted         :                  0/0                   0
    Total Dropped       :                  0/0                   0
```

The nonzero counters for Class AF41 confirm that the ingress DSCP remarking has been applied successfully and is recognized at the egress PE router.

QoS marking in tunneling and encapsulation scenarios

This topic introduces how QoS markings are preserved, mapped, or redefined when packets undergo encapsulation across GRE, MPLS, or Segment Routing tunnels.

QoS marking on GRE tunnels

QoS marking on Generic Routing Encapsulation (GRE) tunnels is a QoS traffic differentiation feature that

- preserves or maps DSCP and Type of Service (ToS) values between inner and outer IP headers when packets are encapsulated or decapsulated
- ensures consistent QoS treatment for tunneled traffic by maintaining class-of-service information across GRE boundaries, and
- coordinates with other encapsulation types, such as MPLS, to copy or derive appropriate QoS field values when MPLS labels coexist with GRE headers.

Generic Routing Encapsulation (GRE)

GRE is an IP tunneling protocol that encapsulates a wide variety of network layer packets inside IP tunnels. It allows one network to transport packets across another network by adding an outer IP header. GRE is commonly used to create logical point-to-point links between routers, enabling the transport of traffic types that are not natively routable across intermediate networks.

For more information on GRE tunnels, refer to the *Interfaces Configuration Guide for Cisco 8000 Series Routers*.

Type of Service (ToS)

ToS is an eight-bit field in the IPv4 header that specifies how an IP packet should be handled during transmission. The ToS field includes bits for DSCP and Explicit Congestion Notification (ECN), which together determine packet priority and congestion handling.

Table 5: Feature History Table

Feature Name	Release Information	Feature Description
QoS Behavior for Generic Routing Encapsulation (GRE) Tunnels: Default Marking	Release 26.3.1	Introduced in this release on: Fixed Systems (8700 [ASIC: K100])(select variants only*) *This feature is supported on Cisco 8711-28H8F-M routers.
QoS Behavior for Generic Routing Encapsulation (GRE) Tunnels: Default Marking	Release 26.3.1	Introduced in this release on: Modular Systems (8800 [LC ASIC: K100])(select variants only*) *This feature is supported on Cisco 88-LC1-16H16F-EM line cards.

Feature Name	Release Information	Feature Description
QoS Behavior for Generic Routing Encapsulation (GRE) Tunnels: Default Marking	Release 25.4.1	Introduced in this release on: Fixed Systems (8010 [ASIC: A100])(select variants only*) *This feature is supported on: • 8011-32Y8L2H2FH • 8011-12G12X4Y-A/D
QoS Behavior for Generic Routing Encapsulation (GRE) Tunnels: Default Marking	Release 25.1.1	Introduced in this release on: Fixed Systems (8700 [ASIC: K100], 8010 [ASIC: A100])(select variants only*) *This feature is supported on: • 8712-MOD-M • 8011-4G24Y4H-I
QoS Behavior for Generic Routing Encapsulation (GRE) Tunnels: Default Marking	Release 24.4.1	Introduced in this release on: Fixed Systems (8200 [ASIC: P100], 8700 [ASIC: P100])(select variants only*); Modular Systems (8800 [LC ASIC: P100])(select variants only*) *This feature is now supported on: • 8212-48FH-M • 8711-32FH-M • 88-LC1-36EH • 88-LC1-12TH24FH-E • 88-LC1-52Y8H-EM
QoS Behavior for Generic Routing Encapsulation (GRE) Tunnels: Default Marking	Release 7.3.1	With the support for GRE encapsulation and decapsulation tunnel interfaces, there are some important updates to QoS behavior for GRE tunnels. These updates are applicable for default packet marking and involve Type of Service (ToS) and MPLS experimental bits.

Guidelines for configuring QoS marking on GRE tunnels

GRE Encapsulation

During encapsulation of IPv4/IPv6 payload inside the GRE header, QoS behavior is as follows:

- Ingress: QoS supports classification on the payload Layer 3 fields or EXP and remarking payload IP header DSCP.
- Egress: QoS supports setting outer GRE IP header DSCP. It doesn't overwrite the Tunnel Type of Service (ToS) configuration and doesn't remark GRE IP header DCSP.

GRE Decapsulation

During decapsulation of the outer GRE header (in which the inner IPv4/IPv6/MPLS payload is forwarded to the next-hop router), QoS behavior is as follows:

- • Ingress: QoS supports classification on Layer 3 fields of outer GRE using the **set qos-group** command. Setting DSCP on the ingress interface sets DSCP for the inner headers.
  - Egress: QoS supports classification using **qos-group** to set DSCP or EXP for egress packets.

Explicit QoS marking for SRv6 encapsulation

Explicit QoS marking for SRv6 encapsulation is a QoS traffic differentiation feature that

- sets DSCP or Traffic Class values in the outer IPv6 header during SRv6 encapsulation, and
- ensures consistent QoS treatment across SRv6 transport paths by aligning encapsulated markings with class-based policy actions.

Explicit QoS marking feature is also known as packet marking.

Table 6: Feature History Table

Feature Name	Release Information	Feature Description
Set IP Marking for SRv6 Encapsulation	Release 26.3.1	Introduced in this release on: Fixed Systems (8700 [ASIC: K100])(select variants only*) *This feature is supported on Cisco 8711-28H8F-M routers.
Set IP Marking for SRv6 Encapsulation	Release 26.3.1	Introduced in this release on: Modular Systems (8800 [LC ASIC: K100])(select variants only*) *This feature is supported on Cisco 88-LC1-16H16F-EM line cards.
Set IP Marking for SRv6 Encapsulation	Release 26.1.1	Introduced in this release on: Centralized Systems (8400 [ASIC: K100]) (select variants only*) *This feature is now supported on the Cisco 8404-SYS-D routers.

Feature Name	Release Information	Feature Description
Set IP Marking for SRv6 Encapsulation	Release 25.4.1	Introduced in this release on: Fixed Systems (8010 [ASIC: A100])(select variants only*) *This feature is supported on: • 8011-32Y8L2H2FH • 8011-12G12X4Y-A/D
Set IP Marking for SRv6 Encapsulation	Release 25.1.1	Introduced in this release on: Fixed Systems (8010 [ASIC: A100])(select variants only*) *This feature is supported on Cisco 8011-4G24Y4H-I routers.
Set IP Marking for SRv6 Encapsulation	Release 24.4.1	Introduced in this release on: Fixed Systems (8200 [ASIC: P100], 8700 [ASIC: P100, K100])(select variants only*); Modular Systems (8800 [LC ASIC: P100])(select variants only*) *This feature is now supported on: • 8212-48FH-M • 8711-32FH-M • 8712-MOD-M • 88-LC1-36EH • 88-LC1-12TH24FH-E • 88-LC1-52Y8H-EM
Set IP Marking for SRv6 Encapsulation	Release 24.2.11	With this feature support for IP marking for SRv6 packets that are encapsulated, there are some important updates to the QoS behavior. This is an explicit packet marking feature that applies only to ingress QoS policies. **CLI:** This feature introduces the **set ip encapsulation** command.

Limitations for configuring explicit QoS marking for SRv6 encapsulation

Configuration constraints

- The explicit packet marking feature is supported only on ingress QoS policies.
- The **set ip encapsulation class-of-service** command is supported only in ingress QoS policies.
- The **set qos-group** configuration cannot be used together with the **set ip encapsulation class-of-service** command.

- The **set ip encapsulation class-of-service** and **set mpls experimental** commands are mutually exclusive and cannot coexist in the same policy configuration.

QoS marking mode conditions

- The encapsulation marking behavior applies exclusively in pipe mode.
- In uniform mode or propagate mode, the CoS value from the inner header is automatically copied to the outer header, regardless of the QoS policy encapsulation settings.

Default QoS marking for VXLAN encapsulation

Default QoS marking for VXLAN encapsulation is a QoS traffic differentiation feature that

- assigns a DSCP value of 0 (Class Selector 0) to the outer IP header when a Provider Edge (PE) device encapsulates IP traffic into a VXLAN tunnel,
- ensures VXLAN transport packets are treated with best-effort service across the underlay network.

VXLAN (Virtual eXtensible LAN) tunnels encapsulate Layer 2 Ethernet frames in UDP/IP packets. When the PE performs this encapsulation, the system must decide what value to place in the outer IP header's DSCP field, which determines per-hop QoS treatment for the VXLAN packet itself.

The default behavior is to clear or reset that field to DSCP 0 (Class Selector 0, best effort).

Table 7: Feature History Table

Feature Name	Release Information	Feature Description
Set VXLAN Outer IP Header DSCP Value to 0	Release 26.3.1	Introduced in this release on: Fixed Systems (8700 [ASIC: K100])(select variants only*) *This feature is supported on Cisco 8711-28H8F-M routers.
Set VXLAN Outer IP Header DSCP Value to 0	Release 26.3.1	Introduced in this release on: Modular Systems (8800 [LC ASIC: K100])(select variants only*) *This feature is supported on Cisco 88-LC1-16H16F-EM line cards.

Feature Name	Release Information	Feature Description
Set VXLAN Outer IP Header DSCP Value to 0	Release 24.4.1	Introduced in this release on: Fixed Systems (8200 [ASIC: P100], 8700 [ASIC: P100, K100])(select variants only*); Modular Systems (8800 [LC ASIC: P100])(select variants only*) *This feature is now supported on: • 8212-48FH-M • 8711-32FH-M • 8712-MOD-M • 88-LC1-36EH • 88-LC1-12TH24FH-E • 88-LC1-52Y8H-EM
Set VXLAN Outer IP Header DSCP Value to 0	Release 24.2.11	When a PE device transports IP traffic over a VXLAN tunnel that originates on the device, it automatically sets the DSCP value in the VXLAN outer IP header to 0 (CS0).

QoS marking on Layer 2 subinterfaces

QoS marking on Layer 2 subinterfaces is a QoS traffic differentiation feature that

- enables per-subinterface traffic classification and marking on Layer 2 transport interfaces
- applies CoS-based marking directly on Layer 2 frames
- supports marking of Layer 2 Ethernet packets in the ingress and egress directions, and
- ensures independent QoS policy enforcement for each subinterface within a physical port or bundle.

Table 8: Feature History Table

Feature Name	Release Information	Feature Description
Classification and Marking for L2 Traffic	Release 26.3.1	Introduced in this release on: Fixed Systems (8700 [ASIC: K100])(select variants only*) *This feature is supported on Cisco 8711-28H8F-M routers.
Classification and Marking for L2 Traffic	Release 26.3.1	Introduced in this release on: Modular Systems (8800 [LC ASIC: K100])(select variants only*) *This feature is supported on Cisco 88-LC1-16H16F-EM line cards.

Feature Name	Release Information	Feature Description
Classification and Marking for L2 Traffic	Release 26.1.1	Introduced in this release on: Centralized Systems (8400 [ASIC: K100]) (select variants only*) *This feature is now supported on the Cisco 8404-SYS-D routers.
Classification and Marking for L2 Traffic	Release 25.4.1	Introduced in this release on: Fixed Systems (8010 [ASIC: A100])(select variants only*) *This feature is supported on: • 8011-32Y8L2H2FH • 8011-12G12X4Y-A/D
Classification and Marking for L2 Traffic	Release 25.1.1	Introduced in this release on: Fixed Systems (8010 [ASIC: A100])(select variants only*) *This feature is supported on Cisco 8011-4G24Y4H-I routers.
Classification and Marking for L2 Traffic	Release 24.4.1	Introduced in this release on: Fixed Systems (8200 [ASIC: P100], 8700 [ASIC: P100, K100])(select variants only*); Modular Systems (8800 [LC ASIC: P100])(select variants only*) *This feature is now supported on: • 8212-48FH-M • 8711-32FH-M • 8712-MOD-M • 88-LC1-36EH • 88-LC1-12TH24FH-E • 88-LC1-52Y8H-EM
Classification and Marking for L2 Traffic	Release 7.7.1	You can now perform packet remarking on Layer 2 subinterfaces. Traffic marking allows you to fine tune the traffic attributes on your network. The increased granularity helps single out traffic that requires special handling, and achieves optimal application performance.

Configure QoS marking on Layer 2 subinterfaces

Before you begin

Complete these prerequisites before you begin:

- Enable Layer 2 service on the device or subinterface as needed. For configuration details, refer to the *L2VPN Configuration Guide*.

- Prepare the class maps and policy maps used for ingress classification and egress remarking. For more information, refer to the *Create a Traffic Class* section in the *Classify Packets to Identify Specific Traffic* chapter.

Follow these steps to configure QoS marking on Layer 2 subinterfaces.

Procedure

Step 1 Create an ingress policy to classify traffic and set internal `qos-group` values.

This policy assigns traffic classes and associates each class with a `traffic-class` and `qos-group` value for later egress remarking.

Example:

```
Router# configure terminal
Router(config)# policy-map INGRESS_L2_AC
Router(config-pmap)# class CONTROL_PLANE
Router(config-pmap-c)# set traffic-class 7
Router(config-pmap-c)# set qos-group 27
Router(config-pmap-c)# exit

Router(config-pmap)# class VOIP
Router(config-pmap-c)# set traffic-class 6
Router(config-pmap-c)# set qos-group 26
Router(config-pmap-c)# exit

Router(config-pmap)# class VIDEO_STREAM
Router(config-pmap-c)# set traffic-class 5
Router(config-pmap-c)# set qos-group 25
Router(config-pmap-c)# exit

Router(config-pmap)# class TRANSACTIONAL_DATA
Router(config-pmap-c)# set traffic-class 4
Router(config-pmap-c)# set qos-group 24
Router(config-pmap-c)# exit

Router(config-pmap)# class DB_SYNC
Router(config-pmap-c)# set traffic-class 3
Router(config-pmap-c)# set qos-group 23
Router(config-pmap-c)# exit

Router(config-pmap)# class BULK_DATA
Router(config-pmap-c)# set traffic-class 2
Router(config-pmap-c)# set qos-group 22
Router(config-pmap-c)# exit

Router(config-pmap)# class SCAVENGER
Router(config-pmap-c)# set traffic-class 1
Router(config-pmap-c)# set qos-group 21
Router(config-pmap-c)# exit

Router(config-pmap)# class class-default
Router(config-pmap-c)# end-policy-map
Router(config)# commit
```

Step 2 Create an egress policy to remark frames based on `qos-group` classification.

Map each `qos-group` to the desired Layer 2 CoS and DEI marking for egress.

Example:

```
Router# configure terminal
Router(config)# policy-map REMARK_EGRESS_QG_L2_AC
Router(config-pmap)# class QoS_GROUP_27
Router(config-pmap-c)# set cos 7
Router(config-pmap-c)# exit

Router(config-pmap)# class QoS_GROUP_26
Router(config-pmap-c)# set cos 7
Router(config-pmap-c)# exit

Router(config-pmap)# class QoS_GROUP_25
Router(config-pmap-c)# set cos 5
Router(config-pmap-c)# exit

Router(config-pmap)# class QoS_GROUP_24
Router(config-pmap-c)# set cos 5
Router(config-pmap-c)# exit

Router(config-pmap)# class QoS_GROUP_23
Router(config-pmap-c)# set cos 3
Router(config-pmap-c)# set dei 0
Router(config-pmap-c)# exit

Router(config-pmap)# class QoS_GROUP_22
Router(config-pmap-c)# set cos 3
Router(config-pmap-c)# set dei 1
Router(config-pmap-c)# exit

Router(config-pmap)# class QoS_GROUP_21
Router(config-pmap-c)# set cos 1
Router(config-pmap-c)# set dei 1
Router(config-pmap-c)# exit

Router(config-pmap)# class class-default
Router(config-pmap-c)# set dei 1
Router(config-pmap-c)# exit
Router(config)# commit
```

Step 3 Attach the egress policy to the Layer 2 subinterface.

Example:

```
Router(config)# interface Bundle-Ether1.104 l2transport
Router(config-if-l2)# service-policy output REMARK_EGRESS_QG_L2_AC
Router(config-if-l2)# commit
```

The egress remarking policy is now active on the specified Layer 2 subinterface.

Step 4 Verify egress remarking on the Layer 2 subinterface.

Confirm class counters and transmitted byte rates for each `qos-group` class on the subinterface.

Example:

```
Router# show policy-map interface Bundle-Ether 1.104 output

            Bundle-Ether1.104 output: REMARK_EGRESS_QG_L2_AC

            Class QoS_GROUP_7
            Classification statistics          (packets/bytes)     (rate - kbps)
            Matched             :            21319554/29847375600          985424
            Transmitted         :            21319554/29847375600          985424
```

```
Total Dropped       :                  0/0                   0
Class QoS_GROUP_6
Classification statistics          (packets/bytes)     (rate - kbps)
Matched             :           21581741/30214437400          997540
Transmitted         :           21581741/30214437400          997540
Total Dropped       :                  0/0                   0
Class QoS_GROUP_5
Classification statistics          (packets/bytes)     (packets/bytes)     (rate - kbps)

Matched             :          106597824/149236953600         4927114
Transmitted         :          106597824/149236953600         4927114
Total Dropped       :                  0/0                   0
Class QoS_GROUP_4
Classification statistics          (packets/bytes)     (rate - kbps)
Matched             :          490350115/686490161000         22664721
Transmitted         :          490350115/686490161000         22664721
Total Dropped       :                  0/0                   0
Class QoS_GROUP_3
Classification statistics          (packets/bytes)     (rate - kbps)
Matched             :                  0/0                   0
Transmitted         :                  0/0                   0
Total Dropped       :                  0/0                   0
Class QoS_GROUP_2
Classification statistics          (packets/bytes)     (rate - kbps)
Matched             :                  0/0                   0
Transmitted         :                  0/0                   0
Total Dropped       :                  0/0                   0
Class QoS_GROUP_1
Classification statistics          (packets/bytes)     (rate - kbps)
Matched             :                  0/0                   0
Transmitted         :                  0/0                   0
Total Dropped       :                  0/0                   0
Class class-default
Classification statistics          (packets/bytes)     (rate - kbps)
Matched             :         1087299229/1522218920600        50256530
Transmitted         :         1087299229/1522218920600        50256530
Total Dropped       :                  0/0                   0

Policy Bag Stats time: 1657531125148  [Local Time: 07/11/22 09:18:45.148]
```

Configure QoS marking on Layer 2 main interfaces

Before you begin

Complete these prerequisites before you begin:

- Enable Layer 2 service on the device or main interface as needed. For configuration details, refer to the *L2VPN Configuration Guide*.
- Prepare the class maps and policy maps used for ingress classification and egress remarking. For more information, refer to the *Create a Traffic Class* section in the *Classify Packets to Identify Specific Traffic* chapter.

Follow these steps to configure QoS marking on Layer 2 main interfaces.

Procedure

Step 1 Create an ingress policy to classify traffic and set internal `qos-group` values.

This policy assigns traffic classes and associates each class with a `traffic-class` and `qos-group` value for later egress remarking.

Example:

```
Router# configure terminal
Router(config)# policy-map INGRESS_L2_AC
Router(config-pmap)# class CONTROL_PLANE
Router(config-pmap-c)# set traffic-class 7
Router(config-pmap-c)# set qos-group 27
Router(config-pmap-c)# exit

Router(config-pmap)# class VOIP
Router(config-pmap-c)# set traffic-class 6
Router(config-pmap-c)# set qos-group 26
Router(config-pmap-c)# exit

Router(config-pmap)# class VIDEO_STREAM
Router(config-pmap-c)# set traffic-class 5
Router(config-pmap-c)# set qos-group 25
Router(config-pmap-c)# exit

Router(config-pmap)# class TRANSACTIONAL_DATA
Router(config-pmap-c)# set traffic-class 4
Router(config-pmap-c)# set qos-group 24
Router(config-pmap-c)# exit

Router(config-pmap)# class DB_SYNC
Router(config-pmap-c)# set traffic-class 3
Router(config-pmap-c)# set qos-group 23
Router(config-pmap-c)# exit

Router(config-pmap)# class BULK_DATA
Router(config-pmap-c)# set traffic-class 2
Router(config-pmap-c)# set qos-group 22
Router(config-pmap-c)# exit

Router(config-pmap)# class SCAVENGER
Router(config-pmap-c)# set traffic-class 1
Router(config-pmap-c)# set qos-group 21
Router(config-pmap-c)# exit

Router(config-pmap)# class class-default
Router(config-pmap-c)# end-policy-map
Router(config)# commit
```

Step 2 Create an egress policy to remark frames based on `qos-group` classification.

Map each `qos-group` to the desired Layer 2 CoS and DEI marking for egress.

Example:

```
Router# configure terminal
Router(config)# policy-map REMARK_EGRESS_QG_L2_AC
Router(config-pmap)# class QoS_GROUP_27
```

```
Router(config-pmap-c)# set cos 7
Router(config-pmap-c)# exit

Router(config-pmap)# class QoS_GROUP_26
Router(config-pmap-c)# set cos 7
Router(config-pmap-c)# exit

Router(config-pmap)# class QoS_GROUP_25
Router(config-pmap-c)# set cos 5
Router(config-pmap-c)# exit

Router(config-pmap)# class QoS_GROUP_24
Router(config-pmap-c)# set cos 5
Router(config-pmap-c)# exit

Router(config-pmap)# class QoS_GROUP_23
Router(config-pmap-c)# set cos 3
Router(config-pmap-c)# set dei 0
Router(config-pmap-c)# exit

Router(config-pmap)# class QoS_GROUP_22
Router(config-pmap-c)# set cos 3
Router(config-pmap-c)# set dei 1
Router(config-pmap-c)# exit

Router(config-pmap)# class QoS_GROUP_21
Router(config-pmap-c)# set cos 1
Router(config-pmap-c)# set dei 1
Router(config-pmap-c)# exit

Router(config-pmap)# class class-default
Router(config-pmap-c)# set dei 1
Router(config-pmap-c)# exit
Router(config)# commit
```

Step 3 Configure Layer 2 transport mode and attach the egress policy to the main interface.

Example:

```
Router(config)# interface HundredGigE0/0/0/23
Router(config-if)# l2transport
Router(config-if-l2)# service-policy output REMARK_EGRESS_QG_L2_AC
Router(config-if-l2)# no shutdown
Router(config-if-l2)# commit
```

The egress remarking policy is now active on the untagged Layer 2 main interface.

Step 4 Verify egress remarking on the Layer 2 main interface.

Confirm class counters and transmitted byte rates for each `qos-group` class on the main interface.

Example:

```
Router# show policy-map interface HundredGigE0/0/0/23 output

            HundredGigE0/0/0/23 output: REMARK_EGRESS_QG_L2_AC

            Class QoS_GROUP_7
            Classification statistics          (packets/bytes)     (rate - kbps)
            Matched             :            21319554/29847375600          985424
            Transmitted         :            21319554/29847375600          985424
            Total Dropped       :                   0/0                    0
            Class QoS_GROUP_6
            Classification statistics          (packets/bytes)     (rate - kbps)
            Matched             :            21581741/30214437400          997540
```

```
Transmitted         :            21581741/30214437400          997540
Total Dropped       :                   0/0                    0
Class QoS_GROUP_5
Classification statistics          (packets/bytes)     (packets/bytes)     (rate - kbps)

Matched             :          106597824/149236953600          4927114
Transmitted         :          106597824/149236953600          4927114
Total Dropped       :                   0/0                    0
Class QoS_GROUP_4
Classification statistics          (packets/bytes)     (rate - kbps)
Matched             :          490350115/686490161000          22664721
Transmitted         :          490350115/686490161000          22664721
Total Dropped       :                   0/0                    0
Class QoS_GROUP_3
Classification statistics          (packets/bytes)     (rate - kbps)
Matched             :                   0/0                    0
Transmitted         :                   0/0                    0
Total Dropped       :                   0/0                    0
Class QoS_GROUP_2
Classification statistics          (packets/bytes)     (rate - kbps)
Matched             :                   0/0                    0
Transmitted         :                   0/0                    0
Total Dropped       :                   0/0                    0
Class QoS_GROUP_1
Classification statistics          (packets/bytes)     (rate - kbps)
Matched             :                   0/0                    0
Transmitted         :                   0/0                    0
Total Dropped       :                   0/0                    0
Class class-default
Classification statistics          (packets/bytes)     (rate - kbps)
Matched             :         1087299229/1522218920600        50256530
Transmitted         :         1087299229/1522218920600        50256530
Total Dropped       :                   0/0                    0

Policy Bag Stats time: 1657531125148  [Local Time: 07/11/22 09:18:45.148]
```