Configuring Quality of Service

This chapter describes the Quality of Service and procedures to configure Quality of Service.

Introduction to Quality of Service

The Cisco Carrier Packet Transport (CPT) system is a Carrier Ethernet based crossponder solution used as an access or an aggregation device. To maximize the utility of network bandwidth, service providers can aggregate different types of traffic (voice, video, broadband data, and so on) and transmit them over the network. Because a single device supports a wide range of traffic (voice, video, broadband data, and so on), it is important to distinguish traffic from one another and provide differential services.

Quality of Service (QoS) refers to the ability of a network to provide improved services to selected network traffic over various underlying technologies including Ethernet and IEEE 802.1 networks, and MPLS networks.

The Cisco CPT system can be configured to provide different levels of treatment to different services. The different levels are defined through the service elements of bandwidth, including loss and delay. A service-level agreement (SLA) is a guaranteed level of these service elements. The CPT system supports flat and hierarchical QoS up to three levels.

You configure QoS throughout a network to provide an end-to-end QoS delivery. The following two components are necessary to deliver QoS across a heterogeneous network:

- QoS within a single network element, which includes queuing, scheduling, and traffic shaping features.
- QoS policing and management functions to control and administer end-to-end traffic across a network.

Advantages of QoS

Enabling QoS in the network has the following advantages:

- Control over resources—You can control resources like bandwidth that is being used.
- Tailored services—If you are a service provider, the control and visibility that QoS provides enable you to offer carefully tailored grades of service differentiation to your customers.
- Coexistence of mission-critical applications:
  - Your WAN is used efficiently by mission-critical applications that are most important to your business.
  - Bandwidth and minimum delays required by time-sensitive multimedia and voice applications are available.
  - Other applications using the link get their fair service without interfering with mission-critical traffic.

Understanding QoS

The QoS mechanism has three basic steps. It classifies types of traffic, specifies what action to take against a type of traffic, and specifies where the action should take place. The following sections explain how the CPT system accomplishes these steps.

Classification Mechanism for IP, Ethernet, and MPLS

For any QoS service to be applied to data, there must be a way to classify an IP packet or an Ethernet frame. When identified, a specific priority can be assigned to each individual IP packet or Ethernet frame. The IP Precedence field or the IP Differentiated Services Code Point (DSCP) field can be used to classify IP packets, and the Ethernet class of service (IEEE 802.1p defined class of service [CoS]) can be used for classifying Ethernet frames. IP precedence, IP DSCP, Ethernet CoS, and MPLS EXP are further described in the following sections.

IP Precedence

Use of IP precedence enables you to specify the class of service (CoS) for a packet using the three precedence bits in the type of service (ToS) field of the IP version 4 (IPv4) header. By default, each precedence corresponds to a name. These names, which continue to evolve, are defined in RFC 791.

Number	Name
0	routine
1	priority

Number	Name
2	immediate
3	flash
4	flash-override
5	critical
6	internet
7	networks

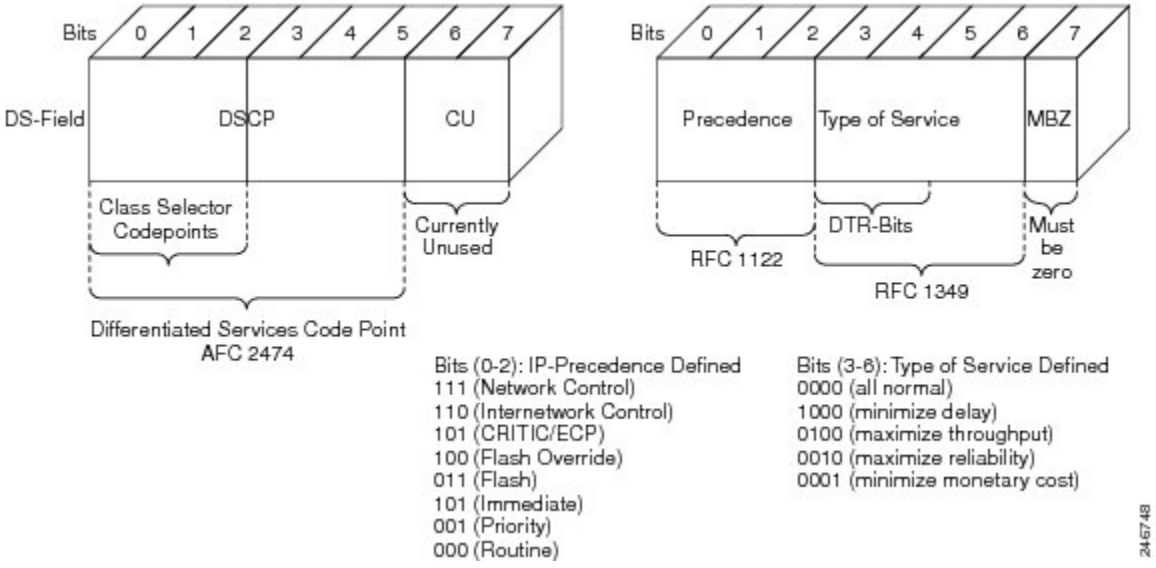
Note IP precedence bit settings 6 and 7 are reserved for network control information, such as routing updates.

IP Differentiated Services Code Point

IP DSCP uses the six bits in the IPv4 header to specify class of service for each IP packet (IETF RFC 2474). The DSCP field classifies packets into any of the 64 possible classes. On the network edge, the IP DSCP is assigned by the client device or the router, so that each subsequent network element can provide services based on the determined policy or the SLA.

IP Precedence and DSCP is illustrated in this figure.

Figure 1: IP Precedence and DSCP

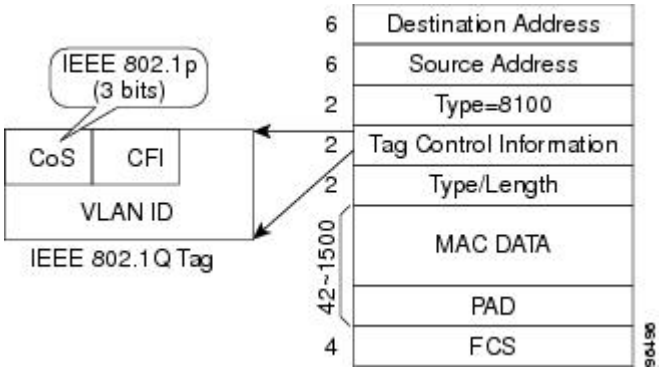


Ethernet CoS

The Ethernet CoS refers to the three bits within a four byte IEEE 802.1Q (VLAN) header used to indicate the priority of the Ethernet frame as it passes through a switched network. The CoS bits in the IEEE 802.1Q header are commonly referred to as the IEEE 802.1p bits. There are three CoS bits that provide eight classes,

matching the IP precedence number. In many real-world networks, a packet might traverse both Layer 2 and Layer 3 domains. To maintain QoS across the network, the IP ToS can be mapped to the Ethernet CoS and vice versa. For example, in a linear or one-to-one mapping where each mechanism supports eight classes. Similarly, a set of DSCP values (64 classes) can be mapped into each of the eight individual Ethernet CoS values. An IEEE 802.1Q Ethernet frame, which consists of a 2-byte Ethertype and a 2-byte tag (IEEE 802.1Q tag) on the Ethernet protocol header is shown in this figure.

Figure 2: Ethernet Frame and the CoS Bit (IEEE 802.1p)



Multiprotocol Label Switching Experimental

The Multiprotocol Label Switching (MPLS) Experimental (EXP) is a 3-bit field and part of the Multiprotocol Label Switching (MPLS) header. It was created by the IETF on an experimental basis, but later became part of the standard MPLS header. The EXP bits in the MPLS header carry the packet priority. Each label switch router (LSR) along the path honors the packet priority by queuing the packet into the proper queue and servicing the packet accordingly.

CPT System QoS

The CPT system QoS classifies each packet in the network based on its Ethernet CoS, IP precedence, IP DSCP, MPLS EXP bits, or VLAN ID. After they are classified into class flows, further QoS functions can be applied to each packet as it traverses the CPT system.

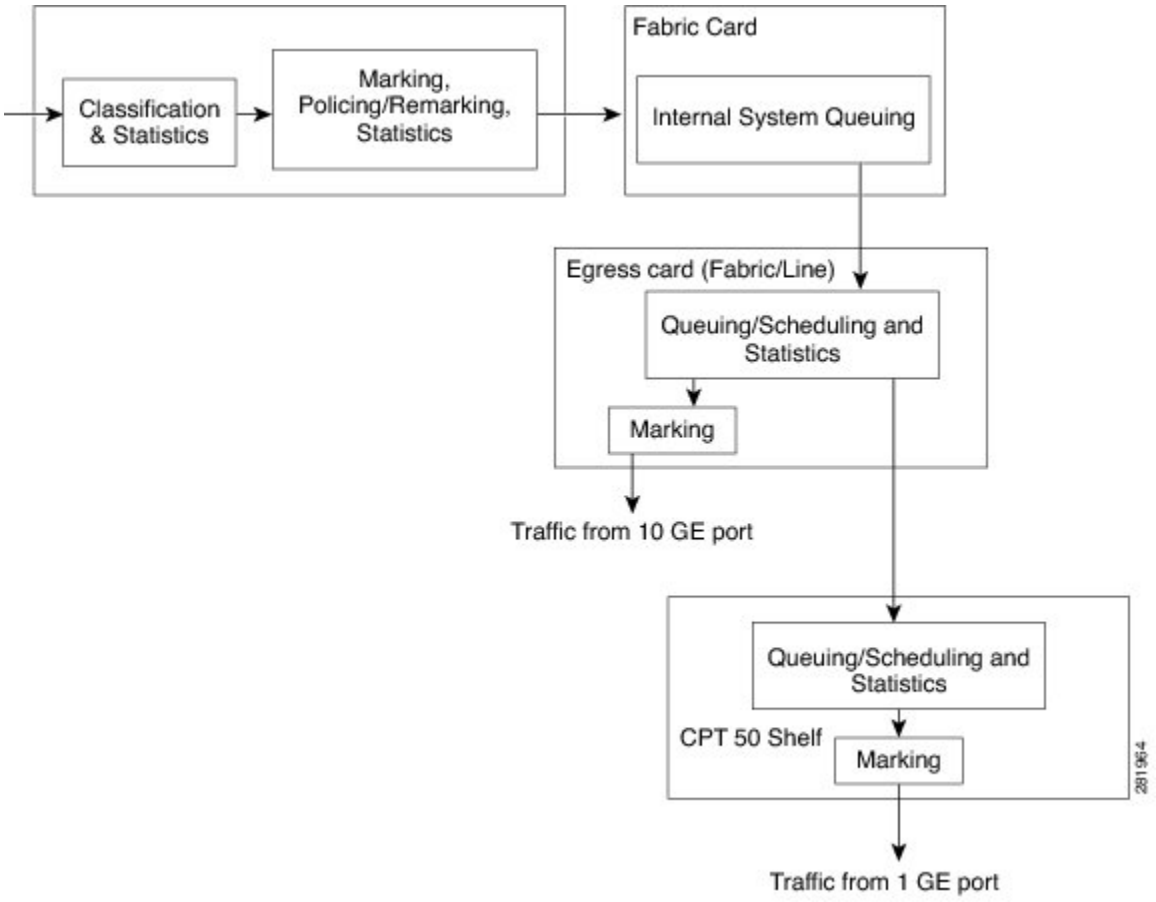
The policing feature of the CPT system ensures that the attached equipment does not submit more than a predefined amount of bandwidth (Rate Limiting) into the network. The policing feature can be used to enforce the committed information rate (CIR) and the peak information rate (PIR) available to a customer at an interface. The policing action is applied per classification.

The marking feature can set the Ethernet CoS, IP precedence, or IP DSCP bits when packets enter the CPT system. For MPLS traffic, marking sets the MPLS EXP bits when the packets leave the system. The marking feature operates on the outer IEEE 802.1p tag, IP precedence, or IP DSCP bits and provides a mechanism for tagging packets at the ingress; and on the MPLS EXP bits at the egress by using table-maps. The subsequent network elements can provide a QoS based only the QoS indicator that the service provider has created.

The per-class queuing allows various queuing applications to support SLA. For example, allocation of committed information rate, ensuring low latencies and rate limiting traffic to down stream nodes based on the configuration, and also enabling fair access to excess network bandwidth. The CPT system uses a combination of Strict Priority Queuing (SPQ) and Weighted Round Robin (WRR) scheduling process to

guarantee throughput and latency requirements and to provide fair access to excess bandwidth. The CPT system QoS flow is illustrated in this figure.

Figure 3: CPT System QoS flow



NTP-J62 Configuring QoS Features Using Cisco IOS Commands

Purpose	This procedure configures QoS features using IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Remote
Security Level	None

Note Users can create traffic policies and attach these policies to targets. A traffic policy contains a traffic class and one or more QoS features. A traffic class is used to classify traffic, while the QoS features in the traffic policy determine how to treat the classified traffic.

Procedure

Step 1 Define a traffic class using the **class-map** command:

a) To configure traffic classification at the ingress, see DLP-J190 Configuring Ingress Classification Using Cisco IOS Commands, on page 8.

b) To configure traffic classification at the egress, see DLP-J199 Configuring Egress Classification Using Cisco IOS Commands, on page 34.

Step 2 Create a traffic policy using the **policy-map** command to associate the traffic class with one or more QoS features (using the **policy-map** command):

a) To configure policing at the ingress, see DLP-J192 Configuring Ingress Policing Using Cisco IOS Commands, on page 14.

b) To configure marking at the ingress, see DLP-J197 Configuring Ingress Marking Using Cisco IOS Commands, on page 30.

c) To configure marking at the egress using table maps, see DLP-J207 Configuring Table Maps for Egress Marking Using Cisco IOS Commands, on page 37.

d) To associate table maps at the egress using table maps, see DLP-J200 Associating Table Maps at Egress Using Cisco IOS Commands, on page 40.

e) To configure shaping at the egress, see DLP-J203 Configuring Egress Shaping Using Cisco IOS Commands, on page 48.

f) To configure the egress bandwidth, see DLP-J202 Configuring Egress Bandwidth Using Cisco IOS Commands, on page 46.

g) To configure low-latency queuing (LLQ), see DLP-J201 Configuring Egress LLQ Using Cisco IOS Commands, on page 43.

h) To configure bandwidth remaining ratio (BRR) or bandwidth remaining percent (BRP), see DLP-J204 Configuring Egress Bandwidth Remaining Ratio or Bandwidth Remaining Percent Using Cisco IOS Commands, on page 51.

Step 3 Attach the traffic policy to the target using the **service-policy** command, see DLP-J195 Attaching or Removing a Traffic Policy from the Target Using Cisco IOS Commands, on page 25.

Step 4 Monitor and verify the QoS configuration. See DLP-J205 Monitoring and Verifying QoS Configuration Using Cisco IOS Commands, on page 53.

NTP-J63 Configuring QoS Features Using CTC

Purpose	This procedure configures QoS using CTC.
Tools/Equipment	None
Prerequisite Procedures	None

Required/As Needed	As needed
Onsite/Remote	Remote
Security Level	None

Procedure

Step 1 Create a class-map.
To create or edit a class-map, see DLP-J191 Creating or Editing a Class Map Using CTC, on page 11.

Step 2 Create a policy-map.
To create or edit a policy-map, see DLP-J193 Creating or Editing a Policy Map Using CTC, on page 21.

Step 3 Create a traffic policy by associating the traffic class with one or more QoS features. See DLP-J194 Setting Policy Class Actions Using CTC, on page 23.

Step 4 Attach the traffic policy to the target.
To attach or remove a traffic policy from the target, see DLP-J196 Attaching or Removing a Traffic Policy from the Target Using CTC, on page 28.

Step 5 Monitor and verify QoS configuration.
To monitor and verify QoS configuration, see DLP-J206 Monitoring and Verifying QoS Configuration Using CTC, on page 55

Ingress QoS Functions

Ingress QoS on the Cisco CPT system involves classification, marking, and policing. The ingress card classifies the packets and assigns a traffic-class to it. The traffic-class is used for internal queuing and congestion management, as well as classification at the egress. At ingress, policy application is supported on multiple targets, which are:

- Ten Gigabit Ethernet (10 GE) and one Gigabit Ethernet (1 GE) interface
- Port-channel interface
- Port-channel member interface
- Service instance on 10 GE and 1 GE interfaces
- Service instance on port-channel

Ingress Classification

Classifying network traffic enables you to organize traffic (that is, packets) into traffic classes or categories on the basis of whether the traffic matches specific criteria. Using the packet classification, you can partition network traffic into multiple priority levels or classes of service. Traffic is classified to determine whether it should be:

- Marked for further processing
- Policed to rate limit specific traffic types

The CPT system supports ingress classification. The default class, named class-default, is the class to which any traffic that does not match any of the selection criteria in the configured class maps, is directed.

Ingress Classification Restrictions and Usage Guidelines

- The **match** commands are used to specify various criteria for classifying packets. The packets are checked to determine whether they match the criteria specified in the **match** commands.
- The **match-any** keyword specifies that the traffic class must match one of the specified criteria. Traffic classification based on multiple QoS fields (Ethernet class of service [CoS], IP precedence, and so on) for a single packet is not supported. Traffic classification is based only on the first matching parameter (in the user-specified order) of the QoS fields, if multiple match criteria are specified in a single class.
- The **match-all** keyword is added to the **match** command and **match-all** is the default. This classification specifies that the traffic class must match all of the specified criteria within the class-map.
- The **match-all** cannot have more than two combinations of the classification criteria. However, the class-map can be created with more than two combinations of classification criteria. The policy with such class-map does not work and reports an error message indicating the failure. You should rectify the class-map with one classification criteria and try again.
- The match on**cos inner** or **vlan inner** is supported only in IOS mode

Configure ingress classification using Cisco IOS commands, see DLP-J190 Configuring Ingress Classification Using Cisco IOS Commands, on page 8.

To create or edit a class-map using CTC, see DLP-J191 Creating or Editing a Class Map Using CTC, on page 11.

DLP-J190 Configuring Ingress Classification Using Cisco IOS Commands

Purpose	This procedure creates a class map using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Remote
Security Level	None

Procedure

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: Router> enable	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**class-map [match-any]** | [**match-all**]*class-map-name* **Example:** Router(config)# class-map match-any class1	Creates a class to be used with a class map and enters the class-map configuration mode. The class map is used for matching packets to the specified class. • **match-any—** Specifies that one of the match criterion must be met. Use this keyword only if you have to specify more than one match command. • **match-all—** Specifies that the traffic class must match all of the specified criteria. • *class-map-name—* Class map name. This is the name of the class map and can have a maximum of 40 alphanumeric characters.
Step 4	**match cos** *cos-number* **Example:** Router(config-cmap)# match cos 2	Matches a packet on the basis of a Layer 2 CoS number. • *cos-number—* CoS value. The value can range from 0 to 7. **Note** The **match cos** command is just an example of one of the match commands that can be used. For a list of other match commands, see Table 1: Traffic Class Commands, on page 9
Step 5	end **Example:** Router(config-cmap)# exit	Exits class-map configuration mode and returns to privileged EXEC mode.

The following table provides the traffic class commands supported at the ingress:

Table 1: Traffic Class Commands

Command	Description
match cos *cos-number* **Example:** Router(config-cmap)# match cos 2	Matches a packet on the basis of a Layer 2 CoS number. • *cos-number—* CoS value. The value can range from 0 to 7.

Command	Description
match ip precedence *ip-precedence-value* **Example:** Router(config-cmap)# match ip precedence 5	Identifies the IP precedence value as match criteria. • *ip-precedence-value*— IP precedence value. The value can range from 0 to 7.
match ip dscp *ip- dscp-value* **Example:** Router(config-cmap)# match ip dscp 6	Identifies a specific IP DSCP value as a match criterion. • *ip- dscp-value* — IP DSCP value. The value can range from 0 to 63.
match mpls experimental topmost *exp-value* **Example:** Router(config-cmap)# match mpls experimental topmost 5	Matches the MPLS EXP value in the topmost label. • *exp-value* — MPLS EXP value. The value can range from 0 to 7.
match vlan [*vlanid*] **Example:** Router(config-cmap)# match vlan 100	Specifies a VLAN ID or range of VLAN IDs in a class-map to match packets. • *vlanid* —VLAN ID. The value can range from 0 to 4096.
match cos inner *cos-number* **Example:** Router(config-cmap)# match cos inner 3	Matches a double tag packet on the basis of a Layer 2 CoS number on inner vlan. • *cos-number* — CoS value. The value can range from 0 to 7.
match vlan inner [*vlanid*] **Example:** Router(config-cmap)# match vlan inner 200	Specifies a VLAN ID or range of VLAN IDs in a class-map to match packets inner vlan. • *vlanid* —VLAN ID. The value can range from 0 to 4096.

Examples: Ingress Classification

The following example shows how to configure a class-map named ipp5, and enter a match statement for IP precedence 5:

```
Router# enable
Router# configure terminal
Router(config)# class-map ipp5
Router(config-cmap)# match ip precedence 5
```

The following example shows how to configure a class-map on multiple match statements:

```
Router# enable
Router# configure terminal
Router(config)# class-map match-any IPP
```

```
Router(config-cmap)# match ip precedence 3
Router(config-cmap)# match ip precedence 4
```

The following example shows how to a configure a class-map using **match-all** and **match-any** keywords:

```
Router# enable
Router# configure terminal
Router(config)# class-map match-any class1
Router(config-cmap)# match vlan 100 200 400-500
Router(config-cmap)# match cos 1
Router(config-cmap)# exit
Router(config)# class-map match-all class2
Router(config-cmap)# match vlan 1000 1100-1120
Router(config-cmap)# match cos 3
Router(config-cmap)# exit
```

The match-all criteria with multiple VLANs and CoS marking gets translated to a combination of match criteria. Therefore matching is based on the following incoming packet:

```
VLAN 1000 AND COS 3
VLAN 1100-1200 AND COS 3
```

The match-any criteria gets translated to individual match criteria. Therefore matching is based on VLAN 100, VLAN 200, VLAN 400-500, or COS 1.

The following example shows a logical OR operation in a child policy with match cos and class-default in a parent class.

```
Router(config)# class-map match-any childOR
Router(config-cmap)# match cos 5
Router(config)# policy-map testchildOR
Router(config-pmap)# class childOR
Router(config-pmap-c)# police cir percent 10
Router(config)# policy-map parentOR
Router(config-pmap)# class class-default
Router(config-pmap-c)# police cir percent 20
Router(config-pmap-c)# service-policy testchildOR
```

This example shows how to display class-map information for a specific class map:

```
Router# show class-map ipp5

class Map match-any ipp5 (id 1)
match ip precedence 5
```

DLP-J191 Creating or Editing a Class Map Using CTC

Purpose	The following procedure creates or edits a class map using CTC.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Remote
Security Level	None

Procedure

Step 1 Complete the "NTP-J22 Log into CTC" procedure at a node where you want to create a class map.

Step 2 In the node view, right-click the Fabric or Line card and choose **Open Packet Transport System View**. The Packet Transport System View dialog box appears.

Step 3 Click the **Provisioning** tab.

Step 4 From the left pane, click the **QoS** tab.

Step 5 To create a class map, in the **Class Map** tab, click **Create Class Map**. In the Class Map Creation dialog box:

a) Enter the class map name in the Class-Map name field.

b) Choose **Match All** or **Match Any** option.

c) Select one of the following match attributes in the Match Attribute field:

- cos
- ip precedence
- ip dscp
- mpls experimental topmost
- vlan
- qos group

d) Enter the attribute value in the Attribute field based on the option that was selected in the Match Attribute field, see this table:

Table 2: Match Attribute and Attribute Value

Match Attribute	Attribute Value
cos	Value between 0-7
ip precedence	Value between 0-7
ip dscp	Value between 0-63
mpls experimental topmost	Value between 0-7
vlan	Value between 0-4096. For each vlan, you can have up to 30 entries.
qos group	Value between 0-7

e) Click **Add**.

f) Repeat Step 5.b to Step 5.d to add additional match criteria to the class map.

g) Click **Finish**.

Step 6 To edit the class map, in the **Class Map** tab, select the class map and click **Edit Class Map**. In the Class Map Creation dialog box:

a) Select the match attribute in the Match Attribute field to edit.

b) Change the attribute value in the Attribute field based on the option that was selected in the Match Attribute field (see Table 2: Match Attribute and Attribute Value, on page 12).
c) Click **Add**.
d) Repeat Step 6.b to Step 6.c to edit the remaining match attributes.
Note To remove the match attribute from the class map, select the match attribute and click **Remove**.

e) Click **Finish**.

Ingress Policing

Ingress policing ensures that an attached equipment does not submit more than a predefined amount of bandwidth (Rate Limiting) into the network. The policing feature can be used to enforce the committed information rate (CIR) and the peak information rate (PIR) available to a customer at an interface or a service instance on an interface. Policing enables to limit the data flow through the CPT system by dropping or marking down the QoS value according to the configuration.

The Cisco CPT system supports ingress policing. When policing is configured, traffic is placed in one of the following categories:

- Conform
- Exceed
- Violate

Within these three categories, users can decide the actions to be applied. For instance, packets that conform to the policy rate can be configured to be transmitted, packets that exceed the policy rate can be configured to be sent with a decreased priority, and packets that violate the policy rate can be configured to be dropped. If no actions are specified, the default conform-action is transmit, and default exceed-action or violate-action is drop.

The following table contains the list of policing actions supported at the ingress:

Table 3: Policing Actions

Action	Purpose
transmit	Transmits the packet.
drop	Drops the packet.
set-discard-class-transmit	Sets the discard-class internal label to a specified value and transmits the packet. This action is effective only when egress QoS marking of an MPLS or Virtual Private Wire Service (VPWS) traffic is achieved using table-maps.
set-cos-transmit	Sets the CoS value and transmits the packet.
set-dscp-transmit	Sets the IP DSCP value and transmit the packet.
set-precedence-transmit	Sets the IP precedence value and transmits the packet.

Action	Purpose
set-qos-transmit	Sets the QoS-group value and transmits the packet.

The policing features supported are:

- Individual actions
- Multiple actions
- Single rate, 2-color policer
- Single rate, 3-color policer
- Dual rate, 3-color policer
- Color blind mode
- Hierarchical policing (two levels)
- Micro-flow policing

Ingress Policing Restrictions and Usage Guidelines

The restrictions and usage guidelines to configure QoS ingress policing on a CPT system are as follows:

- In a hierarchical QoS policy, only a single-rate, 2-color policer is supported at the parent level. This should be configured using the **police [rate]** *bps-value* action command. The **police cir** command is not supported at the parent level.
- In a hierarchical QoS policy with policer configured at the parent level, only a single-rate, 2-color policer or a dual-rate, 3-color policer is supported at the child level.

To create a policy-map using Cisco IOS commands, see DLP-J192 Configuring Ingress Policing Using Cisco IOS Commands, on page 14.

To create or edit a policy-map using CTC, see DLP-J193 Creating or Editing a Policy Map Using CTC, on page 21.

To set policing actions using CTC, see DLP-J194 Setting Policy Class Actions Using CTC, on page 23.

To attach or remove a traffic policy from the interface using Cisco IOS commands, see DLP-J195 Attaching or Removing a Traffic Policy from the Target Using Cisco IOS Commands, on page 25.

To attach or remove a traffic policy from the interface using CTC, see DLP-J196 Attaching or Removing a Traffic Policy from the Target Using CTC, on page 28.

DLP-J192 Configuring Ingress Policing Using Cisco IOS Commands

Purpose	This procedure creates a policy map and sets policing actions using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	DLP-J190 Configuring Ingress Classification Using Cisco IOS Commands, on page 8

Required/As Needed	As needed
Onsite/Remote	Remote
Security Level	None

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**policy-map** *policy-map-name* **Example:** Router(config)# policy-map policy1	Creates or specifies the name of the traffic policy and enters the policy-map configuration mode. • *policy-map-name*—Policy map name. This is the name of the policy map and can have a maximum of 40 alphanumeric characters.
Step 4	**class** {*class-name* | **class-default**} **Example:** Router(config-pmap)# class class1	Specifies the name of a traffic class to which the policy applies and enters the policy-map class configuration mode. • Enter the previously configured class-map name. ◦ *class-name*—User-defined class name to which the policy applies. ◦ **class-default**—Specifies that the policy applies to the default traffic class. **Note** This step associates the traffic class with the traffic policy.
Step 5	**police [cir | rate]** *bps-value* **[bc | burst]** *bc* **[be | peak-burst]** *be* **conform-action** *action* **exceed-action** *action* **violate-action** *action* **Example:** Router(config-pmap-c)# police cir 5000000 bc 200000 be 400000 conform-action transmit	Specifies a maximum bandwidth usage by a traffic class through the use of a token bucket algorithm: • **cir**—Indicates that the committed information rate (CIR) is used for policing traffic. • **rate**—Indicates that the police rate is used for policing traffic. • *bps value*—Average rate in bits per second. The valid values range from 8000 to 10000000000.

	Command or Action	Purpose
	exceed-action set-dscp-transmit violate-action drop	• **bc—**Indicates that the committed (conform) burst size is used for policing traffic. • **burst—**Indicates that the burst size is used for policing traffic. • *bc—*Committed (conform) burst size or burst size in bytes. The valid values range from 1000 to 256000000. • **be—**Indicates that the excess burst size is used for policing traffic. • **peak-burst—**Indicates that the peak-burst size is used for policing traffic. • *be—*Excess burst size or peak-burst size in bytes. The valid values range from 1000 to 256000000. • *action—*Action taken on a packet when it conforms, exceeds, or violates the interface bandwidth. The possible actions are shown in Table 3: Policing Actions, on page 13. **Note** The **police [cir | rate]** *bps-value* **[bc | burst]** *bc* **[be | peak-burst]** *be* **conform-action** *action* **exceed-action** *action* **violate-action** *action* command is just an example of one of the policy commands that can be used. For a list of other policy commands, see Table 4: Traffic Policy Commands, on page 17.
Step 6	end **Example:** Router(config-pmap)# end	Exits policy-map configuration mode and returns to privileged EXEC mode.

The following table provides the traffic policy commands supported at the Ingress:

Table 4: Traffic Policy Commands

Command	Description
police [cir | rate] *bps-value* **[bc | burst]** *bc* **[be | peak-burst]** *be* **conform-action** *action* **exceed-action** *action* **violate-action** *action* **Example:** Router(config-pmap-c)# police cir 5000000 bc 200000 be 400000 conform-action transmit exceed-action set-dscp-transmit violate-action drop	Specifies a maximum bandwidth usage by a traffic class through the use of a token bucket algorithm: • **cir—**Indicates that the committed information rate (CIR) is used for policing traffic. • **rate—**Indicates that the police rate is used for policing traffic. • *bps value*—Average rate in bits per second. The valid values range from 8000 to 10000000000. • **bc—**Indicates that the committed (conform) burst size is used for policing traffic. • **burst—**Indicates that the burst size is used for policing traffic. • *bc*—Committed (conform) burst size or burst size in bytes. The valid values range from 1000 to 256000000. • **be—**Indicates that the excess burst size is used for policing traffic. • **peak-burst—**Indicates that the peak-burst size is used for policing traffic. • *be*—Excess burst size or peak-burst size in bytes. The valid values range from 1000 to 256000000. • *action*—Action taken on a packet when it conforms, exceeds, or violates the interface bandwidth. The possible actions are shown in Table 3: Policing Actions, on page 13.

Command	Description
police [cir | rate] percent *%* **[bc | burst]** *bc* **[be | peak-burst]** *be* **conform-action** *action* **exceed-action** *action* **violate-action** *action* **Example:** Router(config-pmap-c)# police cir percent 10 bc 200000 be 400000 conform-action transmit exceed-action set-dscp-transmit violate-action drop	Configures traffic policing on the basis of a percentage of bandwidth available on an interface, where: • **cir—**Indicates that the committed information rate (CIR) is used for policing traffic. • **rate—**Indicates that the police rate is used for policing traffic. • **percent—**Indicates that a percentage of bandwidth is used for calculating CIR or rate. • *%—* CIR or rate bandwidth percentage. The valid values range from 1 to 100. • **bc—**Indicates that the committed (conform) burst size is used for policing traffic. • **burst—**Indicates that the burst size is used for policing traffic. • *bc—*Committed (conform) burst size or burst size in mill-seconds or micro-seconds. • **be—**Indicates that the excess burst size is used for policing traffic. • **peak-burst—**Indicates that the peak-burst size is used for policing traffic. • *be—*Excess burst size or peak-burst size in mill-seconds or micro-seconds. • *action—*Action taken on a packet when it conforms, exceeds, or violates the interface bandwidth. The possible actions are shown in Table 3: Policing Actions, on page 13.

Command	Description
police [cir | rate] *bps-value* **[bc | burst]** *bc* **[pir | peak-rate]** *pir* **[be | peak-burst]** *be* **conform-action** *action* **exceed-action** *action* **violate-action** *action*	Configures traffic policing using two rates (CIR and PIR) where: • **cir—**Indicates that the committed information rate (CIR) is used for policing traffic. • **rate—**Indicates that the police rate is used for policing traffic. • *bps value***—**Average rate in bits per second. The valid values range from 8000 to 10000000000 • **bc—**Indicates that the committed (conform) burst size is used for policing traffic. • **burst—**Indicates that the burst size is used for policing traffic. • *bc***—**Committed (conform) burst size or burst size in bytes. The valid values range from 1000 to 256000000. • **pir—** Indicates that the peak information rate (PIR) is used for policing traffic. • **peak-rate—** Indicates that the peak rate is used for policing traffic. • *pir***—**Peak information rate or peak rate in bits per second. The valid values range from 8000 to 10000000000 • **be—**Indicates that the excess burst size is used for policing traffic. • **peak-burst—**Indicates that the peak-burst size is used for policing traffic. • *be***—**Excess burst size or peak-burst size in bytes. The valid values range from 1000 to 256000000. • *action***—**Action taken on a packet when it conforms, exceeds, or violates the interface bandwidth. The possible actions are shown in Table 3: Policing Actions, on page 13.

Examples: Ingress Policing

The following example shows how to configure policing actions:

```
Router(config)# policy-map ABC
Router(config-pmap)# class class-default
Router(config-pmap-c)# police 10000000 8000 8000
```

```
Router(config-pmap-c-police)# conform-action set-cos-transmit 2
Router(config-pmap-c-police)# exceed-action set-cos-transmit 1
Router(config-pmap-c-police)# end
Router#
```

The following example shows how to display policy map information:

```
Router# show policy-map ABC
```

```
Policy Map ABC
class class-default
police cir 10000000 bc 8000 be 8000
conform-action set-cos-transmit 2
exceed-action set-cos-transmit 1
Router#
```

The following example shows how to configure a single rate 2-color policer:

```
Router(config)# policy-map 1r2c
Router(config-pmap)# class class-default
Router(config-pmap-c)# police 2000000
Router(config-pmap-c-police)# conform-action transmit
Router(config-pmap-c-police)# exceed-action drop
Router(config-pmap-c-police)# end
```

The following example shows how to configure a single rate, 2-color policer with percent:

```
Router(config)# policy-map 1r2c_percent
Router(config-pmap)# class class-default
Router(config-pmap-c)# police cir percent 20
Router(config-pmap-c-police)# conform-action set-cos-transmit 0
Router(config-pmap-c-police)# exceed-action drop
Router(config-pmap-c-police)# end
Router#
```

The following example shows how to configure a dual rate, 3-color policer:

```
Router(config)# policy-map 2r3c
Router(config-pmap)# class class-default
Router(config-pmap-c)# police cir 2000000 pir 3000000
Router(config-pmap-c-police)# conform-action set-prec-transmit 3
Router(config-pmap-c-police)# exceed-action set-prec-transmit 2
Router(config-pmap-c-police)# violate-action set-prec-transmit 1
Router(config-pmap-c-police)# end
Router#
```

The following example shows how to configure a dual rate, 3-color policer with percent:

```
Router(config)# policy-map 2r3c_percent
Router(config-pmap)# class class-default
Router(config-pmap-c)# police cir percent 10 pir percent 20
Router(config-pmap-c-police)# conform-action transmit
Router(config-pmap-c-police)# exceed-action set-cos-transmit 0
Router(config-pmap-c-police)# violate-action drop
Router(config-pmap-c-police)# end
Router#
```

The following example shows how to configure a single rate, 2-color policer in class-default and a child policy:

```
Router# enable
Router# configure terminal
Router(config)# policy-map police5
Router(config-pmap)# class test18
```

```
Router(config-pmap-c)# service policy child-level
Router(config-pmap-c)# police cir 64000 50
```

The following example shows how to configure a dual rate, 3-color policer configuration in a class and policy-map:

```
Router# enable
Router# configure terminal
Router(config)# policy-map test
Router(config-pmap)# class cos2
Router(config-pmap-c)# police 1000000 pir 2000000 conform-action set-cos-transmit 3
exceed-action set-cos-transmit 1 violate-action drop
```

The following example shows how to configure a dual rate, 3-color policer in class-default with a CIR of 64 Kbps, and PIR doubled the CIR rate, a conform action of transmit, and an exceed action mark dscp af 11:

```
Router# enable
Router# configure terminal
Router(config)# policy-map qos_test
Router(config-pmap)# class class-default
Router(config-pmap-c)# police cir 64000 bc 2000 pir 128000 be 2000 conform-action transmit

exceed-action set-dscp-transmit af11 violate-action set-dscp-transmit cs1
```

The following example shows how to configure a dual rate, 3-color policer in class-default:

```
Router# enable
Router# configure terminal
Router(config)# policy-map qos_test
Router(config-pmap)# class class-default
Router(config-pmap-c)# police cir 64000 bc 2000 pir 128000 be 2000 conform-action transmit

exceed-action set-dscp-transmit af11 violate-action set-dscp-transmit cs1
```

DLP-J193 Creating or Editing a Policy Map Using CTC

Purpose	This procedure creates or edits a policy map using CTC.
Tools/Equipment	None
Prerequisite Procedures	DLP-J191 Creating or Editing a Class Map Using CTC, on page 11
Required/As Needed	As needed
Onsite/Remote	Remote
Security Level	None

Procedure

Step 1 Complete the "NTP-J22 Log into CTC" procedure at a node where you want to create a policy map.

Step 2 In the node view, right-click the Fabric or Line card and choose Open Packet Transport System View. The Packet Transport System View dialog box appears.

Step 3 Click the **Provisioning** tab.

Step 4 From the left pane, click the **QoS** tab.

Step 5 To create a policy map, in the **Policy Map** tab, click **Create Policy Map**. In the Policy Creation dialog box:

a) Enter the policy map name in the Policy-Map field.

b) Choose the class to be added to the policy map.

c) Click **Add**.

d) (Optional) Choose the child policy to be added from the Child Policy column.

Note A child policy is present only if there is another policy map created previously.

e) Add policy actions. See DLP-J194 Setting Policy Class Actions Using CTC, on page 23.

f) Repeat Step 5.a to Step 5.e to create additional policy maps.

g) Click **Finish**.

Step 6 To edit the policy map, in the **Policy Map** tab, select the policy map and click **Edit Policy Map**. In the Policy Creation dialog box, do the following to add a new class map to the policy map:

a) Choose the class to be added to the policy map.

b) Click **Add**.

c) (Optional) Choose the child policy to be added from the Child Policy column.

Note A child policy is present only if there is another policy map created previously.

d) Add policy actions. See DLP-J194 Setting Policy Class Actions Using CTC, on page 23.

e) Repeat Step 6.a to Step 6.d to add the remaining class maps to the policy map.

Note To remove the class map from the policy map, select the class from the Traffic Classes interface area and click **Remove**.
You cannot delete a class map from the policy map that is a child to another policy map.

f) Click **Finish**.

DLP-J194 Setting Policy Class Actions Using CTC

Purpose	This procedure sets the following policy class actions using CTC: • Configuring Ingress Policing • Configuring Ingress Marking • Configuring Egress Shaping • Configuring Egress Bandwidth • Configuring Low-Latency Queuing (LLQ) • Configuring Egress Bandwidth Remaining Ratio (BRR) or Bandwidth Remaining Percent (BRP)
Tools/Equipment	None
Prerequisite Procedures	DLP-J193 Creating or Editing a Policy Map Using CTC, on page 21
Required/As Needed	As needed
Onsite/Remote	Remote
Security Level	None

Procedure

Step 1 Complete the "NTP-J22 Log into CTC" procedure at a node where you want to set the policy class actions.

Step 2 In the node view, right-click the Fabric or Line card and choose **Open Packet Transport System View**. The Packet Transport System View dialog box appears.

Step 3 Click the **Provisioning** tab.

Step 4 From the left pane, click the **QoS** tab.

Step 5 In the **Policy Map** tab, select the policy map and click **Edit Policy Map**. The Policy Map Creation dialog box appears.

Step 6 In the traffic classes area, click **Actions** to set policy actions for a specific class. The Policy Class Actions wizard is displayed.

Step 7 In the **Traffic Marking** tab:

a) Choose the attribute from the Set Attribute drop-down list.

b) Enter the attribute value based on the selection made in the Set Attribute drop-down list:

Table 5: Attribute and Attribute Value

Attribute	Attribute Value
cos	Value between 0-7

Attribute	Attribute Value
ip precedence	Value between 0-7
ip dscp	Value between 0-63
qos group	Value between 0-7
discard class	Value between 0-2
cos inner	Value between 0-7
vlan inner	Value between 0-4096. For each vlan, you can have up to 30 entries.

c) Click **Add**.
d) Repeat steps 7.a through 7.c to set values for the remaining marking attributes.
e) Click **Finish**.

Step 8 In the **Policing** tab:

a) Choose one of the rates:

- Single-Rate Dual Color (CIR)
- Single-Rate Dual Color (PIR)
- Single-Rate Three Color
- Dual-Rate Three Color

b) Enter the rate and burst size for the attributes:

- Committed Information Rate and Burst Size and choose the unit from the drop-down list.
- Peak Information Rate and PeakBurst Size and choose the unit from the drop-down list.

Note The burst size unit must be **ms** if the CIR or the PIR value specified is in terms of percentage (%), and **bytes/Kbytes/mbytes** if the CIR or the PIR value specified is in terms of bits per second (bps).

c) Set the actions:

- From the Conform Action drop-down list, select the action and click **Add**.
- From the Exceed Action drop-down list, select the action and click **Add**.
- From the Violate Action drop-down list, select the action and click **Add**.

d) Click **Finish**.

Step 9 (At Egress Only) In the **Queuing** tab:

a) To set the shape average:

- Select the **Shape Average** radio button.
- Enter the Average Rate value and choose the unit from the drop-down list.

- Select the **Minimum Bandwidth** or the **Remaining Bandwidth** radio button.
- Enter the minimum or the remaining bandwidth configuration values and choose the units.

b) To set the priority:

- Select the **Priority** radio button.
- Enter the priority value and choose the unit.
- Check the **Blank** check box to set the priority without entering any value.

Note CTC supports configuring priority without any values.

c) Click **Finish**.

DLP-J195 Attaching or Removing a Traffic Policy from the Target Using Cisco IOS Commands

Before a traffic policy can be enabled for a class of traffic, it must be configured on a target. Use the **service-policy {input | output}** configuration command to attach a traffic policy to a target and to specify the direction in which the policy should be applied (either on packets entering/ingressing the target or packets exiting/egressing the target). Only one traffic policy can be applied to an interface in a given direction. Use the **no** form of the command, that is, **no service-policy {input | output}** *policy-map-name* to detach a traffic policy from a target.

Purpose	This procedure attaches or removes the traffic policy from the target using Cisco IOS commands.
Tools/Equipment	None

Prerequisite Procedures	One of the following: • DLP-J192 Configuring Ingress Policing Using Cisco IOS Commands, on page 14 • DLP-J197 Configuring Ingress Marking Using Cisco IOS Commands, on page 30 • DLP-J207 Configuring Table Maps for Egress Marking Using Cisco IOS Commands, on page 37 • DLP-J200 Associating Table Maps at Egress Using Cisco IOS Commands, on page 40 • DLP-J203 Configuring Egress Shaping Using Cisco IOS Commands, on page 48 • DLP-J202 Configuring Egress Bandwidth Using Cisco IOS Commands, on page 46 • DLP-J201 Configuring Egress LLQ Using Cisco IOS Commands, on page 43 • DLP-J204 Configuring Egress Bandwidth Remaining Ratio or Bandwidth Remaining Percent Using Cisco IOS Commands, on page 51
Required/As Needed	As needed
Onsite/Remote	Remote
Security Level	None

Procedure

	Command or Action	Purpose
Step 1	enable **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**interface** *interface-type interface-number* **Example:**	Configures an interface type and enters the interface configuration mode. • *interface-type*—Interface type

	Command or Action	Purpose
	Router(config)# interface TenGigabitEthernet 4/1	• *interface-number*—Interface number.
Step 4	**service instance** *id* **ethernet** **Example:** Router(config-if)# service instance 100 ethernet	Enters the service instance mode. • *id*—Service instance ID.
Step 5	**service-policy {input | output}** *policy-map-name* **Example:** Router(config-if-srv-instance)# service-policy input policy1	Attaches a policy map to a target. • Enter either the input or output keyword and the policy map name. • *policy-map-name*—Name of the policy map.
Step 6	**no service-policy {input | output}** *policy-map-name* **Example:** Router(config-if-srv-instance)# no service-policy input policy1	Removes the policy map from the target. • Enter either the input or output keyword and the policy map name.
Step 7	end **Example:** Router(config-if-srv-instance)# end	Exits the service instance mode.

Example: Attaching or Removing a QoS Traffic Policy for a Target

The following example shows how to attach a traffic policy to a target:

```
Router# enable
Router# configure terminal
Router(config)# interface TenGigabitEthernet 4/1
Router(config-if)# service instance 100 ethernet
Router(config-if-srv-instance)# service-policy input policy1
Router(config-if-srv-instance)# end
```

The following example shows how to remove a traffic policy from a target:

```
Router# enable
Router# configure terminal
Router(config)# interface TenGigabitEthernet 4/1
Router(config-if)# service instance 100 ethernet
Router(config-if)# no service-policy input policy1
Router(config-if)# end
```

DLP-J196 Attaching or Removing a Traffic Policy from the Target Using CTC

Purpose	This procedure attaches or removes a traffic policy from the target using CTC.
Tools/Equipment	None
Prerequisite Procedures	• DLP-J193 Creating or Editing a Policy Map Using CTC, on page 21 • DLP-J194 Setting Policy Class Actions Using CTC, on page 23 • DLP-J198 Creating or Editing a Table Map Using CTC, on page 42
Required/As Needed	As needed
Onsite/Remote	Remote
Security Level	None

Note A target can be a port, an EFP, pseudo-wire, or a channel-group.

Procedure

Step 1 Complete the "NTP-J22 Log into CTC" procedure at a node.

Step 2 In the node view, right-click the Fabric or Line card and choose **Open Packet Transport System View**. The Packet Transport System View dialog box appears.

Step 3 Click the **Provisioning** tab.

Step 4 From the left pane, click **QoS**.

Step 5 To attach a traffic policy to the port, in the **Ports** tab:

a) From the **Select the slot** drop-down list, choose the slot.
b) To apply an ingress policy to the port, select the policy from the **Ingress Policy** drop-down list.
c) To apply an egress policy to the port, select the policy from the **Egress Policy** drop-down list.
d) To apply a table map, select the table map and configuration from the **Table Map** and **Table Map Config** drop-down lists.
e) Click **Apply**.
f) Repeat Step 5.a to Step 5.e to attach traffic policies to the remaining ports.

Step 6 To remove a traffic policy from the port:

a) From the **Select the slot** drop-down list, choose the slot.
b) To remove an ingress policy from the port, select **None** from the **Ingress Policy** drop-down list.
c) To remove an egress policy from the port, select **None** from the **Egress Policy** drop-down list.

d) To remove a table map, select **None** from the **Table Map** and **Table Map Config** drop-down lists.
e) Click **Apply**.
f) Repeat Step 6.a to Step 6.e to remove traffic policies from the remaining ports.

Note
- To attach a traffic policy to an EVC circuit, see Step 10 of DLP-J3 Edit an EVC Circuit Using CTC.
- To attach a traffic policy to a pseudo-wire, see Step 12.o and Step 12.p of DLP-J91 Create a Pseudowire Using CTC.
- To attach a traffic policy to a channel group:
  1. Complete the "NTP-J22 Log into CTC" procedure at a node.
  2. In the node view, right-click the Fabric or Line card and choose **Open Packet Transport System View**. The Packet Transport System View dialog box appears.
  3. Click the **Provisioning** tab.
  4. From the left pane, click **Channel Groups**.
  5. Select the channel group and choose the table map or policy map that you want to attach.
  6. Click **Apply**.

Ingress Marking

Marking is a way to selectively modify QoS bits in a packet to identify traffic within the system and/or the network. The downstream devices in the network and the egress targets within the system can match the traffic based on the marking done at the ingress of the system. The Cisco CPT system supports ingress marking.

After you create traffic classes, configure traffic policies and traffic marking features to apply certain actions to the selected traffic in those classes.

In most cases, the purpose of a packet mark is identification. After a packet is marked, downstream devices identify traffic based on the marking and categorize the traffic according to network needs. This categorization occurs when the match commands in the traffic class are configured to identify the packets by their marking (for example, match IP precedence, match IP DSCP, match CoS, and so on). The traffic policy using this traffic class can then set the appropriate QoS features for the marked traffic.

Ingress Marking Restrictions and Usage Guidelines

The restrictions and usage guidelines to configure QoS ingress marking on a CPT system are as follows:

- Marking of the MPLS EXP bits is not supported at the ingress. However, the egress marking feature enables to mark the MPLS EXP bits by using table-maps.
- Marking of the Layer 2 CoS bit for VPWS traffic is not supported.
- The **discard-class** command for marking is not effective for end-to-end Ethernet traffic.

To configure ingress marking using Cisco IOS commands, see DLP-J197 Configuring Ingress Marking Using Cisco IOS Commands, on page 30.

To configure ingress marking using CTC, see Step 7 in DLP-J194 Setting Policy Class Actions Using CTC, on page 23.

DLP-J197 Configuring Ingress Marking Using Cisco IOS Commands

Purpose	This procedure configures ingress marking using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	DLP-J192 Configuring Ingress Policing Using Cisco IOS Commands, on page 14
Required/As Needed	As needed
Onsite/Remote	Remote
Security Level	None

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**policy-map** *policy-map-name* **Example:** Router(config)# policy-map policy1	Creates or specifies the name of the traffic policy and enters the policy-map configuration mode. • *policy-map-name*— Policy map name. This is the name of the policy map and can have a maximum of 40 alphanumeric characters.
Step 4	**class** {*class-name* | **class-default**} **Example:** Router(config-pmap)# class class1	Specifies the name of a traffic class to which the policy applies and enters the policy-map class configuration mode. • Enter the previously configured class-map name. ◦ *class-name*—User-defined class name to which the policy applies. ◦ **class-default**—Specifies that the policy applies to the default traffic class.

	Command or Action	Purpose
		Note This step associates the traffic class with the traffic policy.
Step 5	**set ip precedence** *ip precedence value* **Example:** Router(config-pmap-c)# set ip precedence 2	Marks the precedence value in the IP header with a value between 0 to 7. • *ip precedence value*— IP precedence value. **Note** The **set ip precedence** command is just an example of one of the marking commands that can be used. For a list of other marking commands, see Table 6: Traffic Marking Commands, on page 31.
Step 6	end **Example:** Router(config-pmap)# end	Exits policy-map configuration mode and returns to privileged EXEC mode.

The following table provides the traffic marking commands supported at Ingress:

Table 6: Traffic Marking Commands

Command	Description
set ip precedence *ip-precedence-value* **Example:** Router(config-pmap-c)# set ip precedence 2	Marks the precedence value in the IP header with a value between 0 to 7. • *ip precedence value*—IP precedence value.
set cos *cos-value* **Example:** Router(config-pmap-c)# set cos 2	Marks the CoS value between 0 to 7 in an 802.1Q tagged frame • *cos-value*—CoS value.
set ip dscp *ip-dscp-value* **Example:** Router(config-pmap-c)# set ip dscp 22	Marks the IP DSCP in the ToS byte with a value between 0 to 63. • *ip-dscp-value*—IP DSCP value.
set qos group *qos-group-value* **Example:** Router(config-pmap-c)# set qos group 3	Marks a QoS group identifier (ID) with a value between 0 to 7 that can be used later to classify packets. • *qos-group-value*—QoS group value.

Command	Description
set discard-class *value* **Example:** Router(config-pmap-c)# set discard-class 0	Sets the discard-class internal label to a specified value between 0 to 2. This command is supported only during table-map creation. • *value*—Discard-class value.

Examples: Ingress Marking

The following example shows the creation of a service policy called policy1. This service policy is associated to a previously defined classification policy through the use of the class command. This example assumes that a classification policy called class1 was previously configured. This example configures marking to set the IP precedence value:

```
Router# enable
Router# configure terminal
Router(config)# policy-map policy1
Router(config-pmap)# class class1
Router(config-pmap-c)# set ip precedence 1
```

This example configures marking to set the CoS value:

```
Router# enable
Router# configure terminal
Router(config)# policy-map test
Router(config-pmap)# class test
Router(config-pmap-c)# set cos 1
```

Egress QoS Functions

Egress QoS on the CPT system involves classification, shaping, queuing & scheduling, and marking. At egress, policy application is supported on multiple targets, which are:

- 10 Gigabit Ethernet (10GE) and 1 Gigabit Ethernet (1GE) interface
- Port channel interface
- Service instance on 10GE and 1GE interfaces
- Service instance on port channel

  At egress, QoS traffic can broadly be classified into two types--unicast and multicast traffic. Each of these traffic can be further classified into priority traffic which requires low latency queuing and normal traffic which does not have latency considerations.

In the CPT system, QoS at the egress can be divided into unicast traffic QoS and multicast traffic QoS. Any QoS operation performed at the egress using qos-group as a match criteria is applied only to the unicast traffic.

Unicast Versus Multicast Traffic QoS at Egress

In the CPT system, QoS at egress can be split into unicast traffic QoS and multicast traffic QoS. Any QoS operation performed at egress using qos-group as a match criteria is applied only to the unicast traffic.

Unicast traffic includes:

- Point-to-point EVC traffic
- Point-to-multipoint EVC traffic flows for L2 learned traffic
- VPWS traffic

Multicast traffic includes:

- Broadcast data traffic, unknown destination MAC flood traffic, IP multicast traffic in point-to-multipoint EVC configurations
- VPLS flood traffic

Traffic Handling in the Absence of an Output Policy

If there is no output policy configured on an EVC or an interface, the unicast traffic will be queued at the egress based on the traffic class set at the ingress. In the absence of an output policy, all the egress queues will be treated equally and will be scheduled according to the Round Robin method.

Unicast QoS Restrictions

Traffic is queued in separate queues at the egress based on the traffic-class set in the frame at the ingress. This is irrespective of whether there is an egress policy applied or not.

Note The “class-default” classification does not work at the leaf level of an output policy. This works only at a parent level in a hierarchical policy. It must be ensured that all traffic that needs to be matched using “class-default” at the leaf level is set to “qos-group 0” at the ingress, which forces the traffic-class to 0 resulting in traffic being queued in queue 0 which corresponds to the class-default.

Egress Classification

The egress classification is limited to using a traffic class field in frames to categorize the frames and make them available for QoS handling. Therefore, classification based on frame fields, such as Ethernet CoS, IP DSCP, IP precedence, MPLS EXP, and so on, should be done at ingress, and the traffic class should be assigned to the corresponding frames using the ingress marking feature.

Traffic is classified to determine whether it should be:

- Marked for further processing
- Queued and scheduled

Egress Classification Restrictions and Usage Guidelines

The restrictions and usage guidelines to configure QoS egress classification on a Cisco CPT system are as follows:

- Only one match filter is supported for each class-map.
- Only qos-group based matching is supported for user-defined classes.
- Match based on qos-group 3 and qos-group 7 is used only for low latency queuing across the system.

- Match based on the class-default in the output policy suggests that matching is based on the qos-group 0 and not the class where traffic, which does not match any selection criteria in the configured class maps, is directed.

Note Multicast traffic classification at egress differs from that of the unicast traffic classification. For details, see Understanding Multicast QoS, on page 56.

To configure classification at the egress using Cisco IOS commands, see DLP-J199 Configuring Egress Classification Using Cisco IOS Commands, on page 34.

To configure classification at the egress using CTC, see DLP-J191 Creating or Editing a Class Map Using CTC, on page 11.

DLP-J199 Configuring Egress Classification Using Cisco IOS Commands

Purpose	This procedure explains how to configure classification at the egress using Cisco IOS commands
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Remote
Security Level	None

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**class-map [match-any]** *class-map-name* **Example:** Router(config)# class-map match-any class1	Creates a class to be used with a class map and enters the class-map configuration mode. The class map is used for matching packets to the specified class. • *class-map-name*—Class name. This is the name of the class map and can have a maximum of 40 alphanumeric characters.

	Command or Action	Purpose
		The **match-any** keyword specifies that one of the match criteria must be met. Use this keyword only if you have to specify more than one match command.
Step 4	**match qos-group** *qos-group-number* **Example:** Router(config-cmap)# match qos-group 2	Matches a packet on the basis of traffic class represented by the qos-group. • *qos-group-number*—QoS-group value. The value can range from 0 to 7.
Step 5	end **Example:** Router(config-cmap)# exit	Exits class-map configuration mode and returns to privileged EXEC mode.

The following example shows how to create a class map:

```
Router# enable
Router# configure terminal
Router(config)# class-map c1
Router(config-cmap)# match qos-group 1
```

The following example shows a logical OR operation in a child policy with match qos-group and class-default in a parent class.

```
Router# enable
Router# configure terminal
Router(config)# class-map match-any childOR
Router(config-cmap)# match qos-group 1
Router(config)# policy-map testchildOR
Router(config-pmap)# class childOR
Router(config-pmap-c)# shape average 100000000
Router(config)# policy-map parentOR
Router(config-pmap)# class class-default
Router(config-pmap-c)# shape average 500000000
Router(config-pmap-c)# service-policy testchildOR
```

This example shows how to display class-map information for a specific class map using the **show run class-map** command:

```
Router# show run class-map
```

```
Building configuration...
Current configuration : 275 bytes
!
class-map match-any EgressClassmap
 match qos-group 3
class-map match-any IngressClassMap
 match cos  1
end
```

Egress Marking

The egress marking sets the MPLS EXP bits in frames egressing the Cisco CPT system in case of the VPWS (Virtual Private Wire Service) initiation and MPLS LSR (Label Switching Router) interfaces; and sets CoS bits at the VPWS termination. This is based on the qos-group, discard-class setting at the ingress. At egress, marking is done using table maps. Table-map is used for mapping the values from qos-group and discard-class to the MPLS EXP or Ethernet CoS bit at egress.

Egress Table-Map Marking

Table maps are used to mark traffic attributes. A table-map lists and maps one traffic attribute to another. In the Cisco CPT system, table-maps are created to mark the:

- MPLS EXP bit for the VPWS initiation or LSR traffic
- VLAN CoS bit for the VPWS termination traffic

In the Cisco CPT system, up to 16 table maps can be created.

A table-map is applied on the imposition PE for marking the CoS or IP DSCP/IP Precedence bits to the EXP bits and on the disposition PE for remarking the EXP bits to the CoS bits.

For carrier Ethernet circuits, marking is done using the regular ingress QoS policy options and do not require table-maps.

A table-map is applied at the LER (label edge router) port for marking the CoS or IP DSCP/IP Precedence bits to the EXP bits. A table-Map is applied at the LSR (label switch router) port or the SPE (service provider edge) port to remark the EXP bits.

A table-map is applied to the pseudo-wire (or VPWS) for marking or remarking the EXP bits to the CoS bits. A table-map can be applied only at the VPWS termination point.

Note If a table-map is not attached, the MPLS EXP or the VLAN CoS bit is set to zero. Also, the system default setting is zero.

Egress Table-Map Marking Restrictions and Usage Guidelines

The restrictions and guidelines when configuring the QoS egress marking using table maps on a Cisco CPT system are as follows:

- The **set** action commands are not allowed in an output policy.
- Egress MPLS EXP marking is supported only in the interface mode of an MPLS interface.
- Egress marking of MPLS EXP bits using the **platform set mpls-exp-topmost** command is not effective on penultimate hop popping (PHP) nodes because the tunnel label is popped in PHP scenarios and inner virtual circuit (VC) label EXP marking is forwarded as is.
- Egress CoS marking is supported only for attachment circuits and only in the service instance mode.
- Egress pseudowire CoS marking is supported with the following limitations:
    - For type-5 pseudowires, CoS marking is supported when user-configured tag rewrite actions trigger VLAN tag addition on the egress interface.

- For type-4 pseudowires, CoS marking is supported when user-configured tag rewrite actions trigger VLAN tag addition or modification on the egress interface.

To configure table-maps using Cisco IOS commands, see DLP-J207 Configuring Table Maps for Egress Marking Using Cisco IOS Commands, on page 37 .

To associate table-maps at the egress using Cisco IOS commands, see DLP-J200 Associating Table Maps at Egress Using Cisco IOS Commands, on page 40.

To configure table-maps using CTC, see DLP-J198 Creating or Editing a Table Map Using CTC, on page 42.

To associate table-maps at egress using CTC, see Step 5d in DLP-J196 Attaching or Removing a Traffic Policy from the Target Using CTC, on page 28.

DLP-J207 Configuring Table Maps for Egress Marking Using Cisco IOS Commands

Purpose	This procedure explains how to configure table maps for egress marking using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Remote
Security Level	None

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**table-map** *table-map-name* **Example:** Router(config)# table-map table1	Creates or specifies the name of the table map and enters table-map configuration mode. • *table-map-name*—Table map name. This is the name of the table map and can have a maximum of 40 alphanumeric characters.

	Command or Action	Purpose
Step 4	**map from** *from-value1, from-value2* **to** *to-value* **Example:** Router(config-tablemap)# map from 0, 2 to 2	Maps the QoS-group and discard values to the MPLS EXP or VLAN COS bit. • *from-value1*—Value of the qos-group which can range from 0 to 7. • *from-value2*—Value of the discard class which can range from 0 to 2. • *to-value*—Value of the MPLS EXP or VLAN CoS bits which can range from 0 to 7.
Step 5	**default copy** **Example:** Router(config-tablemap)#default copy	(Optional) Copies the qos-group value set at ingress to the MPLS EXP or VLAN COS bits.
Step 6	**default value** *value* **Example:** Router(config-tablemap)# default value 2	(Optional) Sets the MPLS EXP bits or the VLAN COS bits to the value stated in the command, that is, it sets the "*to-value*" to the value specified in the command, when there is no explicit mapping configured for a specific {qos-group, discard-class} tuple in the given table map. • *value*—Default value which can range from 0 to 7.
Step 7	end **Example:** Router(config-tablemap)# end	Exits table-map configuration mode and returns to privileged EXEC mode.

Note After creating the table map, the users can set the qos-group and discard class parameters to the desired value by using the sequence of commands given below. For more information on these commands, see DLP-J207 Configuring Table Maps for Egress Marking Using Cisco IOS Commands, on page 37:

```
Router(config)# policy-map ingresspolicy1
Router(config-pmap)# class class-default
Router(config-pmap-c)# set qos-group 1
Router(config-pmap-c)# set discard-class 2
```

Table 7: Set Commands

Command	Description
set qos group *qos group value* **Example:** Router(config-pmap-c)# set qos group 3	Marks a QoS group identifier (ID) with a value between 0 to 7 that can be used later to classify packets. • *qos group value*—QoS group value.
set discard-class *value* **Example:** Router(config-pmap-c)# set discard-class 0	Sets the discard-class internal label to a specified value between 0 to 2. • *value*—Discard-class value.

Note To associate table maps to an interface using IOS commands, see DLP-J200 Associating Table Maps at Egress Using Cisco IOS Commands, on page 40.

Examples: Table-Map Marking

The following example shows how to create a table map that contains multiple entries.

```
Router# enable
Router# configure terminal
Router(config)# table-map test_table
Router(config-tablemap)# map from 0,2 to 2
Router(config-tablemap)# map from 0,0 to 0
```

The following example shows how to display the table-map information:

```
Router# show table-map test_table

 Table Map test_table
    map from 0,2 to 2 (hw idx: 2)
    default 0
Router#
```

The following example shows how to create a discard class and attach a policy-map to an interface (associates a table-map to the VPWS initiation or termination):

```
Router(config)# policy-map ingresspolicy1
Router(config-pmap)# class class-default
Router(config-pmap-c)# set qos-group 1
Router(config-pmap-c)# set discard-class 2

Router(config)# interface tenGigabitEthernet 4/2
Router(config-if)# service-policy input ingresspolicy1
Router(config-if)# end
Router#

Router# show running-config policy-map ingresspolicy1

Building configuration...
```

```
Current configuration : 329 bytes
!
policy-map ingresspolicy1
 class class-default
  set qos-group 1
  set discard-class 2
!
End
```

DLP-J200 Associating Table Maps at Egress Using Cisco IOS Commands

Purpose	This procedure explains how to associate table maps at the egress to an interface for VPWS initiation, LSR, and the VPWS termination scenarios using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	DLP-J207 Configuring Table Maps for Egress Marking Using Cisco IOS Commands, on page 37
Required/As Needed	As needed
Onsite/Remote	Remote
Security Level	None

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** Router(config)# interface TengigabitEthernet 4/1	Enters the interface configuration mode. • *type number*—Interface type and interface number.
Step 4	**service-policy output** *policy-map-name* **Example:** Router(config-if)# service-policy output policy1	Attaches a policy map to an interface. • *policy-map-name*— Policy map name.

	Command or Action	Purpose
Step 5	**service instance** *id* **ethernet** **Example:** Router (config-if)# service instance 200 ethernet	(Only for VPWS termination) Enters the service instance mode. • *id* — Service instance id.
Step 6	**platform set mpls-exp-topmost from qos-group, discard-class table** *table-map-name* **Example:** Router(config-if-srv-instance)#platform set mpls-exp-topmost from qos-group, discard-class table table1	(Only for VPWS initiation and LSR scenarios) Maps the MPLS-EXP value from the table map. • *table-map-name*—Name of the table map.
Step 7	**platform set cos from qos-group, discard-class table** *table-map-name* **Example:** Router(config-if-srv-instance)#platform set cos from qos-group, discard-class table table1	(Only for VPWS termination scenario) Maps the VLAN CoS value from the table map. • *table-map-name*—Name of the table map.
Step 8	end **Example:** Router(config-if)# end	Exits the interface configuration mode.

Examples: Egress Table-Map Marking

The following example shows how to map the MPLS-EXP value for VPWS initiation (that is, the frame contains MPLS header):

```
Router(config)# int tenGigabitEthernet 4/4
Router(config-if)# service-policy output egresspolicy1
Router(config-if)# platform set mpls-exp-topmost from qos-group, discard-class table
test_table
```

The following example shows how to map the VLAN CoS value for VPWS termination where the MPLS header is removed from the frame. The **platform set cos from qos-group** command is accepted at the service instance level.

```
Router(config)# int tenGigabitEthernet 4/4
Router(config-if)# service-policy output egresspolicy1
Router(config-if)# service instance 200 ethernet
Router(config-if-srv-instance)# platform set cos from qos-group, discard-class table
test_table
```

DLP-J198 Creating or Editing a Table Map Using CTC

Purpose	The following procedure explains how create or edit a table map using CTC.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Remote
Security Level	None

Procedure

Step 1 Complete the "NTP-J22 Log into CTC" procedure at a node where you want to create a table map.

Step 2 In the node view, right-click the Fabric or Line card and choose **Open Packet Transport System View**. The Packet Transport System View dialog box appears.

Step 3 Click the **Provisioning** tab.

Step 4 From the left pane, click the **QoS** tab.

Step 5 To create a table map, in the **Table Map** tab, click **Create Table Map**. In the Table Map Creation dialog box:

a) Enter the table map name in the Table-Map name field.
b) Enter the default value.
c) Enter the values for QoS Group and Discard Class.
d) Enter the value to set MPLS or CoS attributes.
e) Click **Add**.
f) Repeat Step 5a to Step 5e to create multiple table map entries.
g) Click **Finish**.

Note To associate table maps to an interface using CTC, see Step 5d in DLP-J196 Attaching or Removing a Traffic Policy from the Target Using CTC, on page 28.

Step 6 To edit the table map, in the **Table Map** tab, select the table map and click **Edit Table Map**. In the Table Map Creation dialog box:

a) Change the default value.
b) Change the values for QoS Group and Discard Class.
c) Change the value to set MPLS or CoS attributes.
d) Click **Add**.
e) Click **Finish**.

Egress Queue Scheduling

The CPT system supports Weighted Round Robin (WRR) and Low Latency Queueing (LLQ). Queueing is based on the class based classification done at egress. LLQ prioritizes and ensures low latency to the traffic in queues configured to be in LLQ, and the remaining traffic is scheduled using WRR.

Note Queue depth is not configurable. Each queue has a minimum depth of 25600 bytes and maximum depth of 1048576 bytes.

For information on egress LLQ, see Egress LLQ, on page 43.

For information on egress bandwidth, see Egress Bandwidth, on page 45.

For information on egress shaping, see Egress Shaping, on page 48.

For information egress Bandwidth Remaining Ratio (BRR) or Bandwidth Remaining Percent (BRP), see Egress Bandwidth Remaining Ratio and Bandwidth Remaining Percent, on page 50.

Egress LLQ

Applications which are latency sensitive require handling of data with least possible delay within the system. In the Cisco CPT system, low latencies are guaranteed by using strict priority scheduling at various congestion points and egress.

LLQ Restrictions and Usage Guidelines

The restrictions and usage guidelines to configure QoS egress LLQ on a Cisco CPT system are as follows:

- The **priority** command enables the rate-limit option to ensure that a particular rate is not exceeded. However, in the Cisco CPT system, egress rate limiting is achieved using shapers that can cause additional delays. Therefore, it is advised to ensure that for LLQ traffic, rate limiting is done at ingress, and the rates specified at egress are just placeholders that are never exceeded. Exceeding the rate limit at egress would mean increased latencies for LLQ traffic.
- The **priority** command is supported only under class-map with qos-group 3 or 7 as the match criteria and multicast-priority class.

To configure LLQ using Cisco IOS commands, see DLP-J201 Configuring Egress LLQ Using Cisco IOS Commands, on page 43.

To configure LLQ using CTC, see Step 9.b in DLP-J194 Setting Policy Class Actions Using CTC, on page 23.

DLP-J201 Configuring Egress LLQ Using Cisco IOS Commands

Purpose	This procedure explains how to configure egress LLQ using Cisco IOS commands
Tools/Equipment	None

Prerequisite Procedures	Step 1 to Step 5 of DLP-J192 Configuring Ingress Policing Using Cisco IOS Commands, on page 14
Required/As Needed	As needed
Onsite/Remote	Remote
Security Level	None

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**policy map** *policy-map-name* **Example:** Router(config)# policy-map policy1	Creates or modifies a traffic policy and enters the policy-map configuration mode. The *policy-map-name* specifies the name of the traffic policy, which can have a maximum of 40 alphanumeric characters.
Step 4	**class** {*class-name* | **class-default**} **Example:** Router(config-pmap)# class class_qos_1	Specifies the name of the traffic class to which this policy applies and enters the policy-map class configuration mode, where: • *class-name*—Name of a predefined class included in the service policy. • **class-default**—Specifies that the policy applies to the default traffic class.
Step 5	**priority** *bandwidth value* **Example:** Router(config-pmap-c)# priority 10000	Provides strict priority to a class of traffic belonging to the policy-map. Specifies the maximum bandwidth usage by a traffic class through the use of a token bucket algorithm. The *bandwidth value* is in kbps, and can range from 1 to 10000000. **Note** The **priority** *bandwidth value* command is just an example of one of the priority commands that can be used. For a list of other priority commands, see Table 8: Priority (LLQ) Commands, on page 45.
Step 6	end **Example:**	Exits the configuration mode and returns to privileged EXEC mode.

	Command or Action	Purpose
	Router(config-pmap-c)# end	

The following table provides the priority commands:

Table 8: Priority (LLQ) Commands

Command	Description
priority *bandwidth value* **Example:** Router(config-pmap-c)# priority 10000	Provides strict priority to a class of traffic belonging to the policy-map. Specifies the maximum bandwidth usage by a traffic class through the use of a token bucket algorithm. The *bandwidth value* is in kbps, and can range from 1 to 10000000.
priority **Example:** Router(config-pmap-c)# priority	This command provides low-latency queuing without specifying the rate limiter.
priority percent *x%* **Example:** Router(config-pmap-c)# priority 10%	Indicates that the rate of traffic that is given low latency handling is *x%* of the parent interface bandwidth or *x%* parent class CIR if policy not applied on an interface. The percentage can be a number from 1 to 100.

Examples: Egress LLQ

The following example shows how to configure priority queue at the egress:

```
Router# config terminal
Router(config)# policy-map Test1
Router(config-pmap)# class Test
Router(config-pmap-c)# priority 10000
```

Egress Bandwidth

Applications that require committed information rate (CIR) should reserve the CIR on a per-target basis at the egress. After configuring the CIR, the traffic rates are guaranteed to be met in case of congestion at the egress.

Egress Bandwidth Restrictions and Usage Guidelines

The restrictions and usage guidelines to configure QoS egress bandwidth on a CPT system are as follows:

- Bandwidth action is not supported on classes with qos-group 3 or 7 as the match criteria, or multicast-priority class.

- The **bandwidth** command cannot be used in combination with BRR or BRP in a class-map or a policy-map.
- The system does not validate the total CIR configured on all the targets for various congestion points. Therefore, it should be ensured that the total CIR configured does not exceed the total bandwidth available.
  - Total CIR configured for a 1 Gbps interface should not exceed 1 Gbps, which includes CIR in the policy applied on the interface and services on that interface.
  - Total CIR configured for a 10 Gbps interface should not exceed 10 Gbps, which includes CIR in the policy applied on the interface and services on that interface.
  - Total CIR for all the targets on a CPT 50 shelf should not exceed 9.882 Gbps; this is the least bandwidth for a CPT50 shelf in a scenario where only one of the interconnects for a CPT50 shelf is functional.
  - Total CIR on all the unicast targets on two SFP+ interfaces on a fabric card or two CPT 50 shelves that are connected to two SFP+ interfaces of the same fabric card should not exceed 13 Gbps.

To configure the egress bandwidth using Cisco IOS commands, see DLP-J202 Configuring Egress Bandwidth Using Cisco IOS Commands, on page 46.

To configure the egress bandwidth using CTC, see Step 9.b in DLP-J194 Setting Policy Class Actions Using CTC, on page 23.

DLP-J202 Configuring Egress Bandwidth Using Cisco IOS Commands

Purpose	This procedure explains how to configure egress bandwidth using IOS commands:
Tools/Equipment	None
Prerequisite Procedures	Step 1 to Step 5 of DLP-J192 Configuring Ingress Policing Using Cisco IOS Commands, on page 14
Required/As Needed	As needed
Onsite/Remote	Remote
Security Level	None

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**policy map** *policy-map-name* **Example:** Router(config)# policy-map policy1	Creates or modifies a traffic policy and enters the policy-map configuration mode. The *policy-map-name* specifies the name of the traffic policy that can have a maximum of 40 alphanumeric characters.
Step 4	**class** {*class-name* | **class-default**} **Example:** Router(config)# class c3	Specifies the name of the traffic class to which this policy applies and enters the policy-map class configuration mode, where: • *class-name*—User-defined class name to which the policy applies. • **class-default**—Specifies that the policy applies to the default traffic class.
Step 5	**bandwidth** *bandwidth value* **Example:** Router(config-pmap-c)# bandwidth 10000	Specifies the amount of bandwidth in kbps to be assigned to the class. Implies that the class where this is applied is given a minimum bandwidth guarantee of *bandwidth value* in kbps. The amount of bandwidth configured should be large enough to also accommodate Layer 2 overheads. **Note** The **bandwidth** *bandwidth value* command is just an example of one of the bandwidth commands that can be used. For a list of other bandwidth commands, see Table 9: Bandwidth Commands, on page 47.
Step 6	end **Example:** Router(config-pmap-c)# end	Exits the configuration mode and returns to privileged EXEC mode.

The following table provides the bandwidth commands:

Table 9: Bandwidth Commands

Command	Description
bandwidth *bandwidth-value* **Example:** Router(config-pmap-c)# bandwidth 10000	Specifies the amount of bandwidth in kbps to be assigned to the class. Implies that the class where this is applied is given a minimum bandwidth guarantee of *bandwidth-value* kbps. The amount of bandwidth configured should be large enough to also accommodate Layer 2 overhead.

Command	Description
bandwidth percent *%* **Example:** Router(config-pmap-c)# bandwidth percent 20	Specifies the amount of bandwidth, in percentage from the available bandwidth, to be assigned to the class. The value ranges from 1 to 100.

Examples: Egress Bandwidth

This example shows how to configure minimum bandwidth guarantee at the egress:

```
Router# config terminal
Router(config)# policy-map Test
Router(config-pmap)# class class-default
Router(config-pmap-c)# bandwidth 10000
Router(config-pmap-c)# exit
```

Egress Shaping

Traffic shaping enables you to control the traffic going out of an interface in order to match its flow to the speed of the remote target interface and to ensure that the traffic conforms to policies contracted for it. Shaping can be used to meet downstream requirements, thereby eliminating bottlenecks in topologies with data-rate mismatches.

Shaping is the process of delaying packets in queues to make them conform to a specified profile.

Egress Shaping Restrictions and Usage Guidelines

The restrictions and usage guidelines to configure QoS egress shaping on a CPT system are as follows:

- The **shaping** command is not supported on classes with qos-group 3 or 7 as the match criteria or multicast-priority class.
- Shape on a traffic class would mean buffering of traffic in the system memory, which could result in increased latencies for these streams.

To configure shaping at the egress using IOS commands, see DLP-J203 Configuring Egress Shaping Using Cisco IOS Commands, on page 48.

To configure shaping at the egress using CTC, see Step 9.b in DLP-J194 Setting Policy Class Actions Using CTC, on page 23.

DLP-J203 Configuring Egress Shaping Using Cisco IOS Commands

Purpose	This procedure explains how to configure egress shaping using Cisco IOS commands:
Tools/Equipment	None
Prerequisite Procedures	Step 1 to Step 5 of DLP-J192 Configuring Ingress Policing Using Cisco IOS Commands, on page 14

Required/As Needed	As needed
Onsite/Remote	Remote
Security Level	None

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**class-map [match-any]** *class-map-name* **Example:** Router(config)# class-map class-interface-all	Creates a class map to be used for matching packets to a class.
Step 4	**policy map** *policy-map-name* **Example:** Router(config)# policy-map test2	*policy-map-name*—Name of the policy-map to configure.
Step 5	**class** *class-name* **Example:** Router(config-pmap)# class classtest	*class-name*—Name of a predefined class included in the service policy.
Step 6	**shape average** *cir value* **Example:** Router(config-pmap-c)# shape average 10000000	*cir value*—Average rate traffic shaping. The committed information rate (CIR) value ranges from 8000 to 10000000000 bps. **Note** The **shape average** *cir value* command is just an example of one of the shape commands that can be used. For a list of other shape commands, see Table 10: Traffic Shaping Commands, on page 50.
Step 7	end **Example:** Router(config-pmap-c)# end	Exits the configuration mode and returns to privileged EXEC mode.

Table 10: Traffic Shaping Commands, on page 50 provides the traffic shaping commands:

Table 10: Traffic Shaping Commands

Command	Description
shape average percent *%* **Example:** Router(config-pmap-c)# shape average percent 20	Shapes a class to a percent of visible bandwidth. • *%*—Percentage. The value should range from 1 to 100.
shape average *cir value* **Example:** Router(config-pmap-c)# shape average 10000000	Specifies the average rate traffic shaping. • *cir value*—CIR value in bps. The committed information rate (CIR) value ranges from 8000 to 10000000000 bps.

Examples: Egress Shaping

The following example shows traffic shaping on a main interface; traffic leaving interface gi36/1 is shaped at the rate of 10 Mb/s:

```
Router# enable
Router# configure terminal
Router(config)# class-map class-interface-all
Router(config-cmap)# match qos-group 1
Router(config-cmap)# exit
Router(config)# policy-map dts-interface-all-action
Router(config-pmap)# class class-interface-all
Router(config-pmap-c)# shape average 10000000
Router(config-pmap-c)# exit
Router(config)# interface gi36/1
Router(config-if)# service-policy output dts-interface-all-action
```

In the following example, the **shape average** command is applied at the parent level of an H-QoS policy-map:

```
Router# enable
Router# configure terminal
Router(config)# policy-map child2
Router(config-pmap)# class test
Router(config-pmap-c)# shape average 100000000
Router(config)# policy-map parent
Router(config-pmap)# class class-default
Router(config-pmap-c)# shape average 300000000
Router(config-if)# service-policy child2
```

Egress Bandwidth Remaining Ratio and Bandwidth Remaining Percent

Bandwidth Remaining Ratio (BRR) or Bandwidth Remaining Percent (BRP) specifies the ratio or percentage of the bandwidth that is divided between targets when there is congestion. BRR indicates the ratio with which the various classes are serviced when parent target is scheduled. BRP indicates the bandwidth to be allocated to each class as a percentage of the allocation done to the parent target in a hierarchical QoS model.

Bandwidth Remaining Ratio and Bandwidth Remaining Percent Restrictions and Usage Guidelines

The restrictions and usage guidelines to configure QoS egress BRR or BRP on a CPT system are as follows:

- The **BRR and BRP** commands are not supported in combination with the **bandwidth** action in a class-map or a policy-map.
- The **BRR and BRP** command are not supported on classes with qos-group 3 or 7 as the match criteria as or multicast-priority class.

BRR is implemented on logical interfaces using hierarchical policy-maps.

To configure egress BRR or BRP using Cisco IOS commands, see DLP-J204 Configuring Egress Bandwidth Remaining Ratio or Bandwidth Remaining Percent Using Cisco IOS Commands, on page 51.

To configure egress BRR or BRP using CTC, see Step 9.b in DLP-J194 Setting Policy Class Actions Using CTC, on page 23.

DLP-J204 Configuring Egress Bandwidth Remaining Ratio or Bandwidth Remaining Percent Using Cisco IOS Commands

Purpose	This procedure explains how to configure egress BRR or BRP using Cisco IOS commands
Tools/Equipment	None
Prerequisite Procedures	Step 1 to Step 5 of DLP-J192 Configuring Ingress Policing Using Cisco IOS Commands, on page 14
Required/As Needed	As needed
Onsite/Remote	Remote
Security Level	None

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**policy map** *policy-map-name* **Example:** Router(config)# policy-map policy1	Creates or modifies a traffic policy and enters the policy-map configuration mode. The *policy-map-name* specifies the name of the traffic policy, which can have a maximum of 40 alphanumeric characters.

	Command or Action	Purpose
Step 4	**class** {*class-name* | **class-default**} **Example:** Router(config-pmap)# class c3	Specifies the name of the predefined traffic class to which this policy applies and enters the policy-map class configuration mode, where: • *class-name*—User-defined class name to which the policy applies. • **class-default**—Specifies that the policy applies to the default traffic class.
Step 5	**bandwidth remaining ratio** *ratio* **Example:** Router(config-pmap-c)# bandwidth remaining ratio 2	Specifies a bandwidth-remaining ratio for class-level or subinterface-level queues to be used during congestion to determine the amount of excess bandwidth (unused by priority traffic) to allocate to non priority queues. The value should be between 1 to 127. **Note** The **bandwidth remaining percent** *x%* can be used instead of the **bandwidth remaining ratio** *ratio* command to configure BRP. For details on bandwidth remaining percent command, see Table 11: Bandwidth Remaining Ratio and Bandwidth Remaining Percent Commands, on page 52.
Step 6	end **Example:** Router(config-pmap-c)# end	Exits the configuration mode and returns to privileged EXEC mode.

The following table provides the bandwidth remaining ratio or percent commands:

Table 11: Bandwidth Remaining Ratio and Bandwidth Remaining Percent Commands

Command	Description
bandwidth remaining percent *x%* **Example:** Router(config-pmap-c)# bandwidth remaining percent 20	Specifies that the class where the command is specified should be given x% of the excess bandwidth, where excess bandwidth is the bandwidth in excess of all the minimum bandwidth guarantees of all the classes at the same level. The value should range from 1 to 100.
bandwidth remaining ratio *ratio* **Example:** Router(config-pmap-c)# bandwidth remaining ratio 2	Specifies a bandwidth-remaining ratio for class-level or subinterface-level queues to be used during congestion to determine the amount of excess bandwidth (unused by priority traffic) to allocate to non priority queues. The value should be between 1 to 127.

Examples: Egress Bandwidth Remaining Ratio

The following example shows how to configure bandwidth remaining ratio at the egress:

```
Router(config)# policy-map BRR
Router(config-pmap)# class Test1
Router(config-pmap-c)# bandwidth remaining ratio 10
Router(config-pmap-c)# exit
Router(config-pmap)# class Test2
Router(config-pmap-c)# bandwidth remaining ratio 20
Router(config-pmap-c)# exit
Router(config-pmap)# class Test3
Router(config-pmap-c)# bandwidth remaining ratio 30
Router(config-pmap-c)# exit
Router(config-pmap)# class class-default
Router(config-pmap-c)#bandwidth remaining ratio 40
```

The following example shows how to verify the bandwidth remaining ratio at the egress:

```
Router# show policy-map BRR
```

```
Building configuration...
Current configuration : 209 bytes
!
policy-map BRR
 class Test1
  bandwidth remaining ratio 10
 class Test2
  bandwidth remaining ratio 20
 class Test3
  bandwidth remaining ratio 30
 class class-default
  bandwidth remaining ratio 40
!
end
```

DLP-J205 Monitoring and Verifying QoS Configuration Using Cisco IOS Commands

Purpose	This procedure explains how to display configuration of class maps and policy maps using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	Configuring QoS on a CPT system
Required/As Needed	As needed
Onsite/Remote	Remote
Security Level	None

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show class-map** **Example:** Router# show class-map	(Optional) Displays all class maps and their matching criteria.
Step 3	**show policy-map** *policy-map-name* **class** *class-name* **Example:** Router# show policy-map policy1 class class1	(Optional) Displays the configuration for the specified class of the specified policy map. • Enter the policy map name and the class name.
Step 4	**show policy-map** **Example:** Router# show policy-map	(Optional) Displays the configuration of all classes for all existing policy maps.
Step 5	**show policy-map interface** *interface-type interface-number* **Example:** Router(config-cmap)# show policy-map interface TenGigabitEthernet 4/1	(Optional) Displays the statistics and the configurations of the input and output policies that are attached to an interface. • Enter the interface type and number.
Step 6	exit **Example:** Router# exit	Exits class-map configuration mode and returns to privileged EXEC mode.

Examples: Monitoring and Verifying QoS Configuration

This example shows how to display the class-map information for a specific class map using the **show class-map** command:

```
Router# show class-map ipp5

class Map match-any ipp5 (id 1)
match ip precedence 5
```

This example shows how to display the policy map information using the **show policy-map** command:

```
Router(config)# show policy-map
```

```
policy-map testchildOR
 class childOR
   police  100000000
policy-map parentOR
 class class-default
  police 500000000
  service-policy testchildOR
```

DLP-J206 Monitoring and Verifying QoS Configuration Using CTC

Purpose	This procedure displays configuration of class maps and policy maps using CTC.
Tools/Equipment	None
Prerequisite Procedures	Configuring QoS on a CPT system
Required/As Needed	As needed
Onsite/Remote	Remote
Security Level	None

Procedure

Step 1 Complete the "NTP-J22 Log into CTC" procedure at a node where you want to verify QoS configuration.

Step 2 In the node view, right-click the Fabric or Line card and choose **Open Packet Transport System View**. The Packet Transport System View screen appears.

Step 3 Click the **Maintenance** tab.

Step 4 From the left pane, click **IOS** and click **Open IOS Connection**. The IOS interface screen appears.

Step 5 Enter the user name and password.

Step 6 Enter one of the following show commands:

- **show class-map**
- **show policy-map** *policy-map-name* **class** *class-name*
- **show policy-map**
- **show policy-map interface** *interface-type interface-number*

Step 7 Press **Enter.** The output is displayed.

NTP-J66 Load or Store Class Maps, Table Maps, or Policy Maps Using CTC

Purpose	This procedure explains how to load or store class maps, table maps, or policy maps present in one node into another node in the network.
Tools/Equipment	None
Prerequisite Procedures	• Create a class-map • Create a policy-map • Create a table-map
Required/As Needed	As needed
Onsite/Remote	Remote
Security Level	None

Procedure

Step 1 Complete the "NTP-J22 Log into CTC" procedure at a node.

Step 2 In the node view, click the **Layer2+** tab.

Step 3 From the left pane, click **Provisioning**.

Step 4 Click the **QoS** tab .

Step 5 To load the maps from a node:

a) Click any one of tabs**—Class Map**, **Table Map** or **Policy Map**.
b) Click **Load**. The Load Maps From Selected Node dialog box appears.
c) Select the node from the drop-down list and click **Load**. The maps are displayed on the screen.
d) Select the map(s) that you want load and click **OK**. The selected maps are loaded.

Step 6 To store the maps in a node:

a) Click any one of tabs**—Class Map**, **Table Map** or **Policy Map**.
b) Click **Store**. The Store Maps To Selected Node dialog box appears.
c) Select the node in which you want to store the maps.
d) Select the maps that you want to store and click **Store**. The confirmation dialog box appears.
e) Click **OK**. The selected maps are stored on the selected node.

Understanding Multicast QoS

In the CPT system, multicast traffic at egress is queued differently than the unicast traffic. At the egress of the CPT system, a maximum of two multicast queues can be configured on each interface—a priority queue

and a non-priority queue. In addition to configuring multicast QoS per interface, multicast guarantee can be configured on the interlink interfaces between the fabric or line card and the CPT 50 shelf, for priority and non-priority multicast traffic. The definition of priority traffic for multicast is the same as for unicast, that is, the traffic-class explained in Egress Classification , on page 33 shall be used to differentiate priority traffic from non-priority traffic in the egress hardware.

Note Multicast QoS configurations use predefined multicast classes of which only two classes are supported. They are multicast-priority and multicast-normal. Multicast-priority class matches any multicast traffic with qos-group set to 3 or 7, whereas multicast-normal class matches any multicast-traffic with qos-group set to 0, 1, 2, 4, 5 or 6.

Note Configurations at the egress show classification based on predefined multicast class-maps; however, the CPT system differentiates priority and non priority multicast traffic using traffic-class set at the ingress.

Multicast QoS Restrictions

The following restrictions apply to multicast QoS:

- Multicast QoS is possible only per interface
- Only two queues are available at each interface for multicast traffic—one for priority and one for non-priority

Static Configurations for Multicast Traffic on a Card

The following example displays the static configuration for multicast traffic on a card:

```
 Router# show class-map
```

```
Router# show run class-map
Building configuration...

Current configuration : 170 bytes
!
class-map match-any multicast-normal
match access-group name multicast-normal
class-map match-any multicast-priority
match access-group name multicast-priority
end

Router#
```

Dynamic Configurations for Multicast Traffic on a Card

Note Multicast class-maps are preconfigured. Multicast traffic with qos-group 3 or 7 is considered as priority multicast traffic, and rest of the multicast traffic is considered as normal multicast traffic. You can only decide the bandwidth allocation for CIR, PIR and priority traffic.

The following example shows how to configure multicast QoS at egress:

```
Router(config)# policy-map out2
Router(config-pmap)# class multicast-normal
Router(config-pmap-c)# bandwidth percent 20
Router(config-pmap-c)# shape average percent 30
Router(config-pmap-c)# class multicast-priority
Router(config-pmap-c)# priority percent 15
Router(config-pmap-c)# end
Router#
Router# show policy-map
```

```
  Policy Map out2 (oid: 69874467, cgid: FFFFFFFF)
    Class multicast-normal (classid: 1, cid: FFFFFFFF)
       (Action oid: 933929563)
      bandwidth 20 (%)
       (Action oid: 1470800472)
      Average Rate Traffic Shaping
      cir 30%
    Class multicast-priority (classid: 2, cid: FFFFFFFF)
       (Action oid: 910587090)
      priority 15 (%)
```

```
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int ten4/1
Router(config-if)#service-policy output out2
Router(config-if)#
```

Hierarchical QoS

The Cisco CPT system supports hierarchical quality-of-service (H-QoS) that includes QoS at multiple levels in a hierarchy.

Ingress H-QoS

An H-QoS policy can be attached to an interface or a service instance. The number of levels is limited to two for an input QoS policy, where the parent level denotes the policy target and the child level denotes the QoS traffic class:

- Only the default class, that is, **class-default** is allowed at the parent level. User-defined classes are not supported at the parent level.
- Only the **police** action command is allowed at the parent level. Marking action is not supported. Also, remarking actions are not supported for the parent policer. In effect, a hierarchical policy is configured to achieve only hierarchical metering.

Egress H-QoS

The targets for H-QoS at egress are interface, service instance, and queue. There is support for up to three levels of hierarchy with the following configurations:

- Single-level policy on an interface with multicast classes for multicast traffic and class-default for unicast traffic.
- Two-level policy on a service instance with class-default queuing at parent and per qos-group queuing at the child level.

The various combination of hierarchical and flat policies are in this table.

Serial Number	EVC Policy	EVC Policy Level	EVC Class Actions (parent level[1])	EVC Classes Supported (parent level)	EVC Class Actions (child level[2])	EVC Classes Supported (child level)
1	Flat	1	—	—	• Bandwidth • Shape • Priority	Unicast classes[3]
2	Hierarchical	2	• Bandwidth • Shape	Class-default	• Bandwidth • Shape • Priority	Unicast classes
	Interface Policy	**Interface Policy Level**	**Interface Class Actions (parent level)**	**Interface Classes Supported (parent level)**	**Interface Class Actions (child level)**	**Interface Classes Supported (child level)**
3	Flat	1	—	—	• Bandwidth • Shape • Priority	All classes [4]
4	Flat	1	—	—	• Bandwidth • Shape • Priority (with multicast class)	Class-default and multicast classes[5]

5	Hierarchical	2	• Bandwidth • Shape • Priority (with multicast class)	Class-default and multicast classes	• Bandwidth • Shape • Priority	Unicast classes

1 Higher level in a hierarchical policy.
2 Lower level in a hierarchical policy or the only level in a flat policy.
3 All qos-group based classes and class-default.
4 Unicast and multicast classes.
5 Multicast-priority and multicast-normal classes.

The above table lists the possible level one and level two hierarchies. The possible combination of interface and EVC level policies are as follows:

- Entries of serial number 1 and 4 resulting in a two-level hierarchy
- Entries of serial number 2 and 4 resulting in a three-level hierarchy

EVCS QoS Support

The Ethernet Virtual Connection Services (EVCS) uses the concept of service instances and EVC (Ethernet Virtual Circuit). A service instance is the instantiation of an EVC on a given interface on a given router. An EVC is an end-to-end representation of a single instance of a Layer 2 service being offered by a provider to a customer. It embodies the different parameters on which the service is being offered.

QoS works with the following EVC combinations:

- One TAG case
- Two TAG case
- One TAG to one TAG
- One TAG to two TAG
- Two TAG to one TAG
- Two TAG to two TAG
- One TAG termination
- Two TAG termination
- Tag to Tag translation

Restrictions and Usage Guidelines

The restrictions and usage guidelines to configure QoS on EVCS are as follows:

- CoS marking or remarking is not supported for service instances defined using VLAN ranges or “encapsulation default”.
- CoS marking or remarking action applies to both inner and outer tags, when inner tag is modified within the system. In all other cases, the marking or remarking action that the user specifies is limited only to the outer tag.

Note For information on EVC, see Understanding Ethernet Virtual Circuit.

QoS Support on Port-Channel

This section explains the QoS on the Port-Channel feature support for ingress and egress.

QoS Support on Port-Channel at Ingress

The QoS on the port-channel feature enables QoS service-policies to be applied at the ingress on the following targets:

- Port-channel member link
- Port-channel main interface
- Port-channel EVC

For a policy-map attached to a port-channel main interface, ingress traffic coming from any member link is subjected to the same policy-map configured on the port-channel main interface. If no policy-map is configured on the port-channel main interface, ingress traffic from the member-link is subjected to the policy-map attached to the:

- EVC through which the traffic is flowing.
- Member link.

The QoS policy can be attached to a port-channel even if the member interfaces are on different cards. Policy-maps cannot coexist on a port-channel main interface, EVC, and member link at the same time.

Restrictions and Usage Guidelines QoS Support on Port-Channel at Ingress

The policer configuration is enforced only on a single card and not across cards in a distributed link aggregation group (LAG). However, member links might span across cards.

QoS Support on Port-Channel at Egress

The QoS on port-channel feature enables QoS service-policies to be applied at the egress on the following targets:

- Port-channel main interface
- Port-channel EVC

Note Egress service policy is not supported on the port-channel member link.

At egress, if a policy is applied on both the port-channel main interface and the EVC, only class- default queuing is possible on the port-channel main interface for unicast traffic. In such a scenario, all the EVC traffic is subjected to both port-channel QoS and port channel EVC QoS. In the context of EVCs for which a policy is not applied, only port channel QoS is applied.

Restrictions and Usage Guidelines QoS Support on Port-Channel at Egress

A policy that is applied on a port channel is not applicable to the aggregate port channel traffic. It is applicable only on a per port-channel member basis. Therefore, if a configuration that shapes all the traffic to ***x*** **Mbps** on the port-channel main interface exists, it gets translated to a configuration that shapes each member link to ***x*** **Mbps**. As a result, the aggregate traffic on the port channel could be up to ***n*** times ***x*** **Mbps**, where *n* is the number of links in the port-channel.

QoS Statistics

Enhanced performance monitoring displays QoS statistics on the CPT card interfaces. QoS statistics are supported at the 1GE interface, 10GE interface, and service instance levels. At the ingress, only byte counters are supported and at the egress, both packet and byte counters are supported.

Statistics supported at ingress are shown in this table:

Table 12: Statistics at Ingress

Statistics Collected	1GE Interface	10GE Interface	EVC	Port Channel Interface
Classification statistics— Byte Counters	Yes	Yes	Yes	Yes
Marking Statistics—Byte Counters	No	No	No	Yes
Policing Statistics—Byte Counters	Supported with limitations: • In a 2-color policer, both green and red byte counters are supported. • In a 3-color policer, green/non-green or non-red/red are supported	Supported with limitations: • In a 2-color policer, both green and red byte counters are supported • In a 3-color policer, green and non-green or non-red and red are supported	No	Yes

Statistics supported at egress are shown in this table:

Table 13: Statistics at Egress

Statistics Collected	1GE Interface	10GE Interface	EVC	Port Channel Interface
Classification statistics - Packet and Byte Counters	Yes	Yes	Yes	Yes
Queuing Statistics— (Accepted or Dropped) Packet and Byte Counters	Yes	Yes	Yes	Yes
Match Statistics—Packet and Byte Counters	Yes	Yes	Yes	Yes

Retrieving Egress QoS Statistics

Egress QoS statistics can be viewed by using show commands. To display this information, use one of the commands provided in the following table:

Table 14: Egress QoS Statistics Commands

Command	Purpose
show policy-map interface *interface name*	Displays the QoS statistics available for an interface.
show policy-map interface *interface name service instance number*	Displays the QoS statistics available for a service instance created under Gigabit Ethernet or 10 Gigabit Ethernet interface.

Examples: Egress QoS Statistics

The following example displays statistics available for an interface at the egress:

```
Router# show policy-map interface TenGigabitEthernet4/4
```

```
TenGigabitEthernet4/4
       Service-policy output: p22 (oid: 1310866, cgid: FFFFFFFF)

   Class-map: c1 (match-any)   (oid: 65536, cid: FFFFFFFF)
     0 packets, 0 bytes
     5 minute offered rate 0000 bps, drop rate 0000 bps
     Match: qos-group 1 (oid: 65537, fid: FFFFFFFF)
```

```
      0 packets, 0 bytes
      5 minute rate 0 bps
    (ActionGrp Local Id: 1)
    Queueing
    queue limit 28201 packets
    (queue depth/total drops/no-buffer drops) 100/0/0
    (pkts output/bytes output) 0/0
    (Action oid: 65538)
    bandwidth 800000 kbps

  Class-map: class-default (match-any)   (oid: 131072, cid: 00000639)
    0 packets, 0 bytes
    5 minute offered rate 0000 bps, drop rate 0000 bps
    Match: any  (oid: 131073, fid: 0000063A)
    (ActionGrp Local Id: 0)
```

The following example displays the QoS statistics available for a service instance created under 10 Gigabit Ethernet interface:

```
Router# show policy-map interface TenGigabitEthernet4/3 service instance 2
```

```
 TenGigabitEthernet4/3: EFP 2

 Service-policy output: p22 (oid: 2307558214, cgid: FFFFFFFF)

   Class-map: c1 (match-any)   (oid: 65536, cid: FFFFFFFF)
     0 packets, 0 bytes
     5 minute offered rate 0000 bps, drop rate 0000 bps
     Match: qos-group 1 (oid: 65537, fid: FFFFFFFF)
       0 packets, 0 bytes
       5 minute rate 0 bps
     (ActionGrp Local Id: 1)
     Queueing
     queue limit 28201 packets
     (queue depth/total drops/no-buffer drops) 100/0/0
     (pkts output/bytes output) 0/0
     (Action oid: 65538)
     bandwidth 800000 kbps

   Class-map: class-default (match-any)   (oid: 131072, cid: 00000639)
     0 packets, 0 bytes
     5 minute offered rate 0000 bps, drop rate 0000 bps
     Match: any  (oid: 131073, fid: 0000063A)
     (ActionGrp Local Id: 0)

     queue limit 324314 packets
     (queue depth/total drops/no-buffer drops) 100/0/0
     (pkts output/bytes output) 0/0
```

QoS Configuration Guidelines for the Cisco CPT 50 Shelf

Traffic that is sent to the CPT 50 shelf can either be unicast or multicast traffic. When multicast traffic is sent to a multicast group or a service-instance that is configured on 1 GE interfaces of the Cisco CPT 50 shelf, a copy of each multicast frame is sent to the CPT 50 shelf. The CPT 50 shelf replicates this multicast frame on the 1 GE interfaces based on the multicast group or a service-instance configuration. This replication process

saves the bandwidth usage on the interconnect link for the CPT 50 shelf. However, there are two congestion points that must be configured with the bandwidth that should be reserved for unicast and multicast traffic. The congestion points are:

- Interlink CongestionRestrictionsExample, on page 65
- CPT 50 Shelf 1 GE Interface CongestionExampleExampleExampleRestriction, on page 66

Interlink Congestion

The first congestion point for unicast and multicast traffic is the interlink interface on the fabric or the line card to which the CPT50 shelf is connected. A policy-map with multicast classes must be used to reserve the multicast bandwidth for the CPT 50 shelf.

When multicast-normal and multicast-priority classes are configured with bandwidth, shape, or priority for multicast traffic, the unicast traffic is automatically shaped to the value derived as follows:

Unicast shaper for lowest interlink interface = maximum data bandwidth on the interlink interface – (bandwidth for multicast-normal + bandwidth for multicast-priority), where

- Maximum data bandwidth on the interlink interface = link bandwidth - control bandwidth
- Link bandwidth is 10 Gbps and control bandwidth is 118 Mbps

Therefore, the maximum data bandwidth on the interlink interface = 9.882 Gbps

Restrictions

- All multicast traffic meant for the CPT50 shelf uses the lowest interlink interface. There is no load balancing for multicast traffic that is meant for the CPT50 shelf. Therefore, the total multicast bandwidth for the CPT 50 shelf is limited by the maximum data bandwidth as stated above, which is 9.882 Gbps.
- There should be a shaper configured to the same rate as the bandwidth configured for multicast-normal class. This ensures that the sum of multicast and unicast traffic sent to a CPT 50 shelf does not exceed the interlink bandwidth.
- The same interface-level policy should be applied on all the interlink interfaces meant for the CPT 50 shelf. This is to ensure that the QoS minimum guaranteed bandwidth works even in the event of an interlink failure.

Example

To reserve 250 Mbps bandwidth for normal priority multicast and 120 Mbps bandwidth for priority multicast for a CPT50 shelf, use this configuration:

```
!
policy-map interlink-mc-policy
 class multicast-normal
  bandwidth 250000
  shape average 250000000
 class multicast-priority
  priority 120000
!
Apply the policy on the interconnect port on the fabric or line card
!
interface TenGigabitEthernet4/1
 no ip address
 no keepalive
 fanout-group 37
 service-policy output interlink-mc-policy
 l2protocol peer cdp lacp
```

```
 l2protocol forward stp vtp dtp pagp dot1x
end
```

CPT 50 Shelf 1 GE Interface Congestion

The second congestion point is at the one Gigabit Ethernet interface of the CPT50 shelf, where unicast traffic and the replicated multicast traffic converge. A policy-map is used to configure the unicast and multicast bandwidth reservations. There are three possible combinations that can be used:

- Interface level policy for both multicast and unicast queuing—In this case, there is no specific QoS requirement per service-instance or EVC, but there is a requirement per queue at the interface level as shown in this example.

Example

```
!
policy-map egress
 class q1
  bandwidth 155000
 class q2
  bandwidth 100000
 class q3
  priority 150000
 class q4
  bandwidth 25000
 class q5
  shape average 50000000
  bandwidth 50000
 class q6
  bandwidth 70000
 class q7
  priority 180000
 class multicast-normal
  bandwidth 80000
 class multicast-priority
  priority 150000
 class class-default
  bandwidth 40000
!
```

- Interface level queuing for multicast traffic and CIR for unicast traffic—In order to ensure that unicast traffic receives the required CIR, the unicast non-priority and priority traffic CIR must be configured separately. Use a two-level hierarchical policy as shown in the example below to ensure that the requirements are met.

Example

```
!
policy-map port-level-child
 class q7
  priority 170000
class q7
  priority 50000

 class class-default
  bandwidth 550000
!

!
policy-map port-parent
 class multicast-normal
  bandwidth 80000
 class multicast-priority
```

```
  priority 150000
 class class-default
  service-policy port-level-child
!
```

- Interface level queuing for multicast traffic and CIR/PIR for unicast queues at service-instance or the EVC level—In this configuration, ensure that the sum of unicast and multicast CIR/PIR do not exceed the interface bandwidth.

Example

```
!
policy-map port-default
 class multicast-normal
  bandwidth 80000
 class multicast-priority
  priority 150000
 class class-default
  shape average 770000000
!
end

!
policy-map evc1
 class q1
  bandwidth 30000
 class q2
  bandwidth 50000
 class q3
  priority 75000
 class q4
  bandwidth 12500
 class q5
  shape average 50000000
  bandwidth 25000
 class q6
  bandwidth 90000
 class q7
  priority 90000
 class class-default
  bandwidth 10000
!
end
```

Restriction

If a service-instance or EVC level CIR is present, configure a shaper on the class-default in the policy-map applied on the interface. This ensures that the unicast and multicast traffic converging at the CPT 50 shelf 1 GE interface do not interfere with each other.

Interlink QoS

The user can prioritize the traffic from 1 GE ports of CPT 50 to CPT 200 or CPT 600 when there is congestion on the 10 GE interlink ports. Each 1 GE port has eight queues to control the incoming traffic and each queue is marked with a qos-group value ranging from 0 to 7.

CPT provides strict priority queuing mode. In this mode, two queues with the qos-group value set to 7 and 3 share the highest priority and a low latency, and are scheduled on a round-robin basis if there is traffic on both these queues. The remaining six queues are configured in strict priority scheduling mode in the following order: Qos-group 6, 5, 4, 2, 1, and 0.

For information on how to configure strict priority, refer to the NTP-J72 Create a Fan–Out–Group Using CTC procedure.