Configuring Ethernet Services Plus Line Cards

This chapter describes how to configure the features that are supported on Ethernet Services Plus (ES+) line cards. Release 12.2(33)SXJ1 and later releases support ES+ line cards.

Note

- For complete syntax and usage information for the commands used in this chapter, see the Cisco IOS Master Command List, at this URL:

  http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_book.html
- You can configure ES+ line card ports as MPLS core P router ports that carry L2VPN Advanced VPLS (A-VPLS) feature traffic. See Chapter 33, "Configuring A-VPLS."

This chapter consists of these sections:

Tip

For additional information about Cisco Catalyst 6500 Series Switches (including configuration examples and troubleshooting information), see the documents listed on this page:

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

Participate in the Technical Documentation Ideas forum

Release 12.2SX ES+ Line Card Support and Restrictions

- Ethernet Services Plus Extended Transport (ES+XT) line cards:

Transceivers:	LAN/WAN PHY, OTN/G.709		
Ports	**Product ID**	**DFC**	**Network Processors (NP)**
4 10GE ports: (Dual fabric connections)	76-ES+XT-4TG3CXL	DFC3CXL	Port 1: NP0 Port 2: NP1 Port 3: NP2 Port 4: NP3
	76-ES+XT-4TG3C	DFC3C	
2 10GE ports: (Single fabric connection)	76-ES+XT-2TG3CXL	DFC3CXL	Port 1: NP0 Port 2: NP1
	76-ES+XT-2TG3C	DFC3C	

- Ethernet Services Plus (ES+) line cards:

Transceivers:	XFP		
Ports	**Product ID**	**DFC**	**Network Processors (NP)**
4 10GE ports: (Dual fabric connections)	7600-ES+4TG3CXL	DFC3CXL	Port 1: NP0 Port 2: NP1 Port 3: NP2 Port 4: NP3
	7600-ES+4TG3C	DFC3C	
2 10GE ports: (Single fabric connection)	7600-ES+2TG3CXL	DFC3CXL	Port 1: NP0 Port 2: NP1
	7600-ES+2TG3C	DFC3C	

- ES+ line cards are supported with Supervisor Engine 720-10GE and Supervisor Engine 720.
- ES+ line cards are not supported with Supervisor Engine 32.
- ES+ line cards are not supported in PFC3A mode.
- ES+ line cards do not support these interface types:
  - Layer 2 access or trunk ports (ports configured with the **switchport** command).
  - Port-channel interfaces (ES+ line card ports cannot be members of EtherChannels).
  - Service instances
- CDP is disabled by default on ES+ line card ports (CSCtk12860).

Line Card Configuration

These sections provide information about configuring ES+ line cards:

- Displaying the ES+ Line Card Type, page A-3
- Resetting an ES+ Line Card, page A-3

Displaying the ES+ Line Card Type

To verify the ES+ line card type, you can use the **show module** command. There are other commands that also provide ES+ line card hardware information, such as the **show idprom** command, and the **show running-config interface** command.

The following example shows output from the **show module** command with an ES+ line card installed in slot 8:

```
Router# show module es_plus_slot
```

The following example shows output from the **show idprom** command for an ES+ line card installed in slot 8:

```
Router# show idprom module es_plus_slot
```

The following example shows sample output from the **show running-config interface** command to verify that the newly created interface appears in the running configuration:

```
Router# show running-config interface es_plus_slot
```

Resetting an ES+ Line Card

To reset an ES+ line card, use the following command in privileged EXEC configuration mode:

Command	Purpose
`Router# hw-module module slot reset`	Turns power off and on to the ES+ line card in the specified slot.

Configuring QoS

This section provides information about configuring Quality of Service (QoS) on ES+ line cards.

Note QoS on the ES+ line cards uses Layer 2 frame size.

This chapter includes the following sections:

Supported Interfaces

The ES+ line cards support QoS on these interface types:

- Layer 3 interfaces (routed ports)
- Layer 3 subinterfaces
- SVI interfaces

QoS Functions

Ingress QoS Functions

Ingress Trust

Trust is a port assignment instructing the port to trust (leave) existing priorities as they are on incoming frames or to rewrite the priorities back to zero.

A packet can arrive at an interface with a priority value already present in the packets header. The router needs to determine if the priority setting was set by a valid application or network device according to pre defined rules or if it was set by a user hoping to get better service.

The router has to decide whether to honor the priority value or change it to another value. How the router makes this determination is by using the port "trust" setting.

Layer 3 interfaces (routed ports) and the Layer 3 subinterfaces always trust Differentiated Services Code Point (DSCP) by default.

To change the ingress type of service (ToS), use marking. For information on marking, see the "Configuring Marking" section on page A-16.

Note The ES+ line card marks a packet as *trust cos* when ingress marking for CoS is configured for a routed interface. Hence, the CoS value configured using the **set cos** *value* command is retained on the outgoing packet. This cos value is not overwritten by earl or derived from dscp.

Ingress Classification

Classification entails using a traffic descriptor to categorize a packet within a specific group to define that packet and make it accessible for QoS handling on the network. Using 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

For information on configuring classification, see the "Configuring Classification" section on page A-6.

Ingress Policing

Policing provides a means to limit the amount of bandwidth that traffic traveling through a given port, or a collection of ports in a VLAN, can use. Policing works by defining an amount of data that the router is willing to send or receive in kilobytes per second.

When policing is configured, it limits the flow of data through the router by dropping or marking down the QoS value. Policing allows the router to limit the rate of specific types to a level lower than what they might get otherwise based only the interface bandwidth.

For information on configuring policing, see the "Configuring Policing" section on page A-9.

Ingress Marking

After it has been classified, traffic can be marked. Marking is a way to selectively modify the classification bits in a packet to identify traffic within the network. Other interfaces can then match traffic based on the markings. For information on configuring marking, see the "Configuring Marking" section on page A-16.

Egress QoS Functions

Egress Classification

Classification uses a traffic descriptor to categorize a packet within a specific group to define that packet and make it accessible for QoS handling on the network. Using 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
- Queued to rate limit specific traffic types

For information on configuring classification, see the "Configuring Classification" section on page A-6.

Egress Policing

ES+ line cards support egress port policing.

Egress Marking

After traffic has been classified, the router can mark it. You use marking to selectively modify the classification bits in the packet to differentiate packets based on the designated markings. For information on configuring marking, see the "Configuring Marking" section on page A-16.

Egress Shaping

Traffic shaping allows you to control the traffic going out 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. You can use shaping to meet downstream requirements, thereby eliminating bottlenecks in topologies with data-rate mismatches. For information on configuring shaping, see the "Configuring Shaping" section on page A-19.

Egress Queue Scheduling

The egress line card uses Class-based Weighted Fair Queuing (CBWFQ) and Weighted Random Early Detection (WRED) congestion avoidance to help prevent congestion and keep its buffers from overflowing. For information on configuring egress scheduling, see the "Configuring Bandwidth and CBWFQ" section on page A-24.

Configuring Classification

Classification Overview

Use the QoS classification features to select your network traffic and categorize it into classes for further QoS processing based on matching certain criteria. 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.

Classification Restrictions and Usage Guidelines

Follow these restrictions and usage guidelines when configuring the QoS classification:

- Classification on ES+ line cards on SVIs is supported only for EoMPLS and VPLS.
- The **match not** command is not supported.

Table A-1 provides information about supported QoS classification features.

Table A-1 QoS Classification Feature Support

Feature (match command)	Supported Interfaces
Match on access list (ACL) number (**match access-group** command)	Input and output for the following interface types: • Layer 3 interfaces (routed ports) • Layer 3 subinterfaces **Note** Deny ACL is not supported on ES+ line cards.
Match on Class of Service (CoS) (**match cos** command)	Input and output for the following interface types: • Layer 3 interfaces (routed ports), to match subinterface traffic and policy-map applied on the Layer 3 interface. • Layer 3 subinterfaces • SVI interfaces only for EoMPLS and VPLS
Match on input VLAN (**match input vlan** command)	Output for Layer 3 interfaces (routed ports), used with non-intelligent line card on the input side and an ES+ line card on the output side. The service policy is applied on the output side to match the VLAN from the input side.
Match on IP DSCP (**match ip dscp** command)	Input and output for the following interface types: • Layer 3 interfaces (routed ports) • Layer 3 subinterfaces
Match on IP precedence (**match ip precedence** command)	Input and output for the following interface types: • Layer 3 interfaces (routed ports) • Layer 3 subinterfaces
Match on MPLS experimental (EXP) bit (**match mpls experimental** command)	Input and output for the following interface types: • Layer 3 interfaces (routed ports) • Layer 3 subinterfaces
Match on VLAN (**match vlan** command) **Note** Matches the outer VLAN of a Layer 2 IEEE 802.1Q frame.	Input and output for the following interface types: • Layer 3 interfaces (routed ports) for classification on SVIs only for EoMPLS and VPLS • Layer 3 subinterfaces

	Command	Purpose
Step 1	`Router> enable`	Enables privileged EXEC mode (enter your password if prompted).
Step 2	`Router# configure terminal`	Enters global configuration mode.
Step 3	`Router(config)# class-map [match-all | match-any] class-map-name`	Creates a traffic class, where: • **match-all**—(Optional) Specifies that all match criteria in the class map must be matched, using a logical AND of all matching statements defined under the class. This is the default. • **match-any**—(Optional) Specifies that one or more match criteria must match, using a logical OR of all matching statements defined under the class. • *class-map-name*—Specifies the user-defined name of the class. **Note** You can define up to 1000 unique class maps.
Step 4	`Router(config-cmap)# match type`	Specifies the matching criterion to be applied to the traffic, where *type* represents one of the supported **match** commands shown in Table A-1. **Note** A single class map can contain up to 8 different **match** command statements.

This 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
```

This is an example of configuring class matching on multiple match statements.

```
Router> enable
Router# configure terminal
Router(config)# class-map match-any many (id 1047)
Router(config-cmap)# match ip precedence 3
Router(config-cmap)# match access-group 100
Router(config-cmap)# match mpls experimental 5
```

This is an example of configuring class matching on named ACLS.

```
Router> enable
Router# configure terminal
Router(config)# class-map match-all acl9 (id 1049)
Router(config-cmap)# match access-group name rock
```

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

```
Router# show class-map ipp5
    class map match-all ipp5 (id 1)
        match ip precedence 5
```

This example shows how to display class map information matching on extended ACLs using the **show class-map** command.

```
Router# show class-map acl5
    class map match-all acl5 (id 1042)
        match access-group 102
```

This example shows how to verify classification on a VLAN in the parent class of a H-QoS policy.

```
Router# show policy-map match
    policy map match
        class vlan11
           shape average 2000000 8000 8000
           service-policy match4
        class vlan12
           shape average 2000000 8000 8000
           service-policy match4
        class vlans
           shape average 500000000 2000000 2000000
           service-policy match2
```

Configuring Policing

Policing Overview

The ES+ line cards support the following QoS features:

- Individual actions
- Multiple actions
- Single rate, 2-color and 3-color policers
  - Granularity
  - Accuracy (rate and bucket depths)
  - Statistics
  - Percent based policer
- Dual Rate, 3 color, percent based policer
- Color blind mode (color aware policer not supported)
- Hierarchical policies (up to two levels)
- 255 profiles at different rates

Policing is supported at the input and output for the following interface typess:

- Layer 3 interfaces (routed ports)
- Layer 3 subinterfaces

Policing Restrictions and Usage Guidelines

When configuring policing, follow these restrictions and usage guidelines:

- The ES+ line cards supports a maximum of 1,024 unique global policy-maps per line card.
- Maximum class maps per policy-map are 255.
- Policer CIR and PIR can be any value between 64,000 bps to 10 Gb/s.
- If a service policy configures both class-based marking and marking as part of a policing action, then the marking using policing takes precedence over any class-based marking.
- When configuring policing paired with priority actions:
  - If there are some other bandwidth classes configured in the policy-map, then either **exceed** or **violate** action must be dropped. The **conform** action can be any action.
  - If no other bandwidth class is configured, then **conform**, **exceed**, and **violate** can be any action.
- Up to 48,000 policers per NP are supported for one rate 2 color or two rate 3 color policers.

Table A-2 provides information about which policing features are supported for the ES+ line cards.

Table A-2 QoS Policing Feature Support

Policing Command	Policing Action (set command)
police *bps value* **conform-action** *action* **exceed-action** *action*	• Transmit the packet (**transmit** action) • Drop the packet (**drop** command) • Set the IP precedence value (**set ip precedence** command) • Set the IP DSCP value (**set ip dscp** command) • Set the MPLS EXP bit (0–7) on imposition (**set-mpls-experimental-imposition** command) • Set the MPLS EXP bit in the topmost label (**set-mpls-experimental-topmost** command) • Set the COS value (**set cos** command)
police cir percent % **conform-action** *action* **exceed-action** *action*	• Transmit the packet (**transmit** action) • Drop the packet (**drop** command) • Set the IP precedence value (**set ip precedence** command) • Set the IP DSCP value (**set ip dscp** command) • Set the MPLS EXP bit (0–7) on imposition (**set-mpls-experimental-imposition** command) • Set the MPLS EXP bit in the topmost label (**set-mpls-experimental-topmost** command) • Set the COS value (**set cos** command) • Set the COS-inner value (**set cos-inner** command)

Table A-2 QoS Policing Feature Support (continued)

Policing Command	Policing Action (set command)
police cir *bps value* **pir** *bps value* **conform-action** *action* **exceed-action** *action* **violate-action** *action*	• Transmit the packet (**transmit** action) • Drop the packet (**drop** command) • Set the IP precedence value (**set ip precedence** command) • Set the IP DSCP value (**set ip dscp** command) • Set the MPLS EXP bit (0–7) on imposition (**set-mpls-experimental-imposition** command) • Set the MPLS EXP bit in the topmost label (**set-mpls-experimental-topmost** command) • Set the CoS value (**set cos** command) • Set the CoS-inner value (**set cos-inner** command)
police cir percent % **pir percent** % **conform-action** *action* **exceed-action** *action* **violate-action** *action*	• Transmit the packet (**transmit** action) • Drop the packet (**drop** command) • Set the IP precedence value (**set ip precedence** command) • Set the IP DSCP value (**set ip dscp** command) • Set the MPLS EXP bit (0–7) on imposition (**set-mpls-experimental-imposition** command) • Set the MPLS EXP bit in the topmost label (**set-mpls-experimental-topmost** command) • Set the COS value (**set cos** command) • Set the COS-inner value (**set cos-inner** command)

Configuring Policy Maps, Class Maps, and Policing

	Command	Purpose
Step 1	`Router>` **enable**	Enables privileged EXEC mode (enter your password if prompted).
Step 2	`Router#` **configure terminal**	Enters global configuration mode.
Step 3	`Router(config)#` **policy-map** *policy-map-name*	Creates or modifies a traffic policy and enters policy-map configuration mode, where *policy-map-name* specifies the name of the traffic policy to configure. Names can be a maximum of 40 alphanumeric characters.

	Command	Purpose
Step 4	`Router (config-pmap)# class {class-name | class-default}`	Specifies the name of the traffic class to which this policy applies and enters policy-map class configuration mode, where: • *class-name*—Specifies that the policy applies to a user-defined class name previously configured. • **class-default**—Specifies that the policy applies to the default traffic class.
Step 5	`Router(config-pmap-c)# police bps-value conform-action action exceed-action action`	Specifies a maximum bandwidth usage by a traffic class through the use of a token bucket algorithm, where: • *bps value*—Specifies the average rate in bits per second. Valid values are 16000 to 10Gb/s. • *action*—Specifies the actions that are taken on a packet when it conforms or exceeds. The possible actions are shown in Table A-2.
Or		
	`Router(config-pmap-c)# police cir percent percentage conform-action action exceed-action action`	Configures traffic policing on the basis of a percentage of bandwidth available on an interface, where: • **cir**—Specifies the committed information rate. Indicates that the committed information rate (CIR) will be used for policing traffic. • **percent**—Specifies that a percentage of bandwidth will be used for calculating the CIR. • *percentage*—Specifies the CIR bandwidth percentage. Valid values are 1 to 100. • *action*—Specifies the he actions that are taken on a packet when it conforms or exceeds. The possible actions are shown in Table A-2.
Or		
	`Router(config-pmap-c)# police cir bps-value pir bps-value conform-action action exceed-action action violate-action action`	Configures traffic policing using two rates, the CIR and the peak information rate (PIR), where: • **cir**—Specifies the committed information rate. Indicates that the CIR will be used for policing traffic. • **pir**—Specifies the peak information rate. Indicates that the PIR will be used for policing traffic. • *bps-value*—Specifies the average rate in bits per second. Valid values are 64000 to 200000000. • *action*—Specifies the he actions that are taken on a packet when it conforms or exceeds. The possible actions are shown in Table A-2.

Command	Purpose
Or	
`Router(config-pmap-c)# police cir percent` *percentage* `pir percent` *percentage* `conform-action` *action* `exceed-action` *action* `violate-action` *action*	Configures traffic policing using two rates, the CIR and the PIR, where: • **cir**—Specifies the committed information rate. Indicates that the CIR will be used for policing traffic. • **percent**—Specifies that a percentage of bandwidth will be used for calculating the CIR. • *percentage*—Specifies the CIR or PIR bandwidth percentage. Valid values are 1 to 100. • **pir**—Specifies the peak information rate. Indicates that the PIR will be used for policing traffic. • *action*—Specifies the he actions that are taken on a packet when it conforms or exceeds. The possible actions are shown in Table A-2.

In the following example, all actions are configured in separate lines.

```
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# 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
```

This example configures a 1 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
Router# show policy-map 1r2c
    Policy Map 1r2c
        Class class-default
            police cir 2000000 bc 62500
                conform-action transmit
                exceed-action drop
```

This example configures a 1 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# show policy-map 1r2c_percent
    Policy Map 1r2c_percent
        Class class-default
            police cir percent 20
                conform-action set-cos-transmit 0
                exceed-action drop
```

This example configures a 2 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# show policy-map 2r3c
    Policy Map 2r3c
        Class class-default
            police cir 2000000 bc 62500 pir 3000000 be 93750
                conform-action set-prec-transmit 3
                exceed-action set-prec-transmit 2
                violate-action set-prec-transmit 1
```

This example configures a 2 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# show policy-map 2r3c_percent
    Policy Map 2r3c_percent
        Class class-default
            police cir percent 10 pir percent 20
                conform-action transmit
                exceed-action set-cos-transmit 0
                violate-action drop
```

This example configures a single rate two color policer in class-default with a CIR of 64 Kbps, a conform action of transmit and an exceed action of drop with as small a Bc as possible:

```
Router> enable
Router# configure terminal
Router(config)# policy-map police
Router(config-pmap)# class test8
Router(config-pmap-c)# police 64000 2000
```

This example configures a single rate two color policer in class-default and a child policy with policing:

```
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 a 2R3C 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 configures a dual rate three 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 af11 and violate mark dscp cs1 with default setting on Bc.

```
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 configures a dual rate three color policer in class-default.

```
Router> enable
Router# configure terminal
Router(config)# policy-map test
Router(config-pmap)# class class-default
Router(config-pmap-c)# police cir percent 20 pir percent 40 conform-action transmit
exceed-action set-prec-transmit 1 violate-action drop
```

Use the following commands to verify policing:

Command	Purpose
`Router# show policy-map`	Displays all configured policy-maps.
`Router# show policy-map` *policy-map-name*	Displays the user-specified policy-map.
`Router# show policy-map interface`	Displays statistics and configurations of all input and output policies that are attached to an interface.

This example shows how to display policing statistics using the **show policy-map interface** command in the EXEC mode.

```
Router# show policy-map interface
TenGigabitEthernet3/1
service-policy output: x
class-map: a (match-all)
0 packets, 0 bytes
5 minute rate 0 bps
match: ip precedence 0
police:
1000000 bps, 10000 limit, 10000 extended limit
conformed 0 packets, 0 bytes; action: transmit
exceeded 0 packets, 0 bytes; action: drop
    conformed 0 bps, exceed 0 bps, violate 0 bps
```

Attaching a QoS Traffic Policy to an Interface

Before a traffic policy can be enabled for a class of traffic, it must be configured on an interface. A traffic policy also can be attached to Ethernet subinterfaces and main interfaces. Traffic policies can be applied for traffic coming into an interface (input), and for traffic leaving that interface (output).

- Attaching a QoS Traffic Policy for an Input Interface, page A-16
- Attaching a QoS Traffic Policy to an Output Interface, page A-16

Attaching a QoS Traffic Policy for an Input Interface

When you attach a traffic policy to an input interface, the policy is applied to traffic coming into that interface. To attach a traffic policy for an input interface, use the following command beginning in interface configuration mode:

Command	Purpose
`Router(config-if)# service-policy input policy-map-name`	Attaches a traffic policy to the input direction of an interface, where *policy-map-name* specifies the name of the traffic policy to configure.

Attaching a QoS Traffic Policy to an Output Interface

When you attach a traffic policy to an output interface, the policy is applied to traffic leaving that interface. To attach a traffic policy to an output interface, use the following command beginning in interface configuration mode:

Command	Purpose
`Router(config-if)# service-policy output policy-map-name`	Attaches a traffic policy to the output direction of an interface, where *policy-map-name* specifies the name of the traffic policy to configure.

Configuring Marking

- Marking Overview, page A-16
- Marking Restrictions and Usage Guidelines, page A-17
- Configuring Policy Maps, Class Maps, and Marking, page A-18

Marking Overview

After you have created your traffic classes, you can configure traffic policies to configure 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 the mark (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.

In some cases, the markings can be used for purposes besides identification. Distributed WRED, for instance, can use the IP precedence, IP DSCP, or MPLS EXP values to detect and drop packets.

Marking Restrictions and Usage Guidelines

When configuring class-based marking on an ES+ line card, follow these restrictions and usage guidelines:

- There is no limit on the number of marking statements per class map.
- Marking can be configured at the parent.
- EARL marking is not used.
- Marking can be combined with queueing policies.
- Marking statistics are not provided in **show policy-map interface** command output. You can refer to classification statistics in place of marking statistics.

Table A-3 provides information about supported QoS class-based marking features.

Table A-3 QoS Class-Based Marking Feature Support

Marking Feature (set command)	Supported Interfaces
Set IP DSCP (**set ip dscp** command—Marks the IP differentiated services code point (DSCP) in the type of service (ToS) byte with a value from 0 to 63.)	Input and output for these interface types: • Layer 3 interfaces (routed port) • Layer 3 subinterfaces
Set IP precedence (**set ip precedence** command—Marks the precedence value in the IP header with a value from 0 to 7.)	Input and output for these interface types: • Layer 3 interfaces (routed port) • Layer 3 subinterfaces
Set Layer 2 IEEE 802.1Q CoS (**set cos** command—Marks the CoS value from 0 to 7 in an 802.1Q tagged frame.)	Input and output for these interface types: • Layer 3 interfaces (routed ports) to match subinterface traffic and policy-map applied on the Layer 3 interface. • Layer 3 subinterface
Set MPLS experimental (EXP) bit on label imposition (**set mpls experimental imposition** command)	Input for these interface types: • Layer 3 interfaces (routed port) • Layer 3 subinterfaces
Set MPLS EXP topmost (**set mpls experimental topmost** command)	Input and output for these interface types: • Layer 3 interfaces (routed port) • Layer 3 subinterfaces

Configuring Policy Maps, Class Maps, and Marking

	Command	Purpose
Step 1	`Router> enable`	Enables privileged EXEC mode (enter your password if prompted).
Step 2	`Router# configure terminal`	Enters global configuration mode.
Step 3	`Router(config)# policy-map` *policy-map-name*	Creates or modifies a traffic policy and enters policy-map configuration mode, where *policy-map-name* specifies the name of the traffic policy to configure. Names can be a maximum of 40 alphanumeric characters.
Step 4	`Router(config-pmap)# class` {*class-name* | **class-default**}	Specifies the name of the traffic class to which this policy applies and enters policy-map class configuration mode, where: • *class-name*—Specifies that the policy applies to a user-defined class name previously configured. • **class-default**—Specifies that the policy applies to the default traffic class.
Step 5	`Router(config-pmap-c)# set` *type*	Specifies the marking action to be applied to the traffic, where *type* represents one of the forms of the **set** supported commands as shown in Table A-3.

This 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.

```
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 imposed MPLS EXP bits to 1:

```
Router> enable
Router# configure terminal
Router(config)# policy-map test
Router(config-pmap)# class test
Router(config-pmap-c)# set mpls experimental imposition 1
```

This example configures marking to set the inner cos value:

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

This example configures marking to set the imposed MPLS EXP bits to 1:

```
Router> enable
Router# configure terminal
Router(config)# policy-map test
Router(config-pmap)# class test
Router(config-pmap-c)# set mpls experimental topmost 1
```

Use the following commands to verify marking:

Command	Purpose
`Router# show policy-map`	Displays all configured policy-maps.
`Router# show policy-map` *policy-map-name*	Displays the user-specified policy-map.
`Router# show policy-map interface`	Displays statistics and configurations of all input and output policies that are attached to an interface.

Configuring Shaping

Shaping Restrictions and Usage Guidelines

When configuring shaping, follow these restrictions and usage guidelines:

- Up to 256 shaping profiles are supported at the parent level and 64 at the child level and flat policy.
- Shaping can be performed at all levels of the hierarchy.
- Shaping rates range from 64 Kbps to link rate.
- Dual shapers are not supported.
- Main interface supports two-level policy-maps:
  - Parent user defined classes
  - Child user defined classes
- Shaper CIR granularity for child level shaper:
  - 64,000 bps to 32,768,000 bps: granularity of 16,000 bps
  - 32,768,000 bps to 131,008,000 bps: granularity of 64,000 bps
- Shaper CIR granularity for parent level shaper:
  - Can be any value between 64,000 bps to 10 Gb/s
- Maximum shaper rate in the leaf policy-map is 130 Mb/s.
- The **shape average percent** command is not supported.

Table A-4 lists the supported QoS traffic shaping features.

Table A-4 QoS Traffic Shaping Feature Support

Traffic Shaping Feature (command)	Purpose
Class-based shaping (**shape average** commands)	Input and output for these interface types: • Layer 3 interfaces (routed ports) • Layer 3 subinterfaces

Configuring Class Maps, Policy Maps and Shaping

	Command	Purpose
Step 1	`Router> enable`	Enables privileged EXEC mode (enter your password if prompted).
Step 2	`Router# configure terminal`	Enters global configuration mode.
Step 3	`Router(config)# class-map [match-all | match-any] class-map-name`	Creates a class map to be used for matching packets to a class.
Step 4	`Router(config-cmap)# match [ip dscp ip-dscp-value | ip precedence ip-precedence-value | mpls experimental mpls-exp-value]`	Specifies a specific IP DSCP, IP precedence, or MPLS EXP value as a match criterion.
Step 5	`Router(config)# policy-map policy-name`	Specifies the name of the policy-map to configure.
Step 6	`Router(config-pmap)# class class-name`	Specifies the name of a predefined class included in the service policy.
Step 7	`Router(config-pmap-c)# shape average cir [bc] [be]`	Specifies the average rate traffic shaping.

This example shows traffic shaping on a main interface; traffic leaving interface tengi1/1 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 ip precedence 2
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 tengi1/1
Router(config-if)# service-policy output dts-interface-all-action
```

In this example, shape is applied at the parent level of an HQoS policy-map.

```
Router> enable
Router# configure terminal
Router(config)# policy-map child2
Router(config-pmap)# class prec5
Router(config-pmap-c)# shape average 100000000
Router(config)# policy-map pcd
Router(config-pmap)# class class-default
Router(config-pmap-c)# shape average 300000000
Router(config-if)# service-policy child2
```

This example configures a shaping policy in default-class with WRED:

```
Router> enable
Router# configure terminal
Router(config)# policy map qos_test
Router(config-pmap)# class class-default
Router(config-pmap-c)# shape ave 100mbps
Router(config-pmap-c)# random-detect dscp-based aggregate
```

Use the following commands to verify traffic shaping:

Command	Purpose
`Router# show interface [interface-name]`	Displays detail status of the traffic shaping.
`Router# show policy policy-name`	Displays the configuration of all classes composing the specified traffic policy.
`Router# show policy policy-name class class-name`	Displays the configuration of the specified class of the specified traffic policy.

Configuring QoS Queue Scheduling

QoS Queue Scheduling Restrictions and Usage Guidelines

When configuring queueing features, follow these restrictions and usage guidelines:

- The number of data queues configurable per policy-map at child level depends on the priority queue configuration:
  - If there are no priority queue configured, each subscriber can have up to 8 normal queues.
  - If there is any priority queue of any priority level configured, each subscriber can have 2 priority queues and up to 6 normal queues.
  - If there is only 1 priority queue configured, the other priority queue is reserved and cannot be used as a normal queue.
- 4k parent queues for ingress and 8k parent queues for egress per NP (nonconfigurable).
- 32K child queues on ingress and 64k child queues for egress per NP (nonconfigurable).
- Parent class-default on sub-interface scales more.
- Parent user-defined classmap is supported on Layer 3 interface (routed port; output only).
- QoS queue scheduling supports the following commands:
  - **bandwidth** *x kbps*
  - **bandwidth percent** *x%*
  - **bandwidth remaining percent** *x %*
  - **queue-limit** *queue-size*
  - **queue-limit** *queue-size* **packets**

- **random-detect**
- **random-detect** *min-threshold max-threshold mark-prob*
- **random-detect dscp-based aggregate**
- **random-detect dscp** *0-63 min-threshold max-threshold mark-prob*
- **random-detect prec-based**
- **random-detect precedence** *0-7 min-threshold max-threshold mark-prob*

Configuring WRED

WRED Overview

Weighted RED (WRED) generally drops packets selectively based on IP precedence. Packets with a higher IP precedence are less likely to be dropped than packets with a lower precedence. WRED is supported on the output of these interfaces:

- Layer 3 interfaces (routed ports)
- Layer 3 subinterfaces

WRED Aggregate and Non-Aggregate Mode

WRED Aggregate mode and Non-Aggregate modes define how the hardware resources are internally used to provide the WRED behavior. There are 8 WRED curves. In a WRED Non-Aggregate mode, a single or Prec value maps to one WRED curve and in a WRED Aggregate mode, multiple dscp values are mapped to one WRED curve.

The set of subclass (DSCP precedence) values defined on a random-detect dscp (aggregate) CLI is aggregated into a single hardware WRED resource. The statistics for these subclasses are also aggregated.

WRED Restrictions and Usage Guidelines

When configuring WRED, follow these restrictions and usage guidelines:

- WRED support is precedence-based, DSCP-based, and CoS-based. The default with the **random-detect** command is precedence-based WRED.
  - DSCP-based is supported only in aggregate mode, as dscp takes 64 possible values, and maps multiple DSCP values to each of the 8 WRED curves. Example: DSCP 30, 50, 60 takes WRED Curve1, DSCP 10, 40 takes WRED Curve2.
  - CoS is supported only in non-aggregate mode, as CoS takes eight possible values, and maps single value to each of the 8 WRED curves.
  - IP-prec is supported in both aggregate and non-aggregate mode.

- The support per interface is as follows:
  - For subinterfaces, WRED supports dscp and prec based only.
  - Queue limit is not supported with WRED command.
- WRED is not supported in parent classes.
- WRED is not supported for priority queues of all priority levels.
- Random Detect in class queue needs a queueing feature.
- Random Detect in default class does not need a queueing feature.
- ES+ line cards do not support discard-class-based, ECN, and WRED.
- ES+ line cards support aggregate WRED.
- Supports 8 curves per queue
- The **show policymap interface** command for WRED does not display transmitted packet and tail drop counts. Only random drops are displayed.
- The maximum threshold value must be between 16 and 1000000.
- EXP-based WRED for MPLS packets is supported.

Configuring Policy Maps, Class Maps, and WRED

	Command	Purpose
Step 1	`Router> enable`	Enables privileged EXEC mode (enter your password if prompted).
Step 2	`Router# configure terminal`	Enters global configuration mode.
Step 3	`Router(config)# policy-map` *policy-name*	Specifies the name of the policy-map to configure.
Step 4	`Router(config-pmap)# class` *class-name*	Specifies the name of a predefined class included in the service policy.
Step 5	`Router(config-pmap-c)# shape average cir` [*bc*] [*be*]	Shapes traffic to the indicated bit rate for the specified class.
Step 6	`Router(config-pmap-c)# random-detect`	Enables WRED.

This is an example of a WRED configuration.

```
Router> enable
Router# configure terminal
Router(config)# policy-map wredtest
Router(config-pmap)# class cos5
Router(config-pmap-c)# shape average 200000000
Router(config-pmap-c)# random-detect dscp-based aggregate
Router(config-pmap-c)# random-detect dscp values 0 min 100 max 200 mark-prob 1
Router(config-pmap-c)# random-detect dscp values 1 min 300 max 500 mark-prob 1
Router(config-pmap-c)# random-detect dscp values 2 min 600 max 900 mark-prob 1
```

The following example configures a class-map which matches IPP=1, 3, 5 and 7, and configures a WRED policy that is applied to the egress interface:

```
Router> enable
Router# configure terminal
Router(config)# policy-map wred
Router(config-pmap)# class IPP1
Router(config-pmap-c)# shape average 100000000
```

```
Router(config-pmap-c)# random-detect precedence-based
Router(config-pmap)# class IPP3
Router(config-pmap-c)# shape average 100000000
Router(config-pmap-c)# random-detect precedence-based
Router(config-pmap)# class IPP5
Router(config-pmap-c)# shape average 100000000
Router(config-pmap-c)# random-detect precedence-based
Router(config-pmap)# class class-default
Router(config-pmap-c)# shape average 100000000
Router(config-pmap-c)# random-detect precedence-based
```

The following example show the output of the **show policy-map** interface command (transmit packets are not displayed).

```
Router> enable
Router# configure terminal
Router# show policy-map interface tengig 11/1
TenGigabitEthernet11/1:

Service-policy output: temp_parent

Class-map: class-default (match-any)
139358 packets, 71351296 bytes
5 minute offered rate 1745000 bps, drop rate 283000 bps
Match: any
        0 packets, 0 bytes
        5 minute rate 0 bps
Queueing
queue limit 2048 packets
(queue depth/total drops/no-buffer drops) 0/104062/0
(pkts output/bytes output) 35296/18071552
shape (average) cir 10000000, bc 40000, be 40000
target shape rate 10000000

Service-policy : temp

Counters last updated 00:00:00 ago

Class-map: class-default (match-any)
139358 packets, 71351296 bytes
5 minute offered rate 1745000 bps, drop rate 1304000 bps
Match: any
        0 packets, 0 bytes
        5 minute rate 0 bps
queue limit 2048 packets
(queue depth/total drops/no-buffer drops) 0/104062/0
(pkts output/bytes output) 35296/18071552
Exp-weight-constant: 9 (1/512)
Mean queue depth: 0 packets
class Random drop Tail drop Minimum Maximum Mark
pkts/bytes pkts/bytes thresh thresh prob
```

Configuring Bandwidth and CBWFQ

Bandwidth and CBWFQ Overview

Class-based weighted fair queueing (CBWFQ) extends the standard WFQ functionality to provide support for user-defined traffic classes. For CBWFQ, you define traffic classes based on match criteria and access control lists (ACLs).

Bandwidth is supported on the output of these interface types:

- Layer 3 interfaces (routed ports)
- Layer 3 subinterfaces

WFQ is a method to determine bandwidth or allocating remaining bandwidth to queueing entities at a specific level in the hierarchical QoS. You can distribute bandwidth or remaining bandwidth to each entity based on the commit and excess weights set on the WFQ configuration attached to the entity. The commit and excess WFQ weights are initially programmed into WFQ profile registers, where later the WFQ profiles are attached to one or more queuing entities based on whether or not they share the same or similar bandwidth configuration.

The layer 3 and layer 4 level WFQ profiles belong to one hardware pool and can be commonly used among the layers.

Bandwidth and CBWFQ Restrictions and Usage Guidelines

When configuring Bandwidth and CBWFQ, follow these restrictions and usage guidelines:

- The **bandwidth** *kbps* and **bandwidth percent** *x%* commands are supported.
- The **bandwidth remaining percent** command is supported at the child level. The **bandwidth remaining ratio** command is supported at the parent and child level.
- The **bandwidth** command used within a QoS policy-map must be consistent across classes.

Configuring Policy Maps, Class Maps, and Bandwidth

	Command	Purpose
Step 1	`Router> enable`	Enables privileged EXEC mode (enter your password if prompted).
Step 2	`Router# configure terminal`	Enters global configuration mode.
Step 3	`Router(config)# policy-map` *policy-map-name*	Creates or modifies a traffic policy and enters policy-map configuration mode, where *policy-map-name* specifies the name of the traffic policy to configure. Names can be a maximum of 40 alphanumeric characters.
Step 4	`Router(config)# class {`*class-name* `| class-default}`	Specifies the name of the traffic class to which this policy applies and enters policy-map class configuration mode, where: • *class-name*—Specifies that the policy applies to a user-defined class name previously configured. • **class-default**—Specifies that the policy applies to the default traffic class.
Step 5	`Router(config-pmap-c)# bandwidth {bandwidth-kbps | percent percent | percent` *percent*`}}`	Specifies the amount of bandwidth, in kbps, or percentage of available bandwidth, to be assigned to the class. The amount of bandwidth configured should be large enough to also accommodate Layer 2 overhead.

This example shows a service policy called policy1 that specifies the amount of bandwidth to allocate for traffic classes 1 and 2:

```
Router> enable
Router# configure terminal
Router(config)# class-map class1
Router(config-cmap)# match ip dscp 30
Router(config-cmap)# exit
Router(config)# class-map class2
Router(config-cmap)# match ip dscp 10
Router(config-cmap)# exit
Router(config)# policy-map policy1
Router(config-pmap)# class class1
Router(config-pmap-c)# bandwidth 30000
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config-pmap)# class class2
Router(config-pmap-c)# bandwidth 20000
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface tengigabitethernet 2/1
Router(config-if)# service-policy output policy1
Router(config-if)# exit
```

The following example configures a QoS policy with multiple user class with rate guarantee setting using the **bandwidth** command.

```
Router(config)# policy-map policy1
Router(config)# class c1
Router(config-pmap-c)# bandwidth percent 1%
Router(config-pmap)# class c2
Router(config-pmap-c)# bandwidth percent 10%
Router(config-pmap)# class c3
Router(config-pmap-c)# bandwidth percent 88%
Router(config-pmap)# class class-default
Router(config-pmap-c)# bandwidth 1%
```

The following example configures a QoS policy with multiple user class with rate guarantee setting:

```
Router> enable
Router# configure terminal
Router(config)# policy-map child_policy
Router(config-pmap)# class video
Router(config-pmap-c)# police 10000000
Router(config-pmap)# class critical
Router(config-pmap-c)# bandwidth remaining percent 80
Router(config-pmap)# class class-default
Router(config-pmap-c)# bandwidth remaining percent 20
```

Use the following commands to verify CBWFQ:

Command	Purpose
Router# **show policy-map** *policy-map*	Displays the configuration of all classes that make up the specified policy-map.
Router# **show policy-map** *policy-map* **class** *class-name*	Displays the configuration of the specified class of the specified policy-map.

Command	Purpose
`Router# show policy-map interface interface-name`	Displays the configuration of all classes configured for all policy-maps on the specified interface.
`Router# show queue interface-type interface-number`	Displays queueing configuration and statistics for a particular interface.

Configuring LLQ

LLQ Overview

Low-Latency Queuing (LLQ) uses the **priority** command to allocate bandwidth to the class maps in the policy-map.

LLQ is supported on the output of the following interfaces:

- Main Layer 3 interface
- Layer 3 subinterface

LLQ Restrictions and Usage Guidelines

When configuring LLQ, follow these restrictions and usage guidelines:

- Ingress LLQ is not supported
- Egress LLQ
  - LLQ/PQ is supported only on egress for ES+ Layer 3 and Layer 3 subinterfaces.
  - Dual priority queues are supported (priority level 1 and priority level 2).
  - LLQ configuration is allowed at the child policy.
  - The **priority** and **priority level** commands are supported but you cannot use both in the same policy-map.
  - Basic priority/low latency queue with bit rates is not supported.
  - Basic low latency queue with percent is not supported.
  - Priority queue with bit rates is not supported.

Configuring LLQ

	Command	Purpose
Step 1	`Router> enable`	Enables privileged EXEC mode (enter your password if prompted).
Step 2	`Router# configure terminal`	Enters global configuration mode.
Step 3	`Router(config)# policy-map policy-name`	Specifies the name of the policy-map to configure.

	Command	Purpose
Step 4	`Router(config-pmap)# class {class-name | class-default}`	Specifies the name of a predefined class included in the service policy.
Step 5	`Router(config-pmap-c)# police bps-value conform-action action exceed-action action`	Specifies a maximum bandwidth usage by a traffic class through the use of a token bucket algorithm, where: • *bps-value*—Specifies the average rate in bits per second. Valid values are 64000 to 200000000. • *action*—Specifies the he actions that are taken on a packet when it conforms or exceeds. The possible actions are shown in Table A-2.
	Or	
	`Router(config-pmap-c)# police cir percent % conform-action action exceed-action action`	Configures traffic policing on the basis of a percentage of bandwidth available on an interface, where: • **cir**—Specifies the committed information rate. Indicates that the CIR will be used for policing traffic. • **percent**—Specifies that a percentage of bandwidth will be used for calculating the CIR. • *%*—Specifies the CIR bandwidth percentage. Valid values are 1 to 100. • *action*—Specifies the he actions that are taken on a packet when it conforms or exceeds. The possible actions are shown in Table A-2.
	Or	
	`Router(config-pmap-c)# police cir bps-value pir bps-value conform-action action exceed-action action violate-action action`	Configures traffic policing using two rates, the CIR and the PIR, where: • **cir**—Specifies the committed information rate. Indicates that the CIR will be used for policing traffic. • **pir**—Specifies the peak information rate. Indicates that the PIR will be used for policing traffic. • *bps-value*—Specifies the average rate in bits per second. Valid values are 64000 to 200000000. • *action*—Specifies the he actions that are taken on a packet when it conforms or exceeds. The possible actions are shown in Table A-2.
	Or	

Command	Purpose
`Router(config-pmap-c)# police cir percent` *percentage* `pir percent %` `conform-action` *action* `exceed-action` *action* `violate-action` *action*	Configures traffic policing using two rates, the CIR and the PIR, where: • **cir**—Specifies the committed information rate. Indicates that the CIR will be used for policing traffic. • **percent**—Specifies that a percentage of bandwidth will be used for calculating the CIR. • *%*—Specifies the CIR or PIR bandwidth percentage. Valid values are 1 to 100. • **pir**—Specifies the peak information rate. Indicates that the PIR will be used for policing traffic. • *action*—Specifies the he actions that are taken on a packet when it conforms or exceeds. The possible actions are shown in Table A-2.
Step 6 `Router(config-pmap-c)# priority [level] {1-2}`	Gives strict priority to a class of traffic belonging to the policy-map.

The following example configures a simple LLQ QoS policy on a class c1 with strict priority setting.

```
Router> enable
Router# configure terminal
Router(config)# policy map qos_llq
Router(config-pmap)# class c1
Router(config-pmap-c)# police 500000000
Router(config-pmap-c)# priority
```

The following example configures an LLQ policy with multiple priority classes with a smallest percent value and default burst value for testing:

```
Router> enable
Router# configure terminal
Router(config-pmap)# class-map voice
Router(config-pmap-c)# police cir percent 10
Router(config-pmap-c)# priority
Router(config-pmap)# class-map video
Router(config-pmap-c)# police cir percent 20
Router(config-pmap-c)# priority
Router(config-pmap)# class-default
```

Configuring Hierarchical QoS

Hierarchical QoS Overview

The ES+ line cards support hierarchical QoS (H-QoS) that you configure using Cisco Modular QoS CLI (MQC). The following H-QoS capabilities are supported:

- Two-level H-QoS (A policy-map with two levels has three levels of hierarchy when attached on the main interface.)
- Granular QoS—Policing and shaping, down to 64 Kbps data rate
- Color blind policing—2-rate, 3-color policers and 1-rate, 2-color policers

Note Color aware policing is not supported

- Egress classification
- QoS on TenGigabitEthernet 802.1Q subinterface(s)
- Egress Class-based Weighted Fair Queuing (CBWFQ)
- Low Latency Queuing (LLQ) (Ingress and Egress)
- Egress H-QoS on IP/MPLS and Layer 2 CoS classification
- AToM QoS features on Ethernet L2VPNs
- Hierarchical policing
- Scaling for ES+ line cards:
  - 128,000 queues
  - 16,000 traffic shapers
  - 48,000 policers per NP
  - 8,000 H-QoS policy-maps per NP in egress.
  - 24000 policers per ES+ line card.

Follow these restrictions while configuring Hierarchical QoS:

- Support up to128,000 queues.
- Support up to 16,000 traffic shapers.
- Support up to 48,000 policers per NP.
- Support up to 8,000 H-QoS policy-maps per NP in egress and 3904 policy-maps per NP in ingress.

Follow these restrictions and usage guidelines while configuring Hierarchical QoS:

- Support up to 16 queues for each port.
- Support up to 16 queues per port channel.
- Single fabric connection ES+ line cards support up to 24000 policers per line card.
- Dual fabric connection ES+ line cards support up to 48000 policers per line card.
- Supports up to 8,000 H-QoS policy maps per NP in egress and 3904 H-QoS policy-maps per NP in ingress.
- If a child policy is applied with a QoS queuing feature, only the child classes with queuing feature is considered for the queue restriction per port. The parent class is not considered.
- If a child policy is not applied with a QoS queuing feature, then parent class is considered for queue restriction per port.

ES+ line cards support parent and child class hierarchical levels on the physical (main) interface and subinterface (logical layer).

A policy-map with two levels has three levels of hierarchy when attached on the main interface, and four levels of hierarchy when attached on a subinterface.

Table A-5 provides information about supported H-QoS features.

Table A-5 Hierarchical QoS Feature Support

Interface Type	Marking	Policing	Shaping	Bandwidth	Priority and Priority Percent	Priority and Policing	WRED
Layer 3 interface (routed port)	CoS, precedence/DSCP, EXP	Yes	Yes	Yes	**No**	Yes	Yes
Layer 3 subinterface	CoS, precedence/DSCP, EXP	Yes	Yes	Yes	**No**	Yes	Yes

Hierarchical QoS Examples

This example configures the child policy to allocate different percentages of bandwidth by class:

```
Router> enable
Router# configure terminal
Router(config)# policy-map child
Router(config-pmap)# class user-a
Router(config-pmap-c)# bandwidth percent 40
Router(config-pmap-c)# exit
Router(config-pmap)# class user-b
Router(config-pmap-c)# bandwidth percent 60
Router(config-pmap-c)# exit
Router(config-pmap)# exit
```

This example applies the parent service policy to an output subinterface:

```
Router> enable
Router# configure terminal
Router(config)# interface tengigabitethernet 2/1.1
Router(config-if-srv)# encapsulation dot1q 11
Router(config-if)# service-policy output parent
```

This example shows how to configure a 2 level H-QoS policy on a main interface:

```
Router(config)# policy-map child_1
Router(config-pmap)# class prec1
Router(config-pmap-c)# priority level 1
Router(config-pmap-c)# exit
Router(config-pmap)# class prec2
Router(config-pmap-c)# priority level 2
Router(config-pmap-c)# exit
Router(config-pmap)# class class-default
Router(config-pmap-c)# police 100000
Router(config-pmap-c)# exit
Router(config)# policy-map HQoS_parent
Router(config-pmap)# class class-default
Router(config-pmap-c)# shape average 100000000
Router(config-pmap-c)# service-policy child_1
```

This example shows how to configure a 2 level H-QoS policy on a subinterface:

```
Router(config)# policy-map child_1
Router(config-pmap)# class cos1
Router(config-pmap-c)# priority level 1
Router(config-pmap-c)# exit
Router(config-pmap)# class cos 2
Router(config-pmap-c)# priority level 2
Router(config-pmap-c)# exit
Router(config-pmap)# class class-default
Router(config-pmap-c)# police 100000
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# policy-map HQoS_parent
Router(config-pmap)# class class-default
Router(config-pmap-c)# shape average 100000000
Router(config-pmap-c)# service-policy child_1
```

This example configures an ingress 2-level H-QOS policy on a main-interface:

```
Router(config)# policy-map child_1
Router(config-pmap)# class prec123
Router(config-pmap-c)# random-detect precedence based
Router(config-pmap-c)# exit
Router(config-pmap)# class prec456
Router(config-pmap-c)# shape average 10000000
Router(config-pmap-c)# exit
Router(config-pmap)# class class-default
Router(config-pmap)# exit
Router(config)# policy-map HQoS_parent
Router(config-pmap)# class ACL_c1
Router(config-pmap-c)# police 100000
Router(config-pmap-c)# priority level 1
Router(config-pmap-c)# service policy child_1
Router(config-pmap-c)# exit
Router(config-pmap)# class ACL_c2
Router(config-pmap-c)# police 100000
Router(config-pmap-c)# priority level 2
Router(config-pmap-c)# service policy child_2
Router(config-pmap-c)# exit
Router(config-pmap)# class class-default
Router(config-pmap-c)# police 100000
Router(config-pmap-c)# service policy child_3
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# policy-map HQos_grandparent
Router(config-pmap)# class class-default
Router(config-pmap-c)# shape 100000000
Router(config-pmap-c)# service-policy HQoS_parent
```

Configuring MPLS Traffic Engineering Class-Based Tunnel Selection

MPLS Traffic Engineering Overview

Multiprotocol Label Switching (MPLS) Traffic Engineering (TE) enables you to dynamically route and forward traffic with different class of service (CoS) values onto different TE tunnels between the same tunnel headend and the same tailend. The TE tunnels can be regular TE tunnels or DiffServ-aware TE (DS-TE) tunnels.

The set of TE/DS-TE tunnels from the same headend to the same tailend that you configure to carry different CoS values is referred to as a "tunnel bundle." Tunnels are "bundled" by creating a master tunnel and then attaching member tunnels to the master tunnel. After configuration, CBTS dynamically routes and forwards each packet into the tunnel that meets the following requirements:

- Is configured to carry the CoS of the packet
- Has the right tailend for the destination of the packet

Because CBTS offers dynamic routing over DS-TE tunnels and requires minimum configuration, it greatly eases deployment of DS-TE in large-scale networks.

CBTS can distribute all CoS values on eight different tunnels or multiple COS value to multiple tunnels .

CBTS also allows the TE tunnels of a tunnel bundle to exit headend routers through different interfaces.

CBTS configuration involves performing the following tasks:

- Creating multiple (DS-) TE tunnels with the same headend and tailend and indicating on each of these tunnels which CoSs are to be transported on the tunnel.
- Creating a master tunnel, attaching the member tunnels to it, and making the master tunnel visible for routing.

MPLS Traffic Engineering Class-Based Tunnel Selection Restrictions and Usage Guidelines

When configuring MPLS Traffic Engineering Class-Based Tunnel Selection (CBTS), follow these restrictions and usage guidelines:

- CBTS has the following prerequisites:
  - MPLS enabled on all tunnel interfaces
  - Cisco Express Forwarding (CEF) or distributed CEF (dCEF) enabled in general configuration mode
- CBTS has the following restrictions:
  - For a given destination, all CoS values are carried in tunnels terminating at the same tailend. Either all CoS values are carried in tunnels or no values are carried in tunnels. In other words, for a given destination, you cannot map some CoS values in a DS-TE tunnel and other CoS values in a Shortest Path First (SPF) Label Distribution Protocol (LDP) or SPF IP path.

- No LSP is established for the master tunnel and regular traffic engineering attributes (bandwidth, path option, fast reroute) are irrelevant on a master tunnel. TE attributes (bandwidth, bandwidth pool, preemption, priorities, path options, and so on) are configured completely independently for each tunnel.
- CBTS does not allow load-balancing of a given EXP value in multiple tunnels. If two or more tunnels are configured to carry a given experimental (EXP) value, CBTS picks one of these tunnels to carry this EXP value (which is calculated through pre-defined rules).
- CBTS supports aggregate control of bumping (that is, it is possible to define default tunnels to be used if other tunnels go down). However, CBTS does not allow control of bumping if the default tunnel goes down. CBTS does not support finer-grain control of bumping. For example, if the voice tunnel goes down, redirect voice to T2, but if video goes down, redirect to T3.
- The operation of CBTS is not supported with Any Transport over MPLS (AToM), MPLS TE Automesh, or label-controlled (LC) ATM.

Creating Multiple MPLS Member TE or DS-TE Tunnels with the Same Headend and the Same Tailend

Perform the following task to create multiple MPLS member TE or DS-TE tunnels with the same headend and same tailend and to configure EXP values to be carried by each of these tunnels. The procedure begins in global configuration mode.

	Command	Purpose
Step 1	`Router> enable`	Enables privileged EXEC mode (enter your password if prompted).
Step 2	`Router# configure terminal`	Enters global configuration mode.
Step 3	`Router(config)# interface tunnel` *number*	Configures a tunnel interface type and enters interface configuration mode. • *number*—Number of the tunnel interface that you want to create or configure.
Step 4	`Router(config-if)# ip unnumbered` *type number*	Enables IP processing on an interface without assigning an explicit IP address to the interface. • *type*—Type of another interface on which the router has an assigned IP address. • *number*—Number of another interface on which the router has an assigned IP address. It cannot be another unnumbered interface.
Step 5	`Router(config-if)# tunnel destination {`*hostname* `|` *ip-address*`}`	Specifies the destination of the tunnel for this path option. • *hostname*—Name of the host destination. • *ip-address*—IP address of the host destination expressed in four-part, dotted decimal notation.
Step 6	`Router(config-if)# tunnel mode mpls traffic-eng`	Sets the mode of a tunnel to MPLS for TE.

	Command	Purpose
Step 7	`Router(config-if)# tunnel mpls traffic-eng bandwidth [sub-pool | global] bandwidth`	Configures the bandwidth for the MPLS TE tunnel. If automatic bandwidth is configured for the tunnel, use the **tunnel mpls traffic-eng bandwidth** command to configure the initial tunnel bandwidth, which is adjusted by the auto-bandwidth mechanism. • **sub-pool**—(Optional) Indicates a subpool tunnel. • **global**—(Optional) Indicates a global pool tunnel. Entering this keyword is not necessary, because all tunnels are global pool in the absence of the **sub-pool** keyword. But if users of pre-DiffServ-aware Traffic Engineering (DS-TE) images enter this keyword, it is accepted. • *bandwidth*—Bandwidth, in kilobits per second, set aside for the MPLS traffic engineering tunnel. Range is between 1 and 4294967295. **Note** You can configure any existing **mpls traffic-eng** command on these TE or DS-TE tunnels.
Step 8	`Router(config-if)# tunnel mpls traffic-eng exp [list-of-exp-values] [default]`	Specifies an EXP value or values for an MPLS TE tunnel. • *list-of-exp-values*—EXP value or values that are are to be carried by the specified tunnel. Values range from 0 to 7. • **default**—The specified tunnel is to carry all EXP values that are: – Not explicitly allocated to another tunnel – Allocated to a tunnel that is currently down
Step 9	`Router(config-if)# exit`	Exits to global configuration mode.

Repeat on the same headend router to create additional tunnels from this headend to the same tailend.

Creating a Master Tunnel, Attaching Member Tunnels, and Making the Master Tunnel Visible

Perform the followings task to create a master tunnel, attach member tunnels to it, and make the master tunnel visible for routing. The procedure begins in global configuration mode.

	Command	Purpose
Step 1	`Router> enable`	Enables privileged EXEC mode (enter your password if prompted).
Step 2	`Router# configure terminal`	Enters global configuration mode.

	Command	Purpose
Step 3	`Router(config)# interface tunnel number`	Configures a tunnel interface type and enters interface configuration mode, where *number* is the number of the tunnel interface that you want to create or configure.
Step 4	`Router(config-if)# ip unnumbered type number`	Enables IP processing on an interface without assigning an explicit IP address to the interface. • *type*—Type of another interface on which the router has an assigned IP address. • *number*—Number of another interface on which the router has an assigned IP address. It cannot be another unnumbered interface.
Step 5	`Router(config-if)# tunnel destination {hostname | ip-address}`	Specifies the destination of the tunnel for this path option. • *hostname*—Name of the host destination. • *ip-address*—IP address of the host destination expressed in four-part, dotted decimal notation.
Step 6	`Router(config-if)# tunnel mode mpls traffic-eng exp-bundle master`	Specifies this is the master tunnel for the CBTS configuration.
Step 7	`Router(config-if)# tunnel mode mpls traffic-eng exp-bundle member tunnel-id`	Attaches a member tunnel to the master tunnel. • *tunnel-id*—Number of the tunnel interface to be attached to the master tunnel. Repeat this command for each member tunnel.
Step 8	`Router(config-if)# tunnel mpls traffic-eng autoroute announce`	Specifies that the Interior Gateway Protocol (IGP) should use the tunnel (if the tunnel is up) in its enhanced shortest path first (SPF) calculation.
Step 9	`Router(config-if)# tunnel mpls traffic-eng autoroute metric {absolute | relative} value`	(Optional) Specifies the MPLS TE tunnel metric that the IGP-enhanced SPF calculation uses. • **absolute**—Indicates the absolute metric mode; you can enter a positive metric value. • **relative**—Indicates the relative metric mode; you can enter a positive, negative, or zero value. • *value*—Metric that the IGP enhanced SPF calculation uses. The relative value can be from -10 to 10.

Note Even though the value for a relative metric can be from -10 to +10, configuring a tunnel metric with a negative value is considered a misconfiguration. If the metric to the tunnel tailend appears to be 4 from the routing table, then the cost to the tunnel tailend router is actually 3 because 1 is added to the cost for getting to the loopback address. In this instance, the lowest value that you can configure for the relative metric is -3.

Note Alternatively, static routing could be used instead of autoroute to make the TE or DS-TE tunnels visible for routing.

The following example shows how to configure Multiprotocol Label Switching (MPLS) Traffic Engineering (TE) Class-Based Tunnel Selection (CBTS). Tunnel1, Tunnel2, and Tunnel3 are member tunnels, and Tunnel4 is the master tunnel.

```
Router> enable
Router# configure terminal
Router(config)# interface tunnel1
Router(config-if)# ip unnumbered loopback0
Router(config-if)# tunnel destination 24.1.1.1
Router(config-if)# tunnel mode mpls traffic-eng
Router(config-if)# tunnel mpls traffic-eng bandwidth sub-pool 30000
Router(config-if)# tunnel mpls traffic-eng exp 5
Router(config-if)# exit

Router(config)# interface tunnel2
Router(config-if)# ip unnumbered loopback0
Router(config-if)# tunnel destination 24.1.1.1
Router(config-if)# tunnel mode mpls traffic-eng
Router(config-if)# tunnel mpls traffic-eng bandwidth 50000
Router(config-if)# tunnel mpls traffic-eng exp 3 4
Router(config-if)# exit

Router(config)# interface tunnel3
Router(config-if)# ip unnumbered loopback0
Router(config-if)# tunnel destination 24.1.1.1
Router(config-if)# tunnel mode mpls traffic-eng
Router(config-if)# tunnel mpls traffic-eng bandwidth 10000
Router(config-if)# tunnel mpls traffic-eng exp default
Router(config-if)# exit

Router(config)# interface tunnel4
Router(config-if)# ip unnumbered loopback0
Router(config-if)# tunnel destination 24.1.1.1
Router(config-if)# tunnel mode mpls traffic-eng
Router(config-if)# tunnel mpls traffic-eng exp-bundle master
Router(config-if)# tunnel mpls traffic-eng exp-bundle member tunnel1
Router(config-if)# tunnel mpls traffic-eng exp-bundle member tunnel2
Router(config-if)# tunnel mpls traffic-eng exp-bundle member tunnel3
Router(config-if)# tunnel mpls traffic-eng autoroute announce
```

Verifying the MPLS Configuration

The following **show** commands can be used to verify that the MPLS TE or DS-TE tunnels are operating and announced to the IGP. The commands are all entered in privileged EXEC configuration mode.

Command	Purpose
show mpls traffic-eng topology {*A.B.C.D* | **igp-id** {**isis** *nsap-address* | **ospf** *A.B.C.D*} [**brief**]}	Shows the MPLS traffic engineering global topology as currently known at this node. • *A.B.C.D*—Specifies the node by the IP address (router identifier to interface address). • **igp-id**—Specifies the node by IGP router identifier. • **isis** *nsap-address*—Specifies the node by router identification (*nsap-address*) if you are using Integrated Intermediate System-to-Intermediate System (IS-IS). • **ospf** *A.B.C.D*—Specifies the node by router identifier if you are using Open Shortest Path First (OSPF). • **brief**—Provides a less-detailed version of the topology.
show mpls traffic-eng exp	Displays EXP mapping.
show ip cef [*type number*] [**detail**]	Displays entries in the forwarding information base (FIB) or displays a summary of the FIB. • *type number*—Identifies the interface type and number for which to display FIB entries. • **detail**—Displays detailed FIB entry information.
show mpls forwarding-table [*network* {*mask* | *length*} [**detail**]]	Displays the contents of the MPLS label forwarding information base (LFIB). • *network*—Identifies the destination network number. • *mask*—Identifies the network mask to be used with the specified network. • *length*—Identifies the number of bits in the destination mask. • **detail**—Displays information in long form (includes length of encapsulation, length of MAC string, maximum transmission unit [MTU], and all labels).
show mpls traffic-eng autoroute	Displays tunnels that are announced to the Interior Gateway Protocol (IGP).

The **show mpls traffic-eng topology** command output displays the MPLS TE global topology:

```
Router# show mpls traffic-eng topology 10.0.0.1

IGP Id: 10.0.0.1, MPLS TE Id:10.0.0.1 Router Node  (ospf 10  area 0) id 1
link[0]: Broadcast, DR: 180.0.1.2, nbr_node_id:6, gen:18
      frag_id 0, Intf Address:180.0.1.1
      TE metric:1, IGP metric:1, attribute_flags:0x0
      SRLGs: None
      physical_bw: 100000 (kbps), max_reservable_bw_global: 1000 (kbps)
      max_reservable_bw_sub: 0 (kbps)
```

```
                          Global Pool       Sub Pool
              Total Allocated   Reservable        Reservable
              BW (kbps)         BW (kbps)         BW (kbps)
                  ---------------   -----------       ----------
            bw[0]:             0             1000               0
            bw[1]:             0             1000               0
            bw[2]:             0             1000               0
            bw[3]:             0             1000               0
            bw[4]:             0             1000               0
            bw[5]:             0             1000               0
            bw[6]:             0             1000               0
            bw[7]:           100              900               0

link[1]: Broadcast, DR: 180.0.2.2, nbr_node_id:7, gen:19
      frag_id 1, Intf Address:180.0.2.1
      TE metric:1, IGP metric:1, attribute_flags:0x0
      SRLGs: None
      physical_bw: 100000 (kbps), max_reservable_bw_global: 1000 (kbps)
          max_reservable_bw_sub: 0 (kbps)
                              Global Pool       Sub Pool
                  Total Allocated   Reservable        Reservable
                  BW (kbps)         BW (kbps)         BW (kbps)
                  ---------------   -----------       ----------
        bw[0]:             0             1000               0
        bw[1]:             0             1000               0
        bw[2]:             0             1000               0
        bw[3]:             0             1000               0
        bw[4]:             0             1000               0
        bw[5]:             0             1000               0
        bw[6]:             0             1000               0
        bw[7]:             0             1000               0
```

The **show mpls traffic-eng exp** command output displays EXP mapping information about a tunnel:

```
Router# show mpls traffic-eng exp

Destination: 10.0.0.9
    Master:Tunnel10Status: IP

    Members: StatusConf EXPActual EXP
    Tunnel1UP/ACTIVE55
    Tunnel2UP/ACTIVEdefault0 1 2 3 4 6 7
    Tunnel3UP/INACTIVE(T)2
    Tunnel4DOWN3
    Tunnel5UP/ACTIVE(NE)

(T)=Tailend is different to master
(NE)=There is no exp value configured on this tunnel.
```

The **show ip cef detail** command output displays detailed FIB entry information for a tunnel:

```
Router# show ip cef tunnel1 detail

IP CEF with switching (Table Version 46), flags=0x0
31 routes, 0 reresolve, 0 unresolved (0 old, 0 new), peak 2
2 instant recursive resolutions, 0 used background process
8 load sharing elements, 8 references
6 in-place/0 aborted modifications
34696 bytes allocated to the FIB table data structures
universal per-destination load sharing algorithm, id 9EDD49E1
1(0) CEF resets
    Resolution Timer: Exponential (currently 1s, peak 1s)
    Tree summary:
    8-8-8-8 stride pattern
```

```
    short mask protection disabled
31 leaves, 23 nodes using 26428 bytes
Table epoch: 0 (31 entries at this epoch)
Adjacency Table has 13 adjacencies
10.0.0.9/32, version 45, epoch 0, per-destination sharing
0 packets, 0 bytes
tag information set, all rewrites inherited
local tag: tunnel head
via 0.0.0.0, Tunnel1, 0 dependencies
traffic share 1
next hop 0.0.0.0, Tunnel1
valid adjacency
tag rewrite with Tu1, point2point, tags imposed {12304}
0 packets, 0 bytes switched through the prefix
tmstats: external 0 packets, 0 bytes
internal 0 packets, 0 bytes
```

The **show mpls forwarding-table detail** command output displays detailed information from the MPLS LFIB:

```
Router# show mpls forwarding 10.0.0.9 detail

Local  Outgoing    Prefix            Bytes tag  Outgoing   Next Hop
tag    tag or VC   or Tunnel Id      switched   interface
Tun hd Untagged    10.0.0.9/32       0          Tu1        point2point
    MAC/Encaps=14/18, MRU=1500, Tag Stack{12304}, via Fa6/0
    00027D884000000ED70178A88847 03010000
    No output feature configured
Per-exp selection: 1
Untagged    10.0.0.9/32       0          Tu2        point2point
    MAC/Encaps=14/18, MRU=1500, Tag Stack{12305}, via Fa6/1
    00027D884001000ED70178A98847 03011000
    No output feature configured
Per-exp selection: 2  3
Untagged    10.0.0.9/32       0          Tu3        point2point
    MAC/Encaps=14/18, MRU=1500, Tag Stack{12306}, via Fa6/1
    00027D884001000ED70178A98847 03012000
    No output feature configured
Per-exp selection: 4  5
Untagged    10.0.0.9/32       0          Tu4        point2point
    MAC/Encaps=14/18, MRU=1500, Tag Stack{12307}, via Fa6/1
    00027D884001000ED70178A98847 03013000
    No output feature configured
Per-exp selection: 0  6  7
```

The **show mpls traffic-eng autoroute** command output displays tunnels that are announced to the Interior Gateway Protocol (IGP).

```
Router# show mpls traffic-eng autoroute

MPLS TE autorouting enabled
destination 10.0.0.9, area ospf 10  area 0, has 4 tunnels
Tunnel1     (load balancing metric 20000000, nexthop 10.0.0.9)
(flags: Announce)
Tunnel2     (load balancing metric 20000000, nexthop 10.0.0.9)
(flags: Announce)
Tunnel3     (load balancing metric 20000000, nexthop 10.0.0.9)
(flags: Announce)
Tunnel4     (load balancing metric 20000000, nexthop 10.0.0.9)
(flags: Announce)
```

Configuring IPoDWDM

IPoDWDM-Capable ES+ Line Cards

Dense wavelength-division multiplexing (IPoDWDM) is supported on these ES+ line cards:

- 76-ES+XT-2TG3CXL
- 76-ES+XT-4TG3CXL

WAN PHY and OTN Support on ES+ Line Cards

WAN PHY and OTN Overview

ES+ line card ports support the Optical Transport Network (OTN) and Wide Area Network (WAN) PHY.

This feature provides the software functionality to support OTN and WAN PHY on ES+ line cards.

WAN PHY leverages 10 Gig SONET infrastructure and accesses WAN facilities using:

- Dark Fiber
- Dark Wavelengths
- SONET TDM Networks

This feature provides low cost optic solutions required for short distances networks that implement store and forward network design requiring no optical amplifiers.

The OTN is based on the Optical Transport Hierarchy (OTH) developed by ITU. The OTN is based on the network architecture defined in ITU G.872 "Architecture for the Optical Transport Network (OTN)". The G.872 standard defines an architecture composed of the Optical Channel (OCh), Optical Multiplex Section (OMS), and Optical Transmission Section (OTS). The use of digitally framed signal with digital overhead for optical channel enables you to implement the management requirements of OCh. It also allows the use of Forward Error Correction (FEC) system to improve the system performance. The two new digital layer networks introduced to implement this feature are ODU and OTU.

OTN architecture (ITU-T G.872 standard) defines two interface classes:

- Inter-domain interface (IrDI): The OTN IrDI interface class defines the interface (with the 3Rs [Reamplification, Reshaping and Retiming] processing) at each end of the operator interface. the operator interface can also be the interface between different vendors within the same operator
- Intra-domain interface (IaDI): The IaDI interface class defines the interface within an operator or a vendor domain.

OTN has the following advantages:

- Stronger forward error correction
- More levels of Tandem Connection Monitoring (TCM)
- Transparent transport of client signals
- Switching scalability

Restrictions and Usage Guidelines

When configuring the WAN PHY / OTN support on ES+ line cards, follow these restrictions and usage guidelines:

- The distances between the two switching equipments using the WAN PHY and the DWDM facility depends on the XFP used. Refer the data sheets of relevant XFP.
- The MAC address is common for WAN PHY and LAN PHY. The WAN PHY operates at a rate compatible with the payload rate of OC-192c/VC-464c.

Configuring ITU-T G.709 Transport Modes

Use the **transport-mode** command in interface configuration mode to configure LAN, WAN, and OTN transport modes. The **transport-mode** command **otn** option has the **bit-transparent** sub-option, using which bit transparent mapping into OPU1e or OPU2e can be configured.

Note The hardware combination of Cisco-INTEL OC192 + 10GBASE-L XFP is not supported because of bit rate incompatibility between INTEL XFP and OTN for the following transport mode configurations:

- opu1e - 10GBASE-R over OPU1e without fixed stuffing (11.0491Gb/s)
- opu2e - 10GBASE-R over OPU2e with fixed stuffing (11.0957Gb/s)

	Command or Action	Purpose
Step 1	`Router> enable`	Enables privileged EXEC mode (enter your password if prompted).
Step 2	`Router# configure terminal`	Enters global configuration mode.
Step 3	`Router(config)# interface tengigabitethernet` *slot/port*	Specifies the Ten Gigabit Ethernet interface to configure.
Step 4	`Router(config-if)# transport-mode {lan | wan | otn bit-transparent {opu1e | opu2e}}`	Configures the transport mode.

DWDM Provisioning

All DWDM provisioning configurations take place on the controller. To configure a DWDM controller, use the **controller dwdm** command in global configuration mode.

The g709 configuration commands can be used only when the controller is in the shutdown state. Use the **no shutdown** command after configuring the parameters, to remove the controller from shutdown state and to enable the controller to move to up state.

	Command or Action	Purpose
Step 1	`Router> enable`	Enables privileged EXEC mode (enter your password if prompted).
Step 2	`Router# configure terminal`	Enters global configuration mode.
Step 3	`Router(config)# controller dwdm slot/port`	Configures the DWDM controller.

The following are examples of IP over DWDM commands:

```
Router# show run int tengigabitethernet 2/3
Building configuration...

Current configuration : 96 bytes
!
interface TenGigabitEthernet2/3
 ip address 11.11.11.2 255.255.255.0
 transport-mode otn bit-transparent opu2e
end

Router# show controller dwdm 2/3
G709 Information:

Controller dwdm 3/1, is down (shutdown)

Transport mode LAN (10GBASE-R, 10.3125Gb/s)

TAS state is : OOS
Description: connected to a ginsu LC
G709 status : Disabled

OTU
LOS = 18          LOF = 0           LOM = 0
AIS = 0           BDI = 1           BIP = 14504
TIM = 0           IAE = 0           BEI = 2289

ODU
AIS = 0           BDI = 0           TIM = 0
OCI = 0           LCK = 0           PTIM = 0
BIP = 14500       BEI = 2266

FEC Mode: FEC
EC(current second) = 0
EC = 31361        UC = 56318597


        pre-FEC BER < 9.00E-11
        Q > 6.45        Q Margin > 7.52  DBQ
Detected Alarms: NONE
Asserted Alarms: NONE
Detected Alerts: NONE
Asserted Alerts: NONE
Alarm reporting enabled for: LOS LOF LOM OTU-AIS OTU-IAE OTU-BDI OTU-TIM ODU-AIS ODU-OCI
ODU-LCK ODU-BDI ODU-PTIM ODU-TIM ODU-BIP Alert reporting enabled for: OTU-SM-TCA
ODU-SD-BER ODU-SF-BER ODU-PM-TCA BER thresholds: ODU-SF = 10e-3  ODU-SD = 10e-6 TCA
thresholds: SM = 10e-3  PM = 10e-3

OTU TTI Sent     String ASCII: This_is_a_static_string
OTU TTI Received String ASCII:
OTU TTI Received String HEX  : 00000000000000000000000000000000000000000000000000
                               00000000000000000000000000000000000000000000000000
```

```
                                00000000000000000000000000000000 OTU TTI Expected String
ASCII: This_is_a_static_string

ODU TTI Sent     String ASCII: This_is_a_static_string
ODU TTI Received String ASCII:
ODU TTI Received String HEX  : 00000000000000000000000000000000000000000000000000000000
                                00000000000000000000000000000000000000000000000000000000
                                00000000000000000000000000000000 ODU TTI Expected String
ASCII: This_is_a_static_string

Optics Information:

optics type: DWDM XFP Tunable
Wavelength: C-band, channel 10, 1558.17 nm, 192.40 THz Transceiver Rx optical power  =
-40.0 dBm
Transceiver Tx power        =  1.5 dBm
TX Laser current bias       = 20988 uAmps

Virtual Link Info:

 Adjacency info: This_is_a_static_string


C7600 Node ID :

        0 :26:B :28:68:80


Connectivity Info:

         Network Connection ID : This_is_a_static_string


Network SRLG values:


         Set 1:  6142   19113   14477   26689   4989   31230
         Set 2:  14967   7234   29164   19852   15452   17460
         Set 3:  14852   28561   6364   12832   21486   14312
         Set 4:  30337   19184   28532   15403   21048   27105
         Set 5:  18102   24607   16426   14253   21500   21952
         Set 6:  13523   17545   7863   538   5251   18205
         Set 7:  22331   27781   17862   26935   10028   16539
         Set 8:  865   29015   7144   20299   27504   2190
         Set 9:  13470   7222   8500   6988   18852   20882
         Set 10:  21512   702   14117   1870   19304   13075
         Set 11:  11919   26281   1898   18454   9948   15302
         Set 12:  24263   24747   5275   29138   17325   19226
         Set 13:  10917   18739   16263   20739   13147   18471
         Set 14:  1126   24967   26662   16266   32124   32739
         Set 15:  20342   29828   7591   18968   2421   24934
         Set 16:  3366   27109   22805   3591   7227   9339

Router# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# int tengigabitethernet 2/3
Router(config-if)# transport-mode ?
  lan  10GBASE-R LAN pass-through (10.3125Gb/s)
  otn  10GE over Optical Transport Network (G.709)
  wan  10GBASE-W WAN SONET/SDH (9.95328Gb/s)

Router(config-if)# transport-mode otn ?
  bit-transparent  10GBASE-R transparently mapped into OTU-2
```

```
Router(config-if)# transport-mode otn bit-transparent  ?
  opu1e  10GBASE-R over OPU1e without fixed stuffing (11.0491Gb/s)
  opu2e  10GBASE-R over OPU2e with fixed stuffing (11.0957Gb/s)


Router(config-if)# transport-mode otn bit-transparent opu2e
Router(config-if)# end
Router# show int tengigabitethernet2/3
TenGigabitEthernet2/3 is up, line protocol is up (connected)
  Hardware is X40G 10Gb 802.3, address is 00d0.03e2.1c00 (bia 00d0.03e2.1c00)
  Internet address is 11.11.11.1/24
  MTU 1500 bytes, BW 10000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 10Gb/s, clock source internal
  Transport mode OTN (10GBASE-R over OPU2e with fixed stuffing, 11.0957Gb/s)
  input flow-control is off, output flow-control is off
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:03, output 00:00:03, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
  L2 Switched: ucast: 0 pkt, 0 bytes - mcast: 2360 pkt, 221372 bytes
  L3 in Switched: ucast: 0 pkt, 0 bytes - mcast: 0 pkt, 0 bytes mcast
  L3 out Switched: ucast: 0 pkt, 0 bytes mcast: 0 pkt, 0 bytes
     2392 packets input, 223718 bytes, 0 no buffer
     Received 2477 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 0 multicast, 0 pause input
     0 input packets with dribble condition detected
     2477 packets output, 229905 bytes, 0 underruns
     0 output errors, 0 collisions, 13 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 pause output
     0 output buffer failures, 0 output buffers swapped out

Router#
Router# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# controller dwdm 2/3
Router(config-controller)# ?
Controller configuration commands:
  default      Set a command to its defaults
  description  Controller specific description
  exit         Exit from controller configuration mode
  g709         Configure G709 parameters
  help         Description of the interactive help system
  no           Negate a command or set its defaults
  shutdown     Configure dwdm controller processing

Router(config-controller)# g709 ?
fec  Configure FEC mode
odu  Configure odu parameters
otu  Configure otu parameters
tti-processing Configure Trail Trace Identifier  processing

Router(config-controller)# g709 fec ?
disable   Disable FEC
enhanced  Enhanced FEC mode
```

```
standard  Standard FEC mode

Router(config-controller)# g709 odu ?
overhead   Configure ODU overhead
report     Configure odu alarm reporting
threshold  Configure odu threshold

Router(config-controller)#g709 odu overhead ?
tti  Configure ODU Trail Trace Identifier buffer

Router(config-controller)#g709 odu overhead tti ?
expected   Set expected TTI
sent       Set transmit TTI

Router(config-controller)#g709 odu overhead tti expected ?
ascii  Enter ASCII string
hex    Enter hex string- Length should be even number

Router(config-controller)#g709 odu overhead tti expected ascii ?
    WORD  LINE  ASCII text (Max 64 characters)

Router(config-controller)#g709 odu overhead tti expected hex ?
    Hex-data  LINE  Hex nibbles (Max 128- The string length should
              be an even number)
Router(config-controller)#g709 odu overhead tti sent ?
ascii  Enter ASCII string
hex    Enter hex string- Length should be even number

Router(config-controller)#g709 odu overhead tti sent ascii ?
WORD  LINE ASCII text (Max 64 characters)

Router(config-controller)#g709 odu overhead tti sent hex ?
Hex-data  LINE  Hex nibbles (Max 128- The string length should
            be an even number)
Router(config-controller)# g709 odu report ?
ais     Set Alarm Indication Signal reporting status
bdi     Set Backward Defect Indication reporting status
lck     Set Upstream Connection Locked reporting status
oci     Set Open Connection Indication reporting status
pm-tca  Set Path Monitoring BER TCA reporting status
ptim    Set Payload Type Identifier Mismatch reporting status
sd-ber  Set SM BER in excess of SD threshold reporting status
sf-ber  Set SM BER in excess of SF threshold reporting status
tim     Set Trace Identifier Mismatch reporting status

Router(config-controller)# g709 odu threshold ?
pm-tca  Set Path Monitoring Threshold Crossing Alert threshold
sd-ber  Set Signal Degrade BER threshold
sf-ber  Set Signal Failure BER threshold

Router(config-controller)# g709 odu threshold pm-tca ?
<3-9>  Bit Error Rate (10 to the minus n) (default 3)
<cr>

Router(config-controller)# g709 odu threshold sd-ber ?
<3-9>  Bit Error Rate (10 to the minus n) (default 6)
<cr>

Router(config-controller)# g709 odu threshold sf-ber ?
<3-9>  Bit Error Rate (10 to the minus n) (default 3)
<cr>
Router(config-controller)# g709 otu ?
    overhead   Configure OTU overhead
    report     Configure otu alarm reporting
```

```
    threshold  Configure otu threshold

Router(config-controller)#g709 otu overhead ?
tti  Configure OTU Trail Trace Identifier buffer

Router(config-controller)#g709 otu overhead tti ?
expected   Set expected TTI
sent       Set transmit TTI

Router(config-controller)#g709 otu overhead tti expected ?
ascii  Enter ASCII string
hex    Enter hex string- Length should be even number

Router(config-controller)#g709 otu overhead tti expected ascii ?
    WORD  LINE  ASCII text (Max 64 characters)

Router(config-controller)#g709 otu overhead tti expected hex ?
    Hex-data  LINE  Hex nibbles (Max 128- The string length should be an
            even number)

Router(config-controller)#g709 otu overhead tti sent ?
ascii  Enter ASCII string
hex    Enter hex string- Length should be even number

Router(config-controller)#g709 otu overhead tti sent ascii ?
WORD  LINE ASCII text (Max 64 characters)

Router(config-controller)#g709 otu overhead tti sent hex ?
Hex-data  LINE  Hex nibbles (Max 128- The string length should be an
            even number)

Router(config-controller)# g709 otu report ?
  ais     Set Alarm Indication Signal reporting status
  bdi     Set Backward Defect Indication reporting status
  iae     Set Incoming Alignment Error reporting status
  lof     Set OTU Loss of Frame reporting status
  lom     Set Loss of Multiple Frame reporting status
  los     Set Loss of Signal reporting status
  sm-tca  Set Section Monitoring BER TCA reporting status
  tim     Set Trace Identifier Mismatch reporting status

Router(config-controller)# g709 otu threshold ?
  sm-tca  Set Section Monitoring Threshold Crossing Alert threshold

Router(config-controller)# g709 otu threshold sm-tca ?
  <3-9>  Bit Error Rate (10 to the minus n) (default 3)
  <cr>
```

Enabling OTN Mode Alarms Assertion

By default, all the OTN mode alarms are enabled. To control OTN alarms, disable all the alarms and enable the specific alarms by performing the following steps. Standard FEC is the default FEC mode. Use the **show controller** command to verify the alarm status and FEC mode. Perform the steps detailed in the section to enable OTN mode alarm assertion. Configure same transport mode or FEC mode on both the routers. The FEC modes, standard and disable, are compatible with each other.

	Command or Action	Purpose
Step 1	`Router> enable`	Enables privileged EXEC mode (enter your password if prompted).
Step 2	`Router# configure terminal`	Enters global configuration mode.
Step 3	`Router(config)# controller dwdm slot/port`	Configures the DWDM controller.
Step 4	`Router(config-controller)# shutdown`	Shuts down the DWDM controller.
Step 5	`Router(config-controller)# {g709 | no g709} fec {disable | standard | enhanced}`	Configures the FEC modes
Step 6	`Router(config-controller)# {g709 | no g709} otu report {ais | bdi | iae | lof | los | sm-tca | tim}`	Specifies the supported otu alarms and configures the otu threshold. By default, all alarms are reported.
Step 7	`Router(config-controller)# {g709 | no g709} odu report { ais | bdi | lck | oci | pm-tca | ptim | sd-ber | sf-ber | tim }`	Specifies the supported odu alarms and configures the odu threshold. By default, all the alarms are reported.
Step 8	`Router(config-controller)# {g709 | no g709} otu threshold sm-tca val`	Set the threshold value to detect section monitoring signal degrade or signal failure alerts.
Step 9	`Router(config-controller)# {g709 | no g709} odu threshold {pm-tca | sd-ber | sf-ber} t_value`	Sets the ber threshold limit to t_value power of ten.
Step 10	`Router(config-controller)# {g709 | no g709} otu overhead tti {expected | sent} {ascii | hex} tti-string`	Specifies the trail trace identifier for otu level.
Step 11	`Router(config-controller)# {g709 | no g709} odu overhead tti {expected | sent} {ascii | hex} tti-string`	Specifies the trail trace identifier for odu level.
Step 12	`Router(config-controller)# no shutdown`	Sets the controller to no shutdown mode.
Step 13	`Router(config-controller)# end`	Ends the session.

Note You need to shutdown the interface using **shutdown** command before changing the FEC mode to EFEC.

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# controller dwdm 4/21
Router(config-controller)# shutdown
Router(config-controller)# g709 fec enhanced
Router(config-controller)# g709 otu report los
Router(config-controller)# no g709 otu report lof
Router(config-controller)# no g709 otu threshold sm-tca
Router(config-controller)# g709 odu threshold sd-ber 3
Router(config-controller)# no shutdown
Router(config-controller)# end
```

Use the **show controllers** command to verify the configuration for alarm assertion.

```
Router# show controllers dwdm 4/21
Controller dwdm 4/2, is up (no shutdown)

TAS state is : IS
G709 status : Enabled

OTU
        LOS = 1           LOF = 0           LOM = 0
```

```
        AIS = 0           BDI = 1           BIP = 0
        TIM = 0           IAE = 0           BEI = 0

ODU
        AIS = 0           BDI = 0           TIM = 0
        OCI = 0           LCK = 0           PTIM = 0
        BIP = 0           BEI = 0

FEC Mode: FEC
        EC(current second) = 0
        EC = 0            UC = 0
    pre-FEC BER < 9.00E-11
        Q > 6.45        Q Margin > 7.52  DBQ
Detected Alarms: NONE
Asserted Alarms: NONE
Detected Alerts: NONE
Asserted Alerts: NONE
Alarm reporting enabled for: LOS LOF LOM OTU-AIS OTU-IAE OTU-BDI ODU-AIS ODU-OCI ODU-LCK
ODU-BDI ODU-PTIM ODU-BIP Alert reporting enabled for: OTU-SM-TCA ODU-SD-BER ODU-SF-BER
ODU-PM-TCA BER thresholds: ODU-SF = 10e-3  ODU-SD = 10e-6 TCA thresholds: SM = 10e-3  PM =
10e-3

OTU TTI Sent     String ASCII: Tx TTI Not Configured
OTU TTI Received String ASCII:
OTU TTI Received String HEX  : 00000000000000000000000000000000000000000000000000
                               00000000000000000000000000000000000000000000000000
                               000000000000000000000000000000O OTU TTI Expected String
ASCII: Exp TTI Not Configured

ODU TTI Sent     String ASCII: Tx TTI Not Configured
ODU TTI Received String ASCII:
ODU TTI Received String HEX  : 00000000000000000000000000000000000000000000000000
                               00000000000000000000000000000000000000000000000000
                               0000000000000000000000000000000 ODU TTI Expected String
ASCII: Exp TTI Not Configured
```

Upgrading Field-Programmable Devices

Field-programmable devices (FPDs) support separate upgrades. This chapter includes the following sections:

Overview of FPD Images and Packages

An FPD image package is used to upgrade FPD images. Whenever a Cisco IOS image is released that supports the ES+ line cards, a companion FPD image package is also released for that Cisco IOS software release. The FPD image package is available from Cisco.com and is accessible from the Cisco Software Center page where you also go to download your Cisco IOS software image.

With ES+ line cards, when you upgrade the Cisco IOS image, you should download the FPD image package file before booting the router using the new Cisco IOS release. If the ES+ line cards requires an FPD upgrade and the Cisco IOS image is unable to locate an FPD image package, the system messages will indicate that the FPD image is incompatible and you will need to go to the Cisco Software Center on Cisco.com to download the FPD image package for your Cisco IOS software release. An FPD incompatibility on an ES+ line cards disables all interfaces on that ES+ line cards until the incompatibility is addressed.

ES+ line cards have these FPD-upgradeable components:

- Base board
  - ROMMON
  - I/O field-programmable Gate Array (FPGA)
  - Selene FPGA
- Link daughter card with a link FPGA
- DFC
  - Packet Engine FPGA
  - K' (k prime) FPGA

Note The FPD automatic upgrade feature only searches for the FPD image package file that is the same version number as the Cisco IOS release being used by the system. Ensure that the FPD image package file on your system is compatible with your Cisco IOS release and do not change the name of the FPD image package file.

FPD Quick Upgrade

This section provides information if you want to upgrade ES+ line card FPDs. These instructions are not always feasible for operating network environments and are not the only methods available for upgrading FPDs. This section addresses the following topics:

- FPD Quick Upgrade Before Upgrading your Cisco IOS Release (Recommended), page A-50
- FPD Quick Upgrade After Upgrading your Cisco IOS Release, page A-51

FPD Quick Upgrade Before Upgrading your Cisco IOS Release (Recommended)

Step 1 When getting your Cisco IOS image, download the FPD image package for the Cisco IOS release that you are upgrading to any Flash disk on your router before booting the new version of Cisco IOS. The FPD image package can be retrieved from the same site where you went to get your Cisco IOS image. Do not change the name of the FPD image package.

Step 2 Boot using the new version of Cisco IOS. When the new Cisco IOS boots, it by default searches for the FPD image package in the router flash file systems and the FPD images will be updated automatically as part of the IOS boot process.

FPD Quick Upgrade After Upgrading your Cisco IOS Release

Step 1 An FPD upgrade is not always necessary after Cisco IOS is reloaded. If you have already reloaded your Cisco IOS, enter the **show hw-module all fpd** command to see if all system FPDs are compatible. If the FPDs are compatible, no further action is necessary. If at least one FPD needs an upgrade, proceed to Step 2.

Step 2 Go to the cisco.com site where you downloaded your specific Cisco IOS software and locate the FPD image package.

Step 3 Download this FPD image package to a Flash disk on your router. Do not change the name of the FPD image package.

Do not change any FPD-related settings on your system (if **upgrade fpd auto** or **upgrade fpd path** has been changed, change the settings back to the default settings using the **no** form of the command). Reboot your Cisco IOS release software. When the new Cisco IOS boots, it by default searches for the FPD image package in the Flash file systems and the FPD images will be updated automatically as part of the IOS boot process.

Upgrading FPD Images

This section documents some of the common scenarios where FPD image updates are necessary. It discusses the following scenarios:

- Migrating to a Newer Cisco IOS Release, page A-51
- Upgrading FPD Images in a Non-Production System, page A-52

Migrating to a Newer Cisco IOS Release

This section discusses the following topics:

- Upgrading FPD Images Before Upgrading Cisco IOS Release (Recommended), page A-51
- Upgrade FPD Images after Upgrading the New Cisco IOS Release, page A-52

Upgrading FPD Images Before Upgrading Cisco IOS Release (Recommended)

If you are still running your old Cisco IOS Release but are preparing to load a newer version of Cisco IOS, upgrade FPD for the new Cisco IOS Release. Placing the FPD image package for the IOS release that you are upgrading to before upgrading IOS is the recommended method for upgrading FPD because it is simple in addition to being fast. To perform this type of FPD upgrade, follow these steps:

Step 1 While still running the Cisco IOS release that will be upgraded, place the FPD image package for the new version of Cisco IOS onto one of your router's Flash file systems. You can locate the FPD image package for a specific IOS release on cisco.com from the same area where you download that Cisco IOS software image. The switch and ES+ line cards should continue to operate normally since this action will have no impact on the current FPDs.

Caution Do not change the filename of the FPD image package file. The Cisco IOS searches for the FPD image package file by filename, so the FPD image package file cannot be found if it has been renamed.

Step 2 Reboot your router using the new upgraded Cisco IOS image. As part of the bootup process, the router will search for the FPD image package. Since the default settings for the FPD image package search are to check for the FPD image package for the specific Cisco IOS Release in a Flash file system, the FPD image package will be located during the bootup procedure and all FPDs that required upgrades will be upgraded.

Step 3 When the router has booted, verify the upgrade was successful by entering the **show hw-module all fpd** command.

Upgrade FPD Images after Upgrading the New Cisco IOS Release

The following steps explain how to upgrade FPD images if you have already upgraded your Cisco IOS release but still need to upgrade your FPD images.

To perform an FPD upgrade after the new Cisco release has been booted, follow these steps:

Step 1 If you are unsure if your FPD images for your ES+ line cards are compatible, enter the **show hw-module all fpd** command to verify compatibility of all ES+ line cards. If all of your ES+ line cards are compatible, there is no reason to perform this upgrade.

Step 2 If an FPD upgrade is necessary, place the FPD image package for the new version of Cisco IOS onto the router's Flash Disk or on an accessible FTP or TFTP server. You can locate the FPD image package on cisco.com from the same area where you downloaded your Cisco IOS software image.

Step 3 Enter the **upgrade hw-module** [**slot** *slot-number*] *file-url* command. The *file-url* command should direct users to the location of the FPD image package.

If multiple ES+ line cards require upgrades, the different pieces of hardware will have to be updated individually.

Note With the new Cisco IOS release running, if the ES+ line cards are disabled or powered down due to any FPD upgrade errors, the only way to do an FPD upgrade is by reloading the line card using **hw-module reset** command (assuming that you have already copied the necessary FPD bundle file in to the file system).The **upgrade hw-module** command works only when the line card is in the UP state.

Step 4 Verify the upgrade was successful by entering the **show hw-module all fpd** command.

Upgrading FPD Images in a Non-Production System

Adding an ES+ line cards to a production system presents the possibility that the ES+ line cards may contain versions of FPD images that are incompatible with the Cisco IOS release currently running the router. In addition, the FPD upgrade operation can be a very CPU-intensive operation and therefore the upgrade operation may take more time when it is performed on a production system. The performance impact will vary depending on various factors, including network traffic load, the type of processing engine used, type of ES+ line cards, and the type of service configured. Use a non-production system to upgrade the ES+ line card FPD image.

Before beginning the upgrade, ensure:

- The spare system is running the same version of the Cisco IOS software release that the target production system is running.
- The automatic upgrade feature is enabled on the spare system (the automatic upgrade feature is enabled by default. It can also be enabled using the **upgrade fpd auto** command).

Use the following procedure to perform an upgrade on a spare system:

Step 1 Download the FPD image package file to the router's flash file system or TFTP or FTP server accessible by the spare system. In most cases, it is preferable to place the file in a Flash file system since the router, by default, searches for the FPD image package in the Flash file systems. If the Flash file systems are full, use the **upgrade fpd path** command to direct the router to search for the FPD image package in the proper location.

Step 2 Insert the ES+ line card into the spare system.

If an upgrade is required, the system will perform the necessary FPD image updates so that when this ES+ line card is inserted to the target production system it will not trigger an FPD upgrade operation there.

Step 3 Verify the upgrade was successful by entering the **show hw-module all fpd** command.

Step 4 Remove the ES+ line card from the spare system after the upgrade.

Step 5 Insert the ES+ line card into the target production system.

Verifying System Compatibility

If a spare system is not available to perform an upgrade, you can check for system compatibility by disabling the automatic upgrade feature before inserting the ES+ line card (the automatic upgrade feature is enabled by default. It can be disabled using the **no upgrade fpd auto** command).

- If the FPD images on the ES+ line card are compatible with the system, you will only need to re-enable the automatic upgrade feature (the automatic upgrade feature can be re-enabled using the **upgrade fpd auto** command).
- If the FPD images on the ES+ line card are not compatible with the system, the ES+ line card is disabled but will not impact system performance by attempting to perform an automatic upgrade.

Use the following procedure to check the FPD images on the ES+ line card for system compatibility:

Step 1 Disable the automatic upgrade feature using the **no upgrade fpd auto** global configuration command.

Step 2 Insert the ES+ line card into the system.

If the FPD images are compatible, the ES+ line card will operate successfully after bootup.

If the FPD images are not compatible, the ES+ line card is disabled. At this point we recommend that you wait for a scheduled maintenance when the system is offline to manually perform the FPD upgrade using one of the procedures outlined in the "Upgrading FPD Images" section on page A-51.

Step 3 Re-enable the automatic upgrade feature using the **upgrade fpd auto** global configuration command.

Optional FPD Procedures

This section provides information for optional FPD-related functions. None of the topics discussed in this section are necessary for completing FPD upgrades, but may be useful in some FPD-related scenarios. It covers the following topics:

Manually Upgrading ES+ Line Card FPD Images

To manually upgrade the current FPD version on an ES+ line card, use the following command:

```
Router# upgrade hw-module [slot slot-number] file file-url
```

In this example, *slot-number* is the slot where the ES+ line card is installed, *file-url* is the location and name of the FPD image package file.

Caution An image upgrade can require a long period of time to complete depending on the ES+ line card.

Upgrading FPD from an FTP or TFTP Server

The generally recommended method to perform an FPD image upgrade is to download the FPD image package to a Flash file system and use the FPD automatic upgrade. By default, the system searches the Flash file system for the FPD image package file when an FPD incompatibility is detected.

This default behavior of loading an FPD image from Flash can be changed using the **upgrade fpd path** global configuration command, which sets the path to search for the FPD image package file to a location other than the router's Flash file systems.

For large deployments where all the systems are being upgraded to a specific Cisco IOS software release, we recommend that the FPD image package file be placed on an FTP or TFTP server that is accessible to all the affected systems, and then use the **upgrade fpd path** global configuration command to configure the routers to look for the FPD image package file from the FTP or TFTP server prior to the reloading of the system with the new Cisco IOS release.

Note This approach can also be used if there is not enough disk space on the system Flash card to hold the FPD image package file.

To download an FPD image package file to an FTP or TFTP server, use the following procedure:

Step 1 Copy the FPD image package file to the FTP or TFTP server.

Step 2 From global configuration mode, use the **upgrade fpd path** command to instruct the router to locate the FPD image package file from the FTP or TFTP server location.

For example, enter one of the following global configuration commands from the target system's console:

```
Router(config)# upgrade fpd path tftp://my_tftpserver/fpd_pkg_dir/
```

or

```
Router(config)# upgrade fpd path ftp://login:password@my_ftpserver/fpd_pkg_dir/
```

Note The final "/" at the end of each of the above examples is required. If the path is specified without the trailing "/" character, the command will not work properly.

In these examples, *my_tftpserver* or *my_ftpserver* is the path to server name, *fpd_pkg_dir* is the directory on the TFTP server where the FPD image package is located, and *login:password* is your FTP login name and password.

Step 3 Make sure that the FPD automatic upgrade feature is enabled by examining the output of the **show running-config** command. (Look for the *upgrade fpd auto* configuration line in the output. If there are no upgrade commands in the output, then **upgrade fpd auto** is enabled because it is the default setting.) If automatic upgrades are disabled, use the **upgrade fpd auto** global configuration command to enable automatic FPD upgrades.

Step 4 Enter the **show upgrade fpd file** command to ensure your router is connecting properly to the default FPD image package. If you are able to generate output related to the FPD image package using this command, the upgrade should work properly.

Step 5 Save the configuration and reload the system with the new Cisco IOS release.

During the system startup after the reload, the necessary FPD image version check for all the ES+ line cards will be performed and any upgrade operation will occur automatically if an upgrade is required. In each upgrade operation, the system extracts the necessary FPD images to the ES+ line card from the FPD image package file located on the FTP or TFTP server.

Modifying the Default Path for the FPD Image Package File Location

By default, the Cisco IOS software looks for the FPD image package file on a Flash file system when performing an automatic FPD image upgrade.

Note Be sure there is enough space on one of your Flash file systems to accommodate the FPD image package file.

Alternatively, you can store an FPD image package file elsewhere. However, because the system looks on the Flash file systems by default, you need to change the FPD image package file location so that the system is directed to search an alternate location (such an FTP or TFTP server) that is accessible by the Cisco IOS software. Enter the **upgrade fpd path** *fpd-pkg-dir-url* global configuration command, where *fpd-pkg-dir-url* is the alternate location, to instruct the router to search for the FPD image package elsewhere.

When specifying the *fpd-pkg-dir-url*, be aware of the following:

- The *fpd-pkg-dir-url* is the path to the FPD image package, but do not include the FPD image package as part of *fpd-pkg-dir-url*. Enter:

  upgrade fpd path tftp://*mytftpserver***/***myname***/***myfpdpkgpath***/**

  The filename is not specified.

- The final "/" character in the *fpd-pkg-dir-url* is required.

If the **upgrade fpd path** global configuration command has not been entered to direct the router to locate an FPD image package file in an alternate location, the system searches the Flash file systems on the switch for the FPD image package file.

Failure to locate an FPD image package file when an upgrade is required will disable the ES+ line card. Because ES+ line cards will not come online until FPD is compatible, the ES+ line card will also be disabled if it requires an FPD upgrade and the automatic upgrade feature is disabled.

Displaying Current and Minimum Required FPD Image Versions

To display the current version of FPD images on the ES+ line cards installed on your router, use the **show hw-module** [*slot-number* | **all**] **fpd** command, where *slot-number* is the slot number where the ES+ line card is installed. Entering the **all** keyword shows information for hardware in all router slots.

The following examples show the output when using this **show** command.

The output display in this example shows that FPD versions on the ES+ line cards in the system meet the minimum requirements:

```
Router# show hw-module all fpd
```

This example shows the output when verifying the FPD for the ES+ line card in a specific slot:

```
Router# show hw-module slot 9 fpd
```

Displaying Information About the Default FPD Image Package

You can use the **show upgrade fpd package default** command to find out which ES+ line cards are supported with your current Cisco IOS release and which FPD image package you need for an upgrade.

```
Router# show upgrade fpd package default
```

FPD Image Upgrade Examples

This section provides examples of automatic and manual FPD image upgrades. It includes the following examples:

- Automatic FPD Image Upgrade Example, page A-56
- Manual FPD Image Upgrade Example, page A-57

Automatic FPD Image Upgrade Example

The following example uses the **upgrade fpd auto to do an automatic upgrade**.

```
Router# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# upgrade fpd ?
  auto  Auto upgrade all FPD images
  path  Set path to locate the FPD image package file for auto upgrade

Router(config)# upgrade fpd auto ?
  <cr>

Router(config)# upgrade fpd auto
Router(config)# exit
Router# show version
*Jun 18 10:27:00.078 sum08: %SYS-5-CONFIG_I: Configured from console by consoh ver
```

```
Cisco IOS Software, rsp72043_rp Software (rsp72043_rp-ADVENTERPRISEK9_DBG-M), Version
12.2(nightly.SR080616) NIGHTLY BUILD, synced to rainier
RAINIER_BASE_FOR_V122_33_SRA_THROTTLE
Copyright (c) 1986-2008 by Cisco Systems, Inc.
Compiled Tue 17-Jun-08 00:10 by cuotran

ROM: System Bootstrap, Version 12.2(33r)SRB3, RELEASE SOFTRouterRE (fc1)

 Router uptime is 22 hours, 29 minutes
Uptime for this control processor is 22 hours, 29 minutes
System returned to ROM by reload (SP by reload)
System image file is "disk0:rsp72043-adventerprisek9_dbg-mz.autobahn76_061608"
Last reload type: Normal Reload
```

Manual FPD Image Upgrade Example

In the following example, FPD for the ES+ line card in slot 8 is upgraded manually:

```
Router# upgrade hw-module slot 8 ?
  fpd  Field programmable device upgrade option
Router# upgrade hw-module slot 8 fpd ?
  file  Upgrade with field programmable device package/bundle file

Router# upgrade hw-module slot 8 fpd file c
Router# upgrade hw-module slot 8 fpd file d
*Jun 17 13:24:12.531 sum08: %FPD_MGMT-3-INCOMP_IMG_VER: Incompatible I/O FPGA (FPD ID=2)
image version detected for 7600-ES+40G3CXL card in slot 8. Detected version = 0.16,
minimum required version = 0.17. Current HW version = 0.118.
*Jun 17 13:24:12.531 sum08: %FPD_MGMT-3-INCOMP_IMG_VER: Incompatible 40x1G LinkFPGA (FPD
ID=6) image version detected for 7600-ES+40G card in slot-dc 8-2. Detected version = 0.14,
minimum required version = 0.15. Current HW version = 0.106.
*Jun 17 13:24:12.531 sum08: %FPD_MGMT-5-UPGRADE_ATTEMPT: Attempting to automatically
upgrade the FPD image(s) for 7600-ES+40G3CXL card in slot 8. Use 'show upgrade fpd
progress' command to view the upgrade progress ...
*Jun 17 13:24:12.547 sum08: %FPD_MGMT-6-BUNDLE_DOWNLOAD: Downloading FPD image bundle for
7600-ES+40G3CXL card in slot 8 ...i
Router#upgrade hw-module slot 8 fpd file disk
*Jun 17 16:24:12.551: %FABRIC_INTF_ASIC-DFC8-5-FABRICSYNC_DONE: Fabric ASIC 0 Channel 1:
Fabric sync done.
*Jun 17 16:24:12.575: %FABRIC_INTF_ASIC-DFC8-5-FABRICSYNC_DONE: Fabric ASIC 1 Channel 1:
Fabric sync done.
```

Troubleshooting

These sections describe techniques that you can use to troubleshoot the operation of ES+ line cards.

- Using the Cisco IOS Event Tracer to Troubleshoot Problems, page A-58
- Troubleshooting XFP Issues, page A-58
- Preparing for Online Insertion and Removal of ES+ Line Cards, page A-59

The first section provides information about basic interface troubleshooting. If you are having a problem with your XFP transceivers, use the steps in the "Using the Cisco IOS Event Tracer to Troubleshoot Problems" section to begin your investigation of a possible interface configuration problem.

Using the Cisco IOS Event Tracer to Troubleshoot Problems

Note The Event Tracer feature is intended for use as a software diagnostic tool and should be configured only under the direction of a Cisco Technical Assistance Center (TAC) representative.

The Event Tracer feature provides a binary trace facility for troubleshooting Cisco IOS software. This feature gives Cisco service representatives additional insight into the operation of the Cisco IOS software and can be useful in helping to diagnose problems in the unlikely event of an operating system malfunction or, in the case of redundant systems, Route Processor switch over.

Event tracing works by reading informational messages from specific Cisco IOS software subsystem components that have been pre-programmed to work with event tracing, and by logging messages from those components into system memory. Trace messages stored in memory can be displayed on the screen or saved to a file for later analysis.

For more information about using the Event Tracer feature, refer to the following URL:

http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_event_tracer.html

Troubleshooting XFP Issues

Use the following commands when troubleshooting XFP transceiver issues:

Command	Purpose
Router# **show interfaces** [*interface interface-number*] **capabilities** [**module** *number*]	Displays the interface capabilities for a module, an interface, or all interfaces.
Router# **show interfaces** [*interface interface-number*] **status** [**err-disabled** | **module** *number*]	Displays the interface status.
Router# **show interfaces** [*interface interface-number*] **transceiver** [**threshold violations**] [**detail** | {**module** *number*}]	Displays information about the optical transceivers that have digital optical monitoring (DOM) enabled
Router# **show idprom interface**	Displays IDPROMs for the transceiver plugged into the port.

Make sure the optics power rating are suitable for the link. For both ends of a link, check for "+", "++", "-", "--" in the output the following command to confirm that the power ratings are correct:

```
Router# show interface tengigabitethernet 2/1 transceiver detail
Transceiver monitoring is disabled for all interfaces.

ITU Channel not available (Wavelength not available),
Transceiver is internally calibrated.
mA: milliamperes, dBm: decibels (milliwatts), NA or N/A: not applicable.
++ : high alarm, +  : high warning, -  : low warning, -- : low alarm.
A2D readouts (if they differ), are reported in parentheses.
The threshold values are calibrated.

                            High Alarm  High Warn  Low Warn   Low Alarm
           Temperature         Threshold   Threshold  Threshold  Threshold
Port       (Celsius)          (Celsius)   (Celsius)  (Celsius)  (Celsius)
---------- ------------------  ----------  ---------  ---------  ---------
Te2/1        29.6                74.0        70.0         0.0       -4.0

                            High Alarm  High Warn  Low Warn   Low Alarm
```

```
            Voltage            Threshold   Threshold  Threshold  Threshold
Port        (Volts)            (Volts)     (Volts)    (Volts)    (Volts)
----------  ---------------    ----------  ---------  ---------  ---------
Te2/1        N/A                  N/A         N/A        N/A        N/A

                               High Alarm  High Warn  Low Warn   Low Alarm
            Current            Threshold   Threshold  Threshold  Threshold
Port        (milliamperes)     (mA)        (mA)       (mA)       (mA)
----------  -----------------  ----------  ---------  ---------  ---------
Te2/1        56.8          --    N/A        N/A        N/A       N/A

            Optical            High Alarm  High Warn  Low Warn   Low Alarm
            Transmit Power     Threshold   Threshold  Threshold  Threshold
Port        (dBm)              (dBm)       (dBm)      (dBm)      (dBm)
----------  -----------------  ----------  ---------  ---------  ---------
Te2/1         1.6                7.9         3.9        0.0       -4.0

            Optical            High Alarm  High Warn  Low Warn   Low Alarm
            Receive Power      Threshold   Threshold  Threshold  Threshold
Port        (dBm)              (dBm)       (dBm)      (dBm)      (dBm)
----------  -----------------  ----------  ---------  ---------  ---------
Te2/1        -1.2          ++    -3.0        -7.0       -24.0      -28.2
```

If there is an alarm or warning, verify the following:

- Both ends of a link must use the same tranceiver type.
- The tranceivers (LR, IR, ZR) must be appropriate for the length of the link.
- Use an attenuator to control the power ratings.

Preparing for Online Insertion and Removal of ES+ Line Cards

Online insertion and removal (OIR) supports ES+ line cards, in addition to each of the XFP transceivers.

You can remove an ES+ line card with its transceivers still intact, or you can remove an transceiver independently from the ES+ line card, leaving the ES+ line card installed.

This section includes the following topics on OIR support:

- Preparing for Online Removal of an ES+ Line Card, page A-59
- Verifying Deactivation and Activation of an ES+ Line Card, page A-60
- Deactivation and Activation Configuration Examples, page A-61

Preparing for Online Removal of an ES+ Line Card

To do an OIR, you can power down an ES+ line card (which automatically deactivates any installed optical transceivers) and remove the ES+ line card still intact.

Although graceful deactivation of an ES+ line card is preferred using the **no power enable module** command, the Cisco 7600 series router does support removal of the ES+ line card without deactivating it first. If you plan to remove an ES+ line card, you can deactivate the ES+ line card first, using the **no power enable module** global configuration command. When you deactivate an ES+ line card using this command, it automatically deactivates each of the optical transceivers that are installed in that ES+ line card. Therefore, it is not necessary to deactivate each of the optical transceivers prior to deactivating the ES+ line card.

Either a blank filler plate or a functional optical transceiver should reside in every subslot of an ES+ line card during normal operation.

Deactivating an ES+ Line Card

To deactivate an ES+ line card and its installed optical transceivers prior to removal of the line card, use the following command in global configuration mode:

Command	Purpose
`Router(config)# no power enable module slot`	Shuts down any installed interfaces, and deactivates the ES+ line card in the specified slot.

Reactivating an ES+ Line Card

When you deactivate an ES+ line card, whether or not you have performed an OIR, you must use the **power enable module** global configuration command to reactivate the ES+ line card.

If you did not issue a command to deactivate the optical transceivers installed in an ES+ line card, but you did deactivate the ES+ line card using the **no power enable module** command, then you do not need to reactivate the optical transceivers after an OIR of the ES+ line card. The installed optical transceivers automatically reactivate upon reactivation of the ES+ line card in the router.

For example, consider the case in which you remove an ES+ line card from the router to replace it with another ES+ line card. You reinstall the same optical transceivers into the new ES+ line card. When you enter the **power enable module** command on the router, the optical transceivers will automatically reactivate with the new ES+ line card.

To activate an ES+ line card and its installed optical transceivers after the ES+ line card has been deactivated, use the following command in global configuration mode:

Command	Purpose
`Router(config)# power enable module slot`	Activates the ES+ line card in the specified slot and its installed optical transceivers, where: • *slot*—Specifies the chassis slot number where the ES+ line card is installed.

Verifying Deactivation and Activation of an ES+ Line Card

To verify the deactivation of an ES+ line card, enter the **show module** command in privileged EXEC configuration mode. Observe the Status field associated with the ES+ line card that you want to verify.

The following example shows that the ES+ line card located in slot 10 is deactivated. This is indicated by its “PwrDown” status.

```
Router# show module 10
```

To verify activation and proper operation of an ES+ line card, enter the **show module** command and observe “Ok” in the Status field as shown in the following example:

```
Router# show module 10
```

Deactivation and Activation Configuration Examples

This section provides the following examples of deactivating and activating an ES+ line card and optical transceivers:

Deactivation of an ES+ Line Card Configuration Example

Deactivate an ES+ line card when you want to perform OIR of the ES+ line card. The following example deactivates the ES+ line card that is installed in slot 5 of the router, its optical transceivers, and all of the interfaces. The corresponding console messages are shown:

```
Router# configure terminal
Router(config)# no power enable module 5
1w4d: %OIR-6-REMCARD: Card removed from slot 5, interfaces disabled
1w4d: %C6KPWR-SP-4-DISABLED: power to module in slot 5 set off (admin request)
```

Activation of an ES+ Line Card Configuration Example

Activate an ES+ line card if you have previously deactivated it. If you did not deactivate the optical transceivers, the optical transceivers automatically reactivate with reactivation of the ES+ line card.

The following example activates the ES+ line card that is installed in slot 5 of the router, its optical transceivers, and all of the interfaces (as long as the **hw-module subslot shutdown** command was not issued to also deactivate the optical transceivers):

```
Router# configure terminal
Router(config)# power enable module 5

Notice that there are no corresponding console messages shown with activation. If you
re-enter the power enable module command, a message is displayed indicating that the
module is already enabled:

Router(config)# power enable module 5
% module is already enabled
```