Configuring QoS

This chapter provides information about configuring Quality of Service (QoS) on the Cisco 7600 Series Ethernet Services Plus (ES+) and Ethernet Services Plus T (ES+T) line card on the Cisco 7600 series router.

QoS on the Cisco 7600 Series Ethernet Services Plus line cards uses Layer 2 frame size.

With QoS enabled globally, cross bundling is not allowed between 6xxx cards and ES20 line cards, between 6xxx cards and ES+ line cards, and between ES20 and ES+ line cards.

When mls qos channel-consistency command is disabled, you can configure ports from cards belonging different family, as member-links of the same port-channel if QoS is not applied on service instances, sub-interfaces, service-groups, sessions, and main-interfaces of the port-channel or the member-links of the port-channel.


Before referring to any other QoS documentation for the platform or in the Cisco IOS software, use this chapter to determine Cisco 7600 Series ES+ line card specific QoS feature support and configuration guidelines.

The information provided in this chapter is applicable to both the ES+ and ES+T line cards unless specified otherwise.


This chapter includes the following sections:

- Supported Interfaces, page 7-3
- Mapping Between Bay and Ports, page 7-3
- QoS Functions, page 7-4
- Configuring QoS Features Using MQC, page 7-7
- Configuring Classification, page 7-8
- Configuring Policing, page 7-14
• Configuring Marking, page 7-23
• Configuring Shaping, page 7-27
• Configuring QoS Overhead Accounting for Shaping Parameters, page 7-31
• Configuring QoS Queue Scheduling, page 7-32
• Configuring PFC QoS on a Cisco 7600 Series Ethernet Services Plus Line Card, page 7-60
• Configuring Hierarchical QoS, page 7-61
• EVCS QoS Support, page 7-65
• QoS on Port-Channel Member-Link, page 7-68
• IPv6 - Hop by Hop Rate Limiter, page 7-77
• Service Group QoS Support on the Cisco 7600 Series Router, page 7-89
• Configuring Flexible Service Mapping Based on CoS and Ethertype, page 7-95
• Layer 2 and Layer 3 QoS ACL Classification for EVC, page 7-107
• Deny ACL QoS Classification, page 7-111
• Ingress HQoS for Port Channel Interfaces, page 7-116
• Troubleshooting QoS on a ES+ Line Card, page 7-121
Supported Interfaces

The Cisco 7600 Series ES+ line cards support QoS on the following interfaces:

- Main Layer 3 interface
- Layer 3 subinterface
- Switchport interfaces
- SVI interfaces
- Service instances
- Port-channel service instances

**Note**
Starting with Cisco IOS Release 12.2(33)SRD1, these interfaces support QoS:

- Port-channel subinterface (supported in input direction only).
- Port-channel Layer 3 member-link (supported in output direction only).

**Note**
Starting with Cisco IOS Release 15.1 (01)S, these interfaces support QoS:

- Port-channel Layer 2 main interface
- Port-channel Layer 3 main interface
- Port-channel Layer 2 member link

Mapping Between Bay and Ports

The following table maps the bay and port information in an ES+ line card:

<table>
<thead>
<tr>
<th>Specifications</th>
<th>Port/Bay Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>ES+, 1GIG, 10 GIG variant has 4 NPs</td>
<td>1-10 NP0</td>
</tr>
<tr>
<td></td>
<td>11-20 NP1</td>
</tr>
<tr>
<td></td>
<td>21-30 NP2</td>
</tr>
<tr>
<td></td>
<td>31-40 NP3</td>
</tr>
<tr>
<td>1 GIG: 40 Ports</td>
<td></td>
</tr>
<tr>
<td>10 GIG : 4 (10 gig) ports</td>
<td>1 mapped to NP0</td>
</tr>
<tr>
<td></td>
<td>2 mapped to NP1</td>
</tr>
<tr>
<td></td>
<td>3 mapped to NP2</td>
</tr>
<tr>
<td></td>
<td>4 mapped to NP3</td>
</tr>
</tbody>
</table>

There are other flavors with 20 Ports as well. In all these cases, least number of NP is mapped to the least number ports. For example, 1gig or 10 gig with each NP is mapped to 10 - 1 GIG or 1 - 10 GIG ports.
Table 7-2  Mapping between Bay and Ports in Combo Cards

<table>
<thead>
<tr>
<th>Specifications</th>
<th>Port/Bay Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>40G combo card</td>
<td>1 - 10 G port mapped to NP 2</td>
</tr>
<tr>
<td></td>
<td>11 - 20 G Port mapped to NP 1</td>
</tr>
<tr>
<td></td>
<td>21 TG port mapped to NP0</td>
</tr>
<tr>
<td></td>
<td>22 TG port mapped to NP3</td>
</tr>
<tr>
<td>20G combo card</td>
<td>1 - 10G port mapped to NP1</td>
</tr>
<tr>
<td></td>
<td>11 TG port mapped to NP0</td>
</tr>
</tbody>
</table>

The following table maps the bay and port information in an ES+ HD (both variants) line card:

Table 7-3  Mapping between Bay and Ports in ES+HD line card

<table>
<thead>
<tr>
<th>Specification</th>
<th>Port/Bay Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>ES+ HD (Lowq and Highq)</td>
<td>1 and 5   NP 0</td>
</tr>
<tr>
<td></td>
<td>2 and 6   NP 1</td>
</tr>
<tr>
<td></td>
<td>3 and 7   NP 2</td>
</tr>
<tr>
<td></td>
<td>4 and 8   NP 3</td>
</tr>
</tbody>
</table>

QoS Functions

The following sections describe ingress and egress QoS functions.

Ingress QoS Functions

The following paragraphs describe ingress QoS support on the Cisco 7600 Series ES+ line card.

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 predefined 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.

Note

Starting with Cisco IOS Release 12.2(33)SRE4, for switchport and SVI interfaces, the default port behavior is trust dscp. The cos value is derived from the dscp value.

The main Layer 3 interface and the Layer 3 subinterface 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 7-23.

**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 Queue Scheduling

The Cisco 7600 Series ES+ line card supports ingress queue scheduling. For information on configuring ingress scheduling, see the “Configuring QoS Queue Scheduling” section on page 7-32.

### 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

The Cisco 7600 Series ES+ line card supports ingress classification. For information on configuring classification, see the “Configuring Classification” section on page 7-8.

### 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.

The Cisco 7600 Series ES+ line card supports ingress policing. For information on configuring policing, see the “Configuring Policing” section on page 7-14.

### 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.

The Cisco 7600 Series ES+ line card supports ingress marking. For information on configuring marking, see the “Configuring Marking” section on page 7-23.
**Ingress Bandwidth and Ingress Queuing**

Ingress bandwidth allows you to specify or modify the bandwidth allocated for a class belonging to a policy-map. Class-based weighted fair queuing (CBWFQ) extends the standard WFQ functionality to provide support for user-defined traffic classes. Ingress bandwidth and CBWFQ are supported on main Layer 3 interface, Layer 3 subinterface, and service instances.

The Cisco 7600 Series ES+ line card supports ingress bandwidth, for more information, see the “Configuring QoS Queue Scheduling” section on page 7-32.

**LLQ (Ingress Priority)**

Low-Latency Queuing (LLQ) allows you to allocate bandwidth to the class maps in the policy-map.

The Cisco 7600 Series ES+ line card supports LLQ. For information, see the “Configuring LLQ” section on page 7-53.

**Ingress Shaping**

The Cisco 7600 Series ES+ line card supports ingress shaping. The shape average command is supported in flat/H-QoS policy-maps in ingress on main Layer 3 interface, Layer 3 subinterface, and service instances. For more information, see the “Configuring Shaping” section on page 7-27.

---

**Note**

Ingress queuing commands are not supported on port channel service instances.

---

**Egress QoS Functions**

The following sections describe QoS functions on the Cisco 7600 Series ES+ line card egress ports.

**Restrictions and Usage Guidelines**

Follow these restrictions and usage guidelines when configuring the Egress QoS functions:

- Each port on an ES+ card has a special Tx queue where all traffic originating from RP or SP will be sent, if the packets have DBUS CoS 6 or CoS 7 or BPU bit set. Packets sent to this egress special queue will not be subject to the interface egress QoS and egress ACL.

**Egress 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
- Queued to rate limit specific traffic types

The Cisco 7600 Series ES+ line card supports egress classification. For information on configuring classification, see the “Configuring Classification” section on page 7-8.
Egress Policing

The Cisco 7600 Series ES+ line card supports 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.

The Cisco 7600 Series ES+ line card supports egress port marking. For information on configuring marking, see the “Configuring Marking” section on page 7-23.

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.

The Cisco 7600 Series ES+ line card supports shaping on egress port, subinterfaces, and service instances. For information on configuring shaping, see the “Configuring Shaping” section on page 7-27.

Egress Queue Scheduling

The egress line card uses congestion avoidance to help prevent congestion and keep its buffers from overflowing.

The Cisco 7600 Series ES+ line card supports Class-based Weighted Fair Queuing (CBWFQ), Low Latency Queuing (LLQ), and Weighted Random Early Detection (WRED). For information on configuring egress scheduling, see the Configuring QoS Queue Scheduling, page 7-32 section.

Configuring QoS Features Using MQC

The Modular QoS CLI (MQC) is a CLI structure that allows users to create traffic policies and attach these policies to interfaces. A traffic policy contains a traffic class and one or more QoS features. A traffic class is used to select traffic, while the QoS features in the traffic policy determine how to treat the classified traffic.

To configure QoS features using the Modular QoS CLI on the Cisco 7600 Series ES+ line card, complete the following basic steps:

- **Step 1** Define a traffic class using the `class-map` command.
- **Step 2** Create a traffic policy by associating the traffic class with one or more QoS features (using the `policy-map` command).
- **Step 3** Attach the traffic policy to the interface using the `service-policy` command.

Configuring Classification

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.

Restrictions and Usage Guidelines

Follow these restrictions and usage guidelines when configuring the QoS classification an ES40 line card:

- Only classified based on source MAC address using Layer 2 ACL is supported.
- Cisco 7600 Series ES+ line cards support classification on SVI only for EoMPLS and VPLS.
- The match not command is not supported.
- In a class-map access-list, permit ICMP, IGMP, and Deny statements are not supported. Even if the ICMP, IGMP, and Deny statements are configured, and policy-map is applied on an interface, an error is displayed and the policy will not work at the hardware level. Effective from release 15.2(4)S, Permt ICMP is supported.

Table 7-4 provides information about which QoS classification features are supported for the Cisco 7600 Series ES+ line card on the Cisco 7600 series router. For more information about most of the commands documented in this table, refer to the Cisco IOS Quality of Service Solutions Command Reference.
### Table 7-4  QoS Classification Feature Support

<table>
<thead>
<tr>
<th>Feature (match command)</th>
<th>Supported Interfaces</th>
</tr>
</thead>
</table>
| Match on access list (ACL) number (**match access-group** command) | Input and output for the following interfaces:  
- Main Layer 3 interface  
- Layer 3 subinterface  
- Switchport interfaces  
- Service instances  
- Port-channel service instances  
- Port-channel subinterface  

**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 interfaces:  
- Main Layer 3 interface  
- Layer 3 subinterface  
- Switchport interfaces  
- SVI interfaces  
- Service instances  
- Port-channel service instances  
- Port-channel subinterface  
- Port-channel member link  
- Port-channel layer 2 and layer 3 interface  

**Note**  
Used with non-intelligent line card in the input side and a Cisco 7600 Series 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 inner CoS (**match cos inner** command) | Input and output for the following interfaces:  
- Service instances  
- Port-channel service instances |
| Match on input VLAN (**match input vlan** command) | Output for the following interfaces:  
- Main Layer 3 |

**Note**  
Used with non-intelligent line card in the input side and a Cisco 7600 Series ES+ line card on the output side. The service policy is applied on the output side to match the VLAN from the input side.
### Table 7-4 QoS Classification Feature Support (continued)

<table>
<thead>
<tr>
<th>Feature (match command)</th>
<th>Supported Interfaces</th>
</tr>
</thead>
<tbody>
<tr>
<td>Match on IP DSCP (match ip dscp command)</td>
<td>Input and output for the following interfaces:</td>
</tr>
<tr>
<td></td>
<td>• Main Layer 3 interface</td>
</tr>
<tr>
<td></td>
<td>• Layer 3 subinterface</td>
</tr>
<tr>
<td></td>
<td>• Switchport interfaces</td>
</tr>
<tr>
<td></td>
<td>• Service instances</td>
</tr>
<tr>
<td></td>
<td>• Port-channel service instances</td>
</tr>
<tr>
<td></td>
<td>• Port-channel subinterface</td>
</tr>
<tr>
<td></td>
<td>• Port-channel Layer 3 member link</td>
</tr>
<tr>
<td>Match on IP precedence (match ip precedence command)</td>
<td>Input and output for the following interfaces:</td>
</tr>
<tr>
<td></td>
<td>• Main Layer 3 interface</td>
</tr>
<tr>
<td></td>
<td>• Layer 3 subinterface</td>
</tr>
<tr>
<td></td>
<td>• Switchport interfaces</td>
</tr>
<tr>
<td></td>
<td>• Service instances</td>
</tr>
<tr>
<td></td>
<td>• Port-channel service instances</td>
</tr>
<tr>
<td></td>
<td>• Port-channel subinterface</td>
</tr>
<tr>
<td></td>
<td>• Port-channel Layer 3 member link</td>
</tr>
<tr>
<td>Match on MPLS experimental (EXP) bit (match mpls experimental command)</td>
<td>Input and output for the following interfaces:</td>
</tr>
<tr>
<td></td>
<td>• Main Layer 3 interface</td>
</tr>
<tr>
<td></td>
<td>• Layer 3 subinterface</td>
</tr>
<tr>
<td></td>
<td>• Switchport interfaces</td>
</tr>
<tr>
<td></td>
<td>• Port-channel subinterface</td>
</tr>
<tr>
<td></td>
<td>• Port-channel Layer 3 member link</td>
</tr>
<tr>
<td>Match on VLAN (match vlan command—Matches the outer VLAN of a Layer 2 IEEE 802.1Q frame)</td>
<td>Input and output for the following interfaces:</td>
</tr>
<tr>
<td></td>
<td>• Main Layer 3 interface$^3$</td>
</tr>
<tr>
<td></td>
<td>• Layer 3 subinterface</td>
</tr>
<tr>
<td></td>
<td>• Switchport interfaces</td>
</tr>
<tr>
<td></td>
<td>• Service instances</td>
</tr>
<tr>
<td></td>
<td>• Port-channel service instances</td>
</tr>
<tr>
<td></td>
<td>• Port-channel layer 2 and layer 3 interface</td>
</tr>
<tr>
<td></td>
<td>• Port channel subinterface</td>
</tr>
</tbody>
</table>
Chapter 7      Configuring QoS

**Table 7-4  QoS Classification Feature Support  (continued)**

<table>
<thead>
<tr>
<th>Feature (match command)</th>
<th>Supported Interfaces</th>
</tr>
</thead>
<tbody>
<tr>
<td>Match on VLAN Inner</td>
<td>Input and output for the following interfaces:</td>
</tr>
<tr>
<td>(match vlan inner command—Matches the innermost VLAN of the 802.1Q tag in the Layer 2 frame)</td>
<td>• Layer 3 subinterface</td>
</tr>
<tr>
<td></td>
<td>• Service instances</td>
</tr>
<tr>
<td></td>
<td>• Port-channel service instances</td>
</tr>
<tr>
<td></td>
<td>• Port-channel subinterface (input only)</td>
</tr>
<tr>
<td>Match on source-address MAC</td>
<td>Input and output for the following interfaces:</td>
</tr>
<tr>
<td>match source-address mac command—Matches the source MAC address.</td>
<td>• Switchport interfaces</td>
</tr>
<tr>
<td></td>
<td>• Service instances</td>
</tr>
<tr>
<td></td>
<td>• Port-channel service instances</td>
</tr>
<tr>
<td></td>
<td>• Port-channel layer 2 interface</td>
</tr>
</tbody>
</table>

1. Only classified based on source MAC address using Layer 2 ACL.
2. For more information on ACL Classification on service instances, see [Layer 2 and Layer 3 QoS ACL Classification for EVC](#).
3. To match subinterface/EVC traffic and policy-map applied on the main interface.
4. Cisco 7600 Series ES+ line cards support classification on SVI only for EoMPLS and VPLS.
5. The `match not` command is not supported.

---

**Note**

Starting with Cisco IOS Release 12.2(33)SRD1, these interfaces support QoS:

- Port-channel subinterface (supported in input direction only).
- Port-channel Layer 3 member-link (supported in output direction only).

**Note**

Starting with Cisco IOS Release 15.1(01)S, these interfaces support QoS:

- Port-channel Layer 2 main interface
- Port-channel Layer 3 main interface
- Port-channel Layer 2 member link

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `class-map [match-all | match-any] class-map-name`
4. `match type`
## DETAILED STEPS

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>enable</strong></td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Router# enable</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>configure terminal</strong></td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Router# configure terminal</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>**class-map [match-all</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Router(config)# class-map match-all acl19 (id 1049)</td>
</tr>
<tr>
<td></td>
<td>Note</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><strong>match type</strong></td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Router(config-cmap)# match ip precedence 5</td>
</tr>
<tr>
<td></td>
<td>Note</td>
</tr>
</tbody>
</table>
Examples

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 a logical AND operation in a child policy with match vlan and class-default in a parent.

```
Router# enable
Router# configure terminal
Router(config)# class-map match-all childAND
Router(config-cmap)# match vlan inner 2-3
Router(config-cmap)# match cos inner 5 6
Router(config)# policy-map testchildAND
Router(config-pmap)# class childAND
Router(config-pmap-c)# shape average 100000000
Router(config)# policy-map parentAND
Router(config-pmap)# class vlan12
Router(config-pmap-c)# shape average 500000000
Router(config-pmap-c)# service-policy testchildAND
```

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 acl15
Class Map match-all acl15 (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.

```
head# show policy-map match
Policy Map match
  Class vlan11
    shape average 2000000 8000 8000
```
Configuring Policing

The Cisco 7600 Series ES+ line cards support the following features:

- Individual Actions
- Multiple Actions
- Single Rate, 2 Color Policer
  - Granularity
  - Accuracy (Rate and Bucket Depths)
  - Statistics
  - Percent based policer
- Dual Rate, 3 color
  - Percent based policer
- Color aware policer not supported
- Single-rate 3-color not supported.
- Color blind mode
- Hierarchical Policies (up to two levels)
- 255 Profiles at different rates
- Micro-flow policing

Policing is supported at the input and output for the following interfaces:

- Main Layer 3 interface
- Layer 3 subinterface
- Switchport interfaces
- Service instances
- Port-channel service instances
- Port-channel subinterface (input only) (aggregate per NPE)
- Layer 3 port-channel member link

Micro-flow policing is supported at the input for the following interfaces:

- Main Layer 3 interface (micro-flow policing)
- Layer 3 subinterface (micro-flow policing)
- Port-channel subinterface (micro-flow policing)
Restrictions and Usage Guidelines

When configuring policing, follow these restrictions and usage guidelines:

- The Cisco 7600 Series ES+ line card supports **maximum of 1k unique global policy-maps** per line card.
- The Cisco 7600 Series ES+ line card supports 16K EVCs. 16K ingress service policies and 16K egress service policies are supported per line card.
- Maximum class maps per policy-map are 253.
- 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.
- EVC micro-flow policer is not supported.
- When configuring supported micro-flow policing:
  - A policy must only contain micro-flow policing commands. Micro-flow policing is not supported with other QoS features (that is, with marking, policing, or queuing).
  - Micro-flow policing is PFC action. Other QoS features (that is, marking, policing, or queuing) are implemented in the NPE.
- Effective from Cisco IOS Release15.1(2)S, ISG Control Plane Policing (CoPP) is supported on regular subinterfaces.

Any modification to the micro-flow policing policy that shifts the policy implementation from NPE to the PFC or from the PFC to the NPE is not supported. All such modifications would require the policy to be first removed from the attached ES40 interfaces, modified, and then reattached to ES40 interfaces.

*Table 7-5* provides information about which policing features are supported for the Cisco 7600 Series ES+ line card on the Cisco 7600 series routers.
### Table 7-5 QoS Policing Feature Support

<table>
<thead>
<tr>
<th>Policing Command</th>
<th>Policing Action (set command)</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>police bps value conform-action action</code></td>
<td>• Transmit the packet (transmit action)</td>
</tr>
<tr>
<td><code>exceed-action action</code></td>
<td>• Drop the packet (drop command)</td>
</tr>
<tr>
<td></td>
<td>• Set the IP precedence value (set ip precedence command)</td>
</tr>
<tr>
<td></td>
<td>• Set the IP DSCP value (set ip dscp command)</td>
</tr>
<tr>
<td></td>
<td>• Set the MPLS EXP bit (0–7) on imposition (set-mpls-experimental-imposition command)</td>
</tr>
<tr>
<td></td>
<td>• Set the MPLS EXP bit in the topmost label (set-mpls-experimental-topmost command)</td>
</tr>
<tr>
<td></td>
<td>• Set the COS value (set cos command)</td>
</tr>
<tr>
<td></td>
<td>• Set the COS-inner value (set cos-inner command)</td>
</tr>
<tr>
<td><code>police cir percent % conform-action action</code></td>
<td>• Transmit the packet (transmit action)</td>
</tr>
<tr>
<td><code>exceed-action action</code></td>
<td>• Drop the packet (drop command)</td>
</tr>
<tr>
<td></td>
<td>• Set the IP precedence value (set ip precedence command)</td>
</tr>
<tr>
<td></td>
<td>• Set the IP DSCP value (set ip dscp command)</td>
</tr>
<tr>
<td></td>
<td>• Set the MPLS EXP bit (0–7) on imposition (set-mpls-experimental-imposition command)</td>
</tr>
<tr>
<td></td>
<td>• Set the MPLS EXP bit in the topmost label (set-mpls-experimental-topmost command)</td>
</tr>
<tr>
<td></td>
<td>• Set the COS value (set cos command)</td>
</tr>
<tr>
<td></td>
<td>• Set the COS-inner value (set cos-inner command)</td>
</tr>
</tbody>
</table>
Chapter 7 Configuring QoS

Configuring Policing

### SUMMARY STEPS

1. enable
2. configure terminal
3. policy-map policy-map-name
4. class 
   - class-name
   - class-default
5. police cir bps value pir bps value conform-action action exceed-action action violate-action action
   - police cir percent % pir percent % conform-action action exceed-action action violate-action action

### Table 7-5 QoS Policing Feature Support (continued)

<table>
<thead>
<tr>
<th>Policing Command</th>
<th>Policing Action (set command)</th>
</tr>
</thead>
</table>
| 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) |
### Chapter 7 Configuring QoS

#### Configuring Policing

<table>
<thead>
<tr>
<th>Step 1</th>
<th>enable</th>
<th>Enables privileged EXEC mode.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>Router# enable</td>
<td>- Enter your password if prompted.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>configure terminal</th>
<th>Enters global configuration mode.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>Router# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 3</th>
<th>policy-map policy-map-name</th>
<th>Creates or modifies a traffic policy and enters policy-map configuration mode, where:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config)# policy-map policy-map-test</td>
<td>policy-map-name—Specifies the name of the traffic policy to configure. Names can be a maximum of 40 alphanumeric characters.</td>
</tr>
</tbody>
</table>

| Step 4 | 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: |
|--------|---------------|---------------------------------|
| **Example:** | Router(config-pmap)# class acgroup2 | 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. |

<table>
<thead>
<tr>
<th>Step 5</th>
<th>police bps-value conform-action action exceed-action action</th>
<th>Specifies a maximum bandwidth usage by a traffic class through the use of a token bucket algorithm, where:</th>
</tr>
</thead>
</table>
| **Example:** | Router(config-pmap-c)# police 5000000 conform-action drop exceed-action action set-dscp-transmit | 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 7-5. |

Or

<table>
<thead>
<tr>
<th>police cir percent # conform-action action exceed-action action</th>
<th>Configures traffic policing on the basis of a percentage of bandwidth available on an interface, where:</th>
</tr>
</thead>
</table>
| **Example:** | Router(config-pmap-c)# police cir percent 20 conform-action transmit exceed-action set-prec-transmit 1 | 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.  
%—Specifies the CIR bandwidth percentage. Valid values are 1 to 100.  
action—Specifies the actions that are taken on a packet when it conforms or exceeds. The possible actions are shown in Table 7-5. |

Or
### Examples

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 conform-action
set-cos-transmit 3 exceed-action
set-cos-transmit 1 violate-action drop
```

#### Command Purpose

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| policy 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 action that are taken on a packet when it conforms or exceeds. The possible actions are shown in Table 7-5. |

#### Example:

```
Example:
Router(config-pmap-c)# police cir
10000000 pir 2000000 conform-action
set-cos-transmit 3 exceed-action
set-cos-transmit 1 violate-action drop
```

Or

```
policy cir percent pir percent conform-action action exceed-action action violate-action action
```

#### Example:

```
Example:
Router(config-pmap-c)# police cir
percent 20 pir percent 40 conform-action
transmit exceed-action set-prec-transmit
1 violate-action drop
```

Confirms 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 actions that are taken on a packet when it conforms or exceeds. The possible actions are shown in Table 7-5.
This example configures a 1 rate 2-color policer:

```conf
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
 conform 2000000 bc 62500
 exceed-action drop
Router#
```

This example configures a 1 rate 2-color policer with percent:

```conf
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
 conform cir percent 20
 exceed-action drop
Router#
```

This example configures a 2 rate 3-color policer:

```conf
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
 conform cir 2000000 bc 62500 pir 3000000 be 93750
 exceed-action set-prec-transmit 3
 violate-action set-prec-transmit 2
Router#
```

This example configures a 2 rate 3-color policer with percent:

```conf
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#
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
Router#

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
Verification

Use the following commands to verify policing:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router# show policy-map</td>
<td>Displays all configured policy-maps.</td>
</tr>
<tr>
<td>Router# show policy-map policy-map-name</td>
<td>Displays the user-specified policy-map.</td>
</tr>
<tr>
<td>Router# show policy-map interface</td>
<td>Displays statistics and configurations of all input and output policies that are attached to an interface.</td>
</tr>
</tbody>
</table>

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
```

This is another example of displaying policing statistics using the `show policy-map interface` command; in this case the statistics are for a one rate 2 color per EVC policer.

```
Router# show policy-map interface ten 4/1 service instance 1
TenGigabitEthernet4/1: EFP 1
Service-policy input: evc_ingsress
  Counters last updated 00:00:00 ago
  Class-map: class-default (match-any)
    72077 packets, 36903424 bytes
    5 minute offered rate 981000 bps, drop rate 440000 bps
  Match: any
police:
  cir 10000000 bps, bc 8000 bytes
  conformed 87426 packets, 44762112 bytes; actions:
    transmit
  exceeded 85974 packets, 44018688 bytes; actions:
    drop
  conformed 556000 bps, exceed 448000 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, main interfaces, and service instances.
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**

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:

```
Router(config-if)# service-policy input policy-map-name
```

**Purpose**

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:

```
Router(config-if)# service-policy output policy-map-name
```

**Purpose**

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**

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.

**Restrictions and Usage Guidelines**

When configuring class-based marking on a Cisco 7600 Series 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 parent and leaf.
- EARL marking is not used.
- Marking can be combined with queuing 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 7-6 provides information about which QoS class-based marking features are supported for the Cisco 7600 Series ES+ line card on the Cisco 7600 series router.

<table>
<thead>
<tr>
<th>Marking Feature (set command)</th>
<th>Supported Interfaces</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set IP DSCP</td>
<td>Input and output for the following interfaces:</td>
</tr>
</tbody>
</table>
| (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.) | - Main Layer 3 interface  
- Layer 3 subinterface  
- Service instances  
- Port-channel service instances  
- Port-channel subinterface  
- Port-channel member link  
- Port-channel layer 3 interface |
| Set IP precedence            | Input and output for the following interfaces: |
| (set ip precedence command—Marks the precedence value in the IP header with a value from 0 to 7.) | - Main Layer 3 interface  
- Layer 3 subinterface  
- Service instances  
- Port-channel service instances  
- Port-channel subinterface  
- Port-channel member link  
- Port-channel layer 3 interface |
| Set Layer 2 IEEE 802.1Q CoS  | Input and output for the following interfaces: |
| (set cos command—Marks the CoS value from 0 to 7 in an 802.1Q tagged frame.) | - Main Layer 3 interface  
- Layer 3 subinterface  
- Switchport interfaces  
- Service instances (excluding EoMPLS on input)  
- Port-channel service instances  
- Port-channel subinterface  
- Port-channel member link  
- Port-channel layer 2 and 3 interface |
Table 7-6  QoS Class-Based Marking Feature Support (continued)

<table>
<thead>
<tr>
<th>Marking Feature (set command)</th>
<th>Supported Interfaces</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set Layer 2 802.1Q CoS</td>
<td>Input and output for the following interfaces:</td>
</tr>
<tr>
<td><em>(set cos-inner command)—Marks the inner CoS field from 0 to 7 in a bridged frame.</em></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Layer 3 subinterface</td>
</tr>
<tr>
<td></td>
<td>• Service instances</td>
</tr>
<tr>
<td></td>
<td>• Port-channel service instances</td>
</tr>
<tr>
<td>Set Layer 2 802.1Q CoS</td>
<td>Input and output for the following interfaces:</td>
</tr>
<tr>
<td><em>(set cos-inner cos command)—Copies out CoS to inner CoS.</em></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Layer 3 subinterface</td>
</tr>
<tr>
<td></td>
<td>• Service instances</td>
</tr>
<tr>
<td></td>
<td>• Port-channel service instances</td>
</tr>
<tr>
<td>Set Layer 2 802.1Q CoS</td>
<td>Input and output for the following interfaces:</td>
</tr>
<tr>
<td><em>(set cos cos-inner command)</em></td>
<td>• Layer 3 subinterface</td>
</tr>
<tr>
<td></td>
<td>• Service instances</td>
</tr>
<tr>
<td></td>
<td>• Port-channel service instances</td>
</tr>
<tr>
<td>Set MPLS experimental (EXP) bit on label imposition</td>
<td>Input for the following interfaces:</td>
</tr>
<tr>
<td><em>(set mpls experimental imposition command)</em></td>
<td>• Main Layer 3 interface</td>
</tr>
<tr>
<td></td>
<td>• Layer 3 subinterface</td>
</tr>
<tr>
<td></td>
<td>• Port-channel service instances (Not supported on switchport)</td>
</tr>
<tr>
<td></td>
<td>• Port-channel layer 3 interface</td>
</tr>
<tr>
<td>Set MPLS EXP topmost</td>
<td>Input and output for the following interfaces:</td>
</tr>
<tr>
<td><em>(set mpls experimental topmost command)</em></td>
<td>• Main Layer 3 interface</td>
</tr>
<tr>
<td></td>
<td>• Layer 3 subinterface</td>
</tr>
</tbody>
</table>

1. To match subinterface/EVC traffic and policy-map applied on the main interface.

**Note**
Starting with Cisco IOS Release 12.2(33)SRD1, these interfaces support QoS:
- Port-channel subinterface (supported in input direction only).
- Port-channel Layer 3 member-link (supported in output direction only).

**Note**
Starting with Cisco IOS Release 15.1 (01)S, these interfaces support QoS:
- Port-channel Layer 2 main interface
- Port-channel Layer 3 main interface
- Port-channel Layer 2 member link

**SUMMARY STEPS**

1. **enable**
2. **configure terminal**
3. policy-map policy-map-name
4. class {class-name | class-default}
5. set type

DETAILED STEPS:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode. Example: Router# enable</td>
</tr>
<tr>
<td></td>
<td>Enter your password if prompted.</td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Router# configure terminal</td>
</tr>
<tr>
<td>Step 3 policy-map policy-map-name</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Example: Router(config)# policy-map policymap3</td>
</tr>
<tr>
<td>Step 4 class {class-name</td>
<td>Specifies the name of the traffic class to which this policy applies and enters policy-map class configuration mode, where:</td>
</tr>
<tr>
<td>class-default}</td>
<td>class-name—Specifies that the policy applies to a user-defined class name previously configured.</td>
</tr>
<tr>
<td></td>
<td>class-default—Specifies that the policy applies to the default traffic class.</td>
</tr>
<tr>
<td></td>
<td>Example: Router(config-pmap)# class class1</td>
</tr>
<tr>
<td>Step 5 set type</td>
<td>Specifies the marking action to be applied to the traffic, where type represents one of the forms of the set command supported by the Cisco 7600 Series ES+ line card as shown in Table 7-6.</td>
</tr>
<tr>
<td></td>
<td>Example: Router(config-pmap-c)# set ip precedence2</td>
</tr>
</tbody>
</table>

Examples

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

Verification

Use the following commands to verify marking:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router# show policy-map</td>
<td>Displays all configured policy-maps.</td>
</tr>
<tr>
<td>Router# show policy-map policy-map-name</td>
<td>Displays the user-specified policy-map.</td>
</tr>
<tr>
<td>Router# show policy-map interface</td>
<td>Displays statistics and configurations of all input and output policies that are attached to an interface.</td>
</tr>
</tbody>
</table>

For more detailed information about configuring class-based marking features, refer to the Class-Based Marking document located at the following URL:

http://www.cisco.com/en/US/docs/ios/12_1t/12_1t5/feature/guide/cbpmark2.html

Configuring Shaping

This section describes information for configuring QoS traffic policies for shaping traffic. Shaping is the process of delaying packets in queues to make them conform to a specified profile.

Restrictions and Usage Guidelines

When configuring shaping on an Cisco 7600 Series ES+ line card, 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.
Chapter 7 Configuring QoS

- Dual shapers are not supported.
- Service instance, port channel service instance, and Layer 3 subinterface support two-level policy-map: parent class-default and child policy.
- Main interface supports three-level policy-map: grand-parent class-default, parent user defined classes, and 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.
- Shaper CIR granularity for grand parent level shaper:
  - 160,000 bps to 40,960,000 bps: granularity of 160,000 bps.
  - 40,960,000 bps to 163,840,000 bps: granularity of 640,000 bps.
  - 163,840,000 bps to 655,360,000 bps: granularity of 2,560,000 bps.
  - 655,360,000 bps to 10G: granularity of 40,960,000 bps.
- Maximum shaper rate in the leaf policy-map is 130 Mb/s.
- The shape average percent command is not supported.

For more detailed information about configuring congestion management features, refer to the Cisco IOS Quality of Service Solutions Configuration Guide document corresponding to your Cisco IOS software release.

Table 7-7 provides information about which QoS traffic shaping features are supported for the Cisco 7600 Series ES+ line card on the Cisco 7600 series router.

<table>
<thead>
<tr>
<th>Traffic Shaping Feature (command)</th>
<th>Cisco 7600 Series ES+ Line Card</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class-based shaping</td>
<td>Input and output for the following interfaces:</td>
</tr>
<tr>
<td>(shape average commands)</td>
<td>• Main Layer 3 interface</td>
</tr>
<tr>
<td></td>
<td>• Layer 3 subinterface</td>
</tr>
<tr>
<td></td>
<td>• Switchport interfaces</td>
</tr>
<tr>
<td></td>
<td>• Port-channel service instances (output only)</td>
</tr>
<tr>
<td></td>
<td>• Port-channel Layer 3 member link (output only)</td>
</tr>
</tbody>
</table>

Shaper Tc Granularity for ES+ Line Card

The lowest supported Tc on the hardware is 50 micro sec. The value of Tc is derived as:

\[ Tc = \frac{BC}{CIR} \]

where:
- Tc - Time interval over which the committed burst (Bc) can be sent
- Bc - Committed burst size, represents the amount of traffic that can be sent over Tc interval.
- CIR - Committed Information Rate (in bits per second).
**Note**

Be is Burst Excess. The Be value is derived from PIR. On the ES+ Line Card, the configuration is CIR = PIR. By default, Be= Bc. Therefore, the Be value cannot be taken as zero as the lowest supported Tc on the hardware is 50 micro seconds.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `class-map [match-all | match-any] class-map-name`
4. `match [ip dscp ip-dscp-value | ip precedence ip-precedence-value | mpls experimental mpls-exp-value]`
5. `policy-map policy-name`
6. `class class-name`
7. `shape average cir [bc] [be]`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>enable</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router# enable</td>
</tr>
<tr>
<td>Enables privileged EXEC mode.</td>
<td></td>
</tr>
<tr>
<td>• Enter your password if prompted.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router# configure terminal</td>
</tr>
<tr>
<td>Enters global configuration mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>class-map [match-all</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config)# class-map class-interface-all</td>
</tr>
<tr>
<td>Creates a class map to be used for matching packets to a class.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>match [ip dscp ip-dscp-value</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-cmap)# match ip precedence 2</td>
</tr>
<tr>
<td>Specifies a specific IP DSCP, IP precedence, or MPLS EXP value as a match criterion.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>policy-map policy-name</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config)# policy-map test2</td>
</tr>
<tr>
<td>Specifies the name of the policy-map to configure.</td>
<td></td>
</tr>
</tbody>
</table>
Chapter 7  Configuring QoS

Configuring Shaping

Examples

This example shows traffic shaping on a main interface; traffic leaving interface gi1/1 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 gi1/1
Router(config-if)# service-policy output dts-interface-all-action

This is an example of an output shaping policy on a switchport interface that matches on a CoS value queuing defined in the classes.

Router# enable
Router# configure terminal
Router(config)# policy-map switchport-cos-policy
Router(config-pmap)# class cos1
Router(config-pmap-c)# shape ave 10000000

Now the policy is applied in the egress direction on the main switchport.

Router# enable
Router# configure terminal
Router(config)# interface TenGigabitEthernet9/1
Router(config-if)# switchport
Router(config-if)# switchport access vlan 2000
Router(config-if)# switchport mode access
Router(config-if)# service-policy output switchport-cos-policy

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 10000000
Router(config)# policy-map pcd
Router(config-pmap)# class class-default
Router(config-pmap-c)# shape average 30000000
Router(config-if)# service-policy child2

### Command Purpose

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 6</strong></td>
<td><strong>class class-name</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-pmap-c)# class classtest</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td><strong>shape average cir [bc] [be]</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-pmap-c)# shape average 10000000</td>
</tr>
</tbody>
</table>
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
```

Verification

Use the following commands to verify traffic shaping:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router# show interface [interface-name]</td>
<td>Displays detail status of the traffic shaping.</td>
</tr>
<tr>
<td>Router# show policy policy-name</td>
<td>Displays the configuration of all classes composing the specified traffic policy.</td>
</tr>
<tr>
<td>Router# show policy policy-name class class-name</td>
<td>Displays the configuration of the specified class of the specified traffic policy.</td>
</tr>
</tbody>
</table>

Configuring QoS Overhead Accounting for Shaping Parameters

By default, the ES+ shaper algorithm uses only layer 2 frame length excluding FCS or CRC. This feature helps you to configure shaping the QoS features with overheads like FCS or CRC, IFG, and Preamble.

Use the `hw-module slot slot-number account np np-index out/in length` command in the global configuration mode to enable this feature. You can use this command for both ingress and egress shaping.

Complete the following steps to configure Overhead accounting feature.

Restrictions

This command is not applicable for policer and LLQ classes.

SUMMARY STEPS

<table>
<thead>
<tr>
<th>Step 1</th>
<th>enable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 3</td>
<td>hw-module slot slot-number account np np-index out length</td>
</tr>
<tr>
<td>Step 4</td>
<td>exit</td>
</tr>
</tbody>
</table>
### Configuring QoS Queue Scheduling

This section describes Cisco 7600 Series ES+ line card-specific information for configuring QoS queue scheduling.

### Restrictions and Usage Guidelines

When configuring queuing features on an Cisco 7600 Series ES+ line card, 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.

---

### Detailed Steps

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>enable</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>Router&gt; enable</strong></td>
</tr>
<tr>
<td></td>
<td>Enables privileged EXEC mode. Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>configure terminal</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>Router# configure terminal</strong></td>
</tr>
<tr>
<td></td>
<td>Enters the global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>hw-module slot slot-number account np np-index out length</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>Router(config)# hw-module slot 1 account np 0 out 4</strong></td>
</tr>
<tr>
<td></td>
<td>Enables Layer 2 overhead encapsulation for calculating shaped bit rates.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> This command is applicable to all the ports in the specific NP on the ES40 linecard.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><strong>end</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>Router(config-if)# end</strong></td>
</tr>
<tr>
<td></td>
<td>Returns the command-line interface (CLI) to privileged EXEC mode.</td>
</tr>
</tbody>
</table>

### Configuration Examples

This example describes how to configure shaping and policing QoS features:

```plaintext
Router> enable
Router# configure terminal
Router(config)# hw-module slot 1 account np 0 out 4
Router(config-if)# end
```
Configuring QoS Queue Scheduling

- 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 NPE (nonconfigurable).
- 32K child queues on ingress and 64k child queues for egress per NPE (nonconfigurable).
- Parent class-default on sub-interface/EVCs scales more.
- Parent user-defined classmap is supported on main Layer 3 interface, and port-channel Layer 3 member link (output only).
- QoS queue scheduling supports the following commands:
  - `bandwidth x kbps`
  - `bandwidth percent x%`
  - `bandwidth remaining percent x%`
  - `bandwidth remaining ratio`
  - `priority`
  - `priority level level`
  - `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`

For more detailed information about configuring congestion management features, refer to the *Cisco IOS Quality of Service Solutions Configuration Guide* document corresponding to your Cisco IOS software release.

Configuring WRED

Weighted RED (WRED) drops packets selectively based on DSCP, IP precedence (the default), or CoS QoS values. Packets with higher QoS values are less likely to be dropped than packets with lower QoS values. WRED is supported on the output of the following interfaces:

- Main Layer 3 interface
- Layer 3 subinterface
- Switchport interfaces
- Service instances
- Port-channel service instances
- Port-channel Layer 3 member link
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. On an ES+ linecard, there are 8 WRED curves. In a WRED Non-Aggregate mode, a single CoS or Prec value maps to one WRED curve, and in a WRED Aggregate mode, multiple dscp or Prec values are mapped to one WRED curve.

For more information on this, see

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

Restrictions and Usage Guidelines

When configuring WRED on Cisco 7600 Series ES+ line cards, 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 support is available only in the aggregate mode, as DSCP takes 64 possible values. By default, all 64 DSCP values map to one WRED curve; however, mapping multiple DSCP values to each of the 8 WRED curves is configurable. For example, if the requirement is to configure DSCP 30, 50 to take WRED Curve1 and DSCP 10, 40 to take WRED Curve2, the configurations in a policy-map must be as follows:
    - random-detect dscp-based aggregate minimum-thresh 32 maximum-thresh 64 mark-prob 20
    - random-detect dscp values 30 50 minimum-thresh 32 maximum-thresh 64 mark-prob 20
    - random-detect dscp values 10 40 minimum-thresh 80 maximum-thresh 112 mark-prob 20
  - 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 switchport, only cos-based is supported.
  - For EVC and Layer 3 main interface the WRED support is dscp-based, precedence-based, and cos-based.
  - For subinterfaces, WRED supports dscp and prec based only.
  - Queue limit is not supported with WRED command.
  - The limit for class-level queue that is reported in "show policy-map interface" is not applicable in the classes where WRED is configured. This is applicable for the default WRED threshold configuration even for releases earlier than 12.2(33)SRD5.
- Not supported in input direction and parent classes.
- Not supported for priority queues of all priority levels.
- Random Detect in class queue needs a queueing feature. WRED needs queues for packets. During traffic congestion, as WRED gets applied, packets are randomly dropped from the queue. The bandwidth or shape average command can be used to configure queues.
- Random Detect in default class does not need a queueing feature.
Cisco 7600 Series ES+ line cards do not support discard-class-based WRED and ECN with WRED. The ES+ line card does not modify ECN bits for traffic passing through it.

Cisco 7600 Series 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 user configurable maximum value must be between 17 and 1000000. If you use the default profile, the calculated maximum threshold may be lower.

EXP-based WRED for MPLS packets is supported.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `policy-map policy-name`
4. `class class-name`
5. `shape average [target bit rate | percent] or bandwidth [kilo bits/sec | percent | remaining]`
6. `random-detect [aggregate | cos | cos-based | dscp | dscp-based | ecn | exponential-weighting-constant | precedence | precedence-based]`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>- Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router# configure terminal</td>
</tr>
<tr>
<td><strong>Step 3</strong> policy-map policy-name</td>
<td>Specifies the name of the policy-map to configure.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config)# policy-map wred</td>
</tr>
<tr>
<td><strong>Step 4</strong> class class-name</td>
<td>Specifies the name of a predefined class included in the service policy.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-pmap)# class IPP1</td>
</tr>
</tbody>
</table>
### Chapter 7 Configuring QoS

#### Configuring QoS Queue Scheduling

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 5</strong></td>
<td></td>
</tr>
<tr>
<td><code>shape average</code> [target bit rate</td>
<td>Shapes traffic to the indicated bit rate for the specified class, or the percentage of interface bandwidth for the committed information rate.</td>
</tr>
<tr>
<td>percent]</td>
<td>or</td>
</tr>
<tr>
<td>or <code>bandwidth</code> [kilo bits/sec</td>
<td>Indicates bandwidth as kilo bits per second, percentage of total bandwidth, or percentage or ratio of the remaining bandwidth.</td>
</tr>
<tr>
<td>percent</td>
<td></td>
</tr>
<tr>
<td><code>remaining</code> [percent</td>
<td></td>
</tr>
<tr>
<td>remaining]</td>
<td></td>
</tr>
</tbody>
</table>

**Example:**

```
Router(config-pmap-c)# shape average 200000000
```

<table>
<thead>
<tr>
<th><strong>Step 6</strong></th>
<th>Enables WRED.</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>random-detect</code> [aggregate</td>
<td>You can optionally configure the aggregate subclasses (aggregate), the parameters for each cos value (cos), each dscp value (dscp), or each precedence value (precedence), the enabling of cos-class-based, (cos-based), dscp-based (dscp-based), or precedence-based (precedence-based) WRED as drop policy, explicit congestion notification (ecn), or weight for mean queue depth calculation (exponential-weighting-constant).</td>
</tr>
<tr>
<td>cos</td>
<td></td>
</tr>
<tr>
<td>cos-based</td>
<td></td>
</tr>
<tr>
<td>dscp</td>
<td></td>
</tr>
<tr>
<td>dscp-based</td>
<td></td>
</tr>
<tr>
<td>ecn</td>
<td></td>
</tr>
<tr>
<td>exponential-weighting-constant</td>
<td></td>
</tr>
<tr>
<td>precedence</td>
<td></td>
</tr>
<tr>
<td>precedence-based</td>
<td></td>
</tr>
</tbody>
</table>

**Example:**

```
Router(config-pmap-c)# random-detect dscp-based aggregate
```

### Examples for WRED Configurations

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-c)# class IPP3
Router(config-pmap-c)# shape average 100000000
Router(config-pmap-c)# random-detect precedence-based
Router(config-pmap-c)# class IPP5
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 int gig 11/1 service instance 1

GigabitEthernet11/1: EFP 1

Service-policy output: temp_parent

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 283000 bps
Match: any
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
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

WRED Profiles

A WRED profile is a set of minimum thresholds, maximum thresholds, and Mark Probability Denominator (MPD) settings for a class. MPD represents the fraction for the amount of packets that will be dropped during periods of congestion when the average queue size is at maximum capacity. The minimum and maximum thresholds are defined as the number of entries in the queue. WRED can have a WRED minimum threshold, maximum threshold, and MPD settings for each QoS priority marking. Applying different drop thresholds for QoS priority markings differentiates the traffic flows. Hence, different types of traffic have different QoS.

In ES+ line cards, there are 16 unique drop profiles for a Traffic Manager (TM), of which 4 profiles are used for internal queuing configurations. WRED profiles differ from each other in the threshold values, mark probability values, and the values on which thresholds and probability are defined.

For example, consider a WRED cos-based configuration and a WRED precedence-based configuration that are identical in all respects except for one being cos-based and the other, precedence-based. The two configurations then constitute one profile. The same applies to WRED dscp configurations too. Also, two WRED configurations that are identical except for one minimum threshold configuration constitute two profiles. Similarly, differences in the maximum threshold, mark probability value, and the value on which thresholds and probability are defined also constitute different profiles.

With regard to WRED settings, you can do either of the following:

- Use the default WRED settings.
Manually configure the WRED settings.

When you configure WRED without specifying the WRED minimum threshold, maximum threshold, and MPD settings, the configuration uses the default WRED settings. When programming the ES+ module hardware, the default WRED settings ensure the application of WRED profile optimization. For details, see WRED Profile Optimization.

The ES+ module supports 12 user-defined WRED profiles in hardware for every TM. For more information, see TM - Port Mapping. If you specify the WRED settings, the WRED minimum threshold, the maximum threshold, and MPD, ensure that you do not exceed the supported number of user-defined WRED profiles that can be programmed in the ES+ hardware.

Optimize the programming of user-defined WRED settings in the following ways:

- Profile usage largely depends on the use of different WRED user-defined settings that are applied to different classes. To avoid exceeding the 12 user-defined WRED profiles hardware limit, apply the same WRED settings to each class, when possible. In this way, the WRED profile is shared between the classes. For more information, see Example for Changed Threshold Configuration.

- If a class with the same user-defined WRED configuration as another class uses a different queue-limit value, another WRED profile resource is consumed. This can occur when a parent policy queue-limit, derived from the parent shaper by default, is used to program the queue-limit for each child class based on the “bandwidth” configured for the class using Bandwidth Remaining Ratio (BRR), Bandwidth Percent (BP), or Bandwidth Remaining Percent (BRP). Use the show policy-map command to check the queue-limit set for the parent policy and the child classes. To overcome this limitation, set the same queue-limit for every parent policy, irrespective of the shaper value set in the parent policy. Please refer the Queue-limit Calculation section for details on how each child class queue limits are calculated.

  **Note** When a WRED configuration is specified, you cannot manually configure the queue-limit under the child policy class. For details, see Example for Using Queue-limit in the Parent Policy to Reduce WRED Profile Utilization.

- Include the “default” curve in the values of one of the user-defined curves. For information to do this, see the configuration steps in Configuring WRED.

  **Note** To monitor the usage of the 12 user defined WRED profiles supported by the ES+ in hardware on a TM, use the commands in Example for Default WRED Configuration.

  **Note** For information on NP (Network processor) and ES+ interface mapping, see TM - Port Mapping.

---

**Queue-limit Calculation**

Queue-limit calculation algorithm has been changed in IOS version 15.1(3)S. Formula to calculate queue-limit for a class is as follows:

- In releases before 15.1(3)S:
  
  \[ \text{queue-limit} = \text{current bitrate} \times \text{parent's available buffers} / \text{parent's allocated bandwidth}. \]

- In releases after 15.1(3)S:
Chapter 7 Configuring QoS

Configuring QoS Queue Scheduling

- queue-limit = current bitrate \* parent’s queue-limit / parent’s allocated bandwidth

In case of flat-policy, assume parent queue-limit to be 66050 (for 1G port) and 330290 (for 10G port)

In case of HQoS policy, use the same formula to calculate parent queue-limit first.

Set of predefined queue-limit values for priority and non-priority queues are below:

### Table 7-8 Priority and Non-Priority queue limits

<table>
<thead>
<tr>
<th>Queue Type</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority Queue (buffers)</td>
<td>32, 64, 128, 256, 512, 1024, 2048, 4096</td>
</tr>
<tr>
<td>Ingress Normal Queue (buffers)</td>
<td>16, 32, 48, 64, 96, 128, 192, 256, 384, 512, 768, 1024, 1536, 2K, 3K, 4K, 6K, 8K, 16K, 32K, 64K, 128K</td>
</tr>
<tr>
<td>Egress Normal Queue (buffers)</td>
<td>16, 32, 48, 64, 96, 128, 192, 256, 384, 512, 768, 1024, 1536, 2K, 3K, 4K, 6K, 8K, 16K, 32K, 64K, 128K, 256K</td>
</tr>
</tbody>
</table>

Any calculated child class queue-limit falls in between will be rounded off to the nearest value from the above table.

### WRED Profile Optimization

Release 12.2(33)SRD5 and 12.2(33)SRE2 onwards, WRED profile optimization that is specific to the default random detect configuration has been made available. Earlier, the default aggregate curve value largely depended on the parent shape rate, and ignored the queue-limit completely for the class. If the parent was configured with a shape rate of 10mbps and two classes, each class configured with a different queue-limit, they still had the same threshold despite having different queue limits. Now there are, primarily, three base WRED profiles that are predefined in hardware, along with different scale factors, to achieve the various threshold values.

The three base WRED profiles are initialized as the following:

- Queue-limits less than 512
- Queue-limits greater than 512
- Queue-limits greater than 64000

As hardware only supports values in multiples of 16, values that are not multiples of 16 do not use the same scale factor.

Profile usage largely depends on different thresholds and different mark-probabilities. The threshold, in turn, depends upon the queue-limit configuration of the class. Hence, differences in the queue limits between two classes result in two different WRED profiles. The parent queue-limit, derived from the parent shaper by default, is used to program the queue-limit for each child class based on the “bandwidth” configured for the class using either Bandwidth, Bandwidth Remaining Ratio (BRR), Bandwidth Percent (BP), or Bandwidth Remaining Percent (BRP). This queue-limit forms the basis for the programming of the default WRED profile for the class. Use the `show policy-map` command to check the queue-limit set for the parent policy and child classes.

**Note** Profile optimization is not applicable to random detect with explicit threshold configurations.
WRED Scale Factors

Default WRED configurations use the scale factor. Scale factors are used in the WRED profile to optimize WRED profile usage. To achieve different WRED minimum or maximum thresholds, scale factors can be considered multiplication factors along with base values.

Note

The usage of scale factors for the optimization of WRED profile usage is applicable only to default random-detect.

With a scale factor of three, the WRED profile is used to provide 20 combinations of unique max-threshold values which will be mapped to the different queue-limit values that are received.

Scale factor implementation is as follows:

<table>
<thead>
<tr>
<th>Profile ID</th>
<th>Scale ID</th>
<th>Min Threshold</th>
<th>Max Threshold</th>
<th>Queue Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>16</td>
<td>32</td>
<td>32</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>16</td>
<td>32</td>
<td>64</td>
</tr>
<tr>
<td>2</td>
<td>8</td>
<td>16</td>
<td>32</td>
<td>80</td>
</tr>
<tr>
<td>3</td>
<td>9</td>
<td>16</td>
<td>32</td>
<td>160</td>
</tr>
<tr>
<td>4</td>
<td>2</td>
<td>16</td>
<td>32</td>
<td>128</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>128</td>
<td>256</td>
<td>256</td>
</tr>
<tr>
<td>6</td>
<td>1</td>
<td>128</td>
<td>256</td>
<td>512</td>
</tr>
<tr>
<td>7</td>
<td>0</td>
<td>384</td>
<td>768</td>
<td>768</td>
</tr>
<tr>
<td>8</td>
<td>2</td>
<td>128</td>
<td>256</td>
<td>1024</td>
</tr>
<tr>
<td>9</td>
<td>1</td>
<td>384</td>
<td>768</td>
<td>1536</td>
</tr>
<tr>
<td>10</td>
<td>3</td>
<td>128</td>
<td>256</td>
<td>2048</td>
</tr>
<tr>
<td>11</td>
<td>2</td>
<td>384</td>
<td>768</td>
<td>3072</td>
</tr>
<tr>
<td>12</td>
<td>4</td>
<td>128</td>
<td>256</td>
<td>4096</td>
</tr>
<tr>
<td>13</td>
<td>3</td>
<td>384</td>
<td>768</td>
<td>6144</td>
</tr>
<tr>
<td>14</td>
<td>5</td>
<td>128</td>
<td>256</td>
<td>8192</td>
</tr>
<tr>
<td>15</td>
<td>4</td>
<td>384</td>
<td>768</td>
<td>12288</td>
</tr>
<tr>
<td>16</td>
<td>6</td>
<td>128</td>
<td>256</td>
<td>16384</td>
</tr>
<tr>
<td>17</td>
<td>5</td>
<td>384</td>
<td>768</td>
<td>24576</td>
</tr>
<tr>
<td>18</td>
<td>7</td>
<td>128</td>
<td>256</td>
<td>32768</td>
</tr>
<tr>
<td>19</td>
<td>6</td>
<td>384</td>
<td>768</td>
<td>49152</td>
</tr>
<tr>
<td>20</td>
<td>7</td>
<td>384</td>
<td>768</td>
<td>98304</td>
</tr>
</tbody>
</table>

A requested queue-limit of 1024 for default random-detect takes profile ID = 8 and scale ID = 2. A subsequent request for a queue-limit of 192 for default random-detect selects profile ID=5 and scale ID=0. With one WRED configuration, requests can use the same WRED profile with different scale values. If the WRED profile ID is 4, then one request takes WRED profile ID=4 and scale ID=2 and the other takes WRED profile ID=4 and scale ID=0.
Example for WRED Scale Factor Usage

The following example shows how a WRED policy is configured and then applied to an interface.

Step 1: Use a sample WRED configuration and current profile usage.

```plaintext
class-map match-all c1_test
  match ip dscp cs5
!
class-map match-all c2_test
  match ip dscp 33
!
class-map match-all c3_test
  match ip dscp af31
!
policy-map CHILD_WRED
  class c1_test
    bandwidth percent 30
    random-detect
  class c2_test
    bandwidth percent 18
    random-detect
  class c3_test
    bandwidth percent 6
    random-detect
policy-map PARENT_WRED
  class class-default
    shape average 25000000
    service-policy CHILD_WRED
```

Router# attach module 10
Router-dfc10# show plat hardware qos np 0 prof res
* WFQ profiles at TM level3 and level4 belong to one common pool. Profile usage is shared between the entities at L3 and L4 layers; hence same WFQ profile Total and Used counts are shown in the below output.

<table>
<thead>
<tr>
<th>Shaper</th>
<th>wfq</th>
<th>wred</th>
</tr>
</thead>
<tbody>
<tr>
<td>np</td>
<td>tm</td>
<td>level</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>L4</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>L3</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>L2</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>L1</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>L4</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>L3</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>L2</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>L1</td>
</tr>
<tr>
<td>0</td>
<td>2</td>
<td>L4</td>
</tr>
<tr>
<td>0</td>
<td>2</td>
<td>L3</td>
</tr>
<tr>
<td>0</td>
<td>2</td>
<td>L2</td>
</tr>
<tr>
<td>0</td>
<td>2</td>
<td>L1</td>
</tr>
</tbody>
</table>

Policy:
max used
--------------------
256 0
Router-dfc10# exit

Step 2: Apply the configured WRED policy to an interface.
interface GigabitEthernet10/3
no ip address
mpls propagate-cos
service-policy output PARENT_WRED

Router# show policy-map int e gig10/3 | inc Class-map|queue limit
Class-map: class-default (match-any)
  queue limit 6144 packets
  Class-map: c1_test (match-all)
    queue limit 2048 packets
    <<<<<<<<<<&&Q-limit for c1_test
  class-map
  Class-map: c2_test (match-all)
    queue limit 1024 packets
    <<<<<<<<<<&&Q-limit for c2_test
  class-map
  Class-map: c3_test (match-all)
    queue limit 384 packets
    <<<<<<<<<<&&Q-limit for c3_test
  class-map
Class-map: class-default (match-any)
  queue limit 3072 packets

Router# attach module 10
Router-dfc10# show plat hardware qos np 0 prof res
* WFQ profiles at TM level3 and level4 belong to one common pool. Profile usage is shared between the entities at L3 and L4 layers; hence same WFQ profile Total and Used counts are shown in the below output.

<table>
<thead>
<tr>
<th>np</th>
<th>tm</th>
<th>level</th>
<th>Shaper total/used</th>
<th>wfg total/used</th>
<th>wred total/used</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>L4</td>
<td>64/1</td>
<td>64/1*</td>
<td>12/0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>L3</td>
<td>256/6</td>
<td>64/1*</td>
<td>n/a</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>L2</td>
<td>32/3</td>
<td>16/1</td>
<td>n/a</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>L1</td>
<td>32/1</td>
<td>32/1</td>
<td>n/a</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>np</th>
<th>tm</th>
<th>level</th>
<th>Shaper total/used</th>
<th>wfg total/used</th>
<th>wred total/used</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>L4</td>
<td>64/0</td>
<td>64/6*</td>
<td>12/1</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>L3</td>
<td>256/2</td>
<td>64/6*</td>
<td>n/a</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>L2</td>
<td>32/1</td>
<td>16/1</td>
<td>n/a</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>L1</td>
<td>32/1</td>
<td>32/1</td>
<td>n/a</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>np</th>
<th>tm</th>
<th>level</th>
<th>Shaper total/used</th>
<th>wfg total/used</th>
<th>wred total/used</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>2</td>
<td>L4</td>
<td>64/0</td>
<td>64/1*</td>
<td>12/0</td>
</tr>
<tr>
<td>0</td>
<td>2</td>
<td>L3</td>
<td>256/1</td>
<td>64/1*</td>
<td>n/a</td>
</tr>
<tr>
<td>0</td>
<td>2</td>
<td>L2</td>
<td>32/1</td>
<td>16/1</td>
<td>n/a</td>
</tr>
<tr>
<td>0</td>
<td>2</td>
<td>L1</td>
<td>32/1</td>
<td>32/1</td>
<td>n/a</td>
</tr>
</tbody>
</table>

Police :
max used
-------------------------------
256 0

Router-dfc10# exit

Router# attach module 10
Router-dfc10# show plat npc qos action np 0 interface gigabitEthernet 10/3 output queue | inc WRED|Level 4:

GigabitEthernet10/3 - if_number 65 0 policymap PARENT_WRED dir Output
  policymap CHILD_WRED classid 1 dfs classid 0 class index 0
  Shape mode/factor: Unshaped/One Profiles- WRED/Scale:4/2 Shape:0 WFQ:2
  policymap CHILD_WRED classid 2 dfs classid 1 class index 1
  Shape mode/factor: Unshaped/One Profiles- WRED/Scale:4/1 Shape:0 WFQ:3
  policymap CHILD_WRED classid 3 dfs classid 2 class index 2
Configuring QoS Queue Scheduling

The example shows scale factor usage:

- Class c1_test has queue limit = 2048, so the max limit = queue limit/2 = 1024. So, it will select a scale profile from the 20 scale profiles listed above: Scale id=8, min threshold=128, max threshold=256, scale profile=2. (The WRED profile id = 4 and scale factor = 2.)
- Class c2_test has queue limit = 1024, so max limit = queue limit/2 = 512. So, it will select a scale profile from the 20 scale profiles listed above: Scale id=6, min threshold=128, max threshold=256, scale profile=1. (The WRED profile id = 4 and the scale factor = 1.)
- Class c3_test has queue limit = 384, so the max limit = queue limit/2 = 192. It selects a scale profile from the 20 scale profiles listed above: Scale id=5, min threshold=128, max threshold=256, scale profile = 0. (In this case, the WRED profile id = 4 and scale factor = 0.)

Note

Scale factors are not supported for all scenarios e.g. using service-groups + service-policies in HQF. If interface service-policy configured before service-group, then scale factors are used. However, the order of the running and start-up configuration places groups prior to service-policy and consequently scale factors are not implemented. Any higher scale w.r.t to scale factors would not be persistent after reload. So, it's recommended to use "group <service-group-id>" prior to "service-policy <direction> <service-policy-name>" under the interface configuration.

Example for Default WRED Configuration

```
Policy-map details
 =====================
RSP#sh running-config policy-map hqosparent
Building configuration...
Current configuration : 107 bytes
!
policy-map hqosparent
 class class-default
 shape average 100000000
 service-policy hqoschild
!
end

RSP#sh running-config policy-map hqoschild
Building configuration...
Current configuration : 155 bytes
!
policy-map hqoschild
 class cos0
 bandwidth remaining percent 10
 random-detect
 class cos1
```
bandwidth remaining percent 30
random-detect
!
end

Sh Policy-map interface
==========================

- Here we have a parent policy with shaper action
- The queue limit in the child classes are calculated as per the parent shaper
- According to that the thresholds are calculated and WRED profiles are determined
- From the output below you can see that for the first threshold values, max threshold will
  be half the queue-limit and min threshold half of max threshold.

RSP#sh policy-map interface gig8/5
GigabitEthernet8/5

Service-policy output: hqosparent

Counters last updated 00:02:56 ago

Class-map: class-default (match-any)
 0 packets, 0 bytes
5 minute offered rate 0000 bps, drop rate 0000 bps
Match: any
Queueing
queue limit 32768 packets
(queue depth/total drops/no-buffer drops) 0/0/0
(pkts output/bytes output) 0/0
shape (average) cir 100000000, bc 400000, be 400000
target shape rate 100000000

Service-policy: hqoschild

Counters last updated 00:02:56 ago

Class-map: cos0 (match-all)
 0 packets, 0 bytes
5 minute offered rate 0000 bps, drop rate 0000 bps
Match: cos 0
Queueing
queue limit 3072 packets
(queue depth/total drops/no-buffer drops) 0/0/0
(pkts output/bytes output) 0/0
bandwidth remaining 10%
Exp-weight-constant: 9 (1/512)
Mean queue depth: 0 packets

<table>
<thead>
<tr>
<th>class</th>
<th>Random drop</th>
<th>Tail drop</th>
<th>Minimum thresh</th>
<th>Maximum thresh</th>
<th>Mark prob</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0/0</td>
<td>0/0</td>
<td>768</td>
<td>1536</td>
<td>1/10</td>
</tr>
<tr>
<td>1</td>
<td>0/0</td>
<td>0/0</td>
<td>864</td>
<td>1536</td>
<td>1/10</td>
</tr>
<tr>
<td>2</td>
<td>0/0</td>
<td>0/0</td>
<td>960</td>
<td>1536</td>
<td>1/10</td>
</tr>
<tr>
<td>3</td>
<td>0/0</td>
<td>0/0</td>
<td>1056</td>
<td>1536</td>
<td>1/10</td>
</tr>
<tr>
<td>4</td>
<td>0/0</td>
<td>0/0</td>
<td>1152</td>
<td>1536</td>
<td>1/10</td>
</tr>
<tr>
<td>5</td>
<td>0/0</td>
<td>0/0</td>
<td>1248</td>
<td>1536</td>
<td>1/10</td>
</tr>
<tr>
<td>6</td>
<td>0/0</td>
<td>0/0</td>
<td>1344</td>
<td>1536</td>
<td>1/10</td>
</tr>
<tr>
<td>7</td>
<td>0/0</td>
<td>0/0</td>
<td>1440</td>
<td>1536</td>
<td>1/10</td>
</tr>
</tbody>
</table>

Class-map: cos1 (match-all)
 0 packets, 0 bytes
5 minute offered rate 0000 bps, drop rate 0000 bps
Match: cos 1
Queueing
queue limit 8192 packets
(queue depth/total drops/no-buffer drops) 0/0/0
(pkts output/bytes output) 0/0
bandwidth remaining 30%
Exp-weight-constant: 9 (1/512)
Mean queue depth: 0 packets

<table>
<thead>
<tr>
<th>class</th>
<th>Random drop</th>
<th>Tail drop</th>
<th>Minimum</th>
<th>Maximum</th>
<th>Mark</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>pkts/bytes</td>
<td>pkts/bytes</td>
<td>thresh</td>
<td>thresh</td>
<td>prob</td>
</tr>
<tr>
<td>0</td>
<td>0/0</td>
<td>0/0</td>
<td>2048</td>
<td>4096</td>
<td>1/10</td>
</tr>
<tr>
<td>1</td>
<td>0/0</td>
<td>0/0</td>
<td>2304</td>
<td>4096</td>
<td>1/10</td>
</tr>
<tr>
<td>2</td>
<td>0/0</td>
<td>0/0</td>
<td>2560</td>
<td>4096</td>
<td>1/10</td>
</tr>
<tr>
<td>3</td>
<td>0/0</td>
<td>0/0</td>
<td>2816</td>
<td>4096</td>
<td>1/10</td>
</tr>
<tr>
<td>4</td>
<td>0/0</td>
<td>0/0</td>
<td>3072</td>
<td>4096</td>
<td>1/10</td>
</tr>
<tr>
<td>5</td>
<td>0/0</td>
<td>0/0</td>
<td>3328</td>
<td>4096</td>
<td>1/10</td>
</tr>
<tr>
<td>6</td>
<td>0/0</td>
<td>0/0</td>
<td>3584</td>
<td>4096</td>
<td>1/10</td>
</tr>
<tr>
<td>7</td>
<td>0/0</td>
<td>0/0</td>
<td>3840</td>
<td>4096</td>
<td>1/10</td>
</tr>
</tbody>
</table>

Class-map: class-default (match-any)
0 packets, 0 bytes
5 minute offered rate 0000 bps, drop rate 0000 bps
Match: any
queue limit 16384 packets
(queue depth/total drops/no-buffer drops) 0/0/0
(pkts output/bytes output) 0/0
RSP#
RSP# attach module 8
RSP-dfc8#sh platform hardware qos np 0 profile resources
* WFQ profiles at TM level3 and level4 belong to one common pool.
Profile usage is shared between the entities at L3 and L4 layers;
hence same WFQ profile Total and Used counts are shown in the
below output.

<table>
<thead>
<tr>
<th>np</th>
<th>tm</th>
<th>level</th>
<th>Shaper</th>
<th>wfg</th>
<th>wred</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>total/used</td>
<td>total/used</td>
<td>total/used</td>
</tr>
<tr>
<td>----</td>
<td>----</td>
<td>-------</td>
<td>-----------</td>
<td>-----------</td>
<td>-----------</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>L4</td>
<td>64/1</td>
<td>64/1*</td>
<td>12/0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>L3</td>
<td>256/6</td>
<td>64/1*</td>
<td>n/a</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>L2</td>
<td>32/3</td>
<td>16/1</td>
<td>n/a</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>L1</td>
<td>32/1</td>
<td>32/1</td>
<td>n/a</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>np</th>
<th>tm</th>
<th>level</th>
<th>Shaper</th>
<th>wfg</th>
<th>wred</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>total/used</td>
<td>total/used</td>
<td>total/used</td>
</tr>
<tr>
<td>----</td>
<td>----</td>
<td>-------</td>
<td>-----------</td>
<td>-----------</td>
<td>-----------</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>L4</td>
<td>64/0</td>
<td>64/4*</td>
<td>12/2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>L3</td>
<td>256/2</td>
<td>64/4*</td>
<td>n/a</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>L2</td>
<td>32/1</td>
<td>16/1</td>
<td>n/a</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>L1</td>
<td>32/1</td>
<td>32/1</td>
<td>n/a</td>
</tr>
</tbody>
</table>

Police :
max    used
---------
256     0
RSP-dfc8#exit
Note

Service-policy configuration update would take few seconds to program the hardware and reflect in the internal counters. So, please wait few seconds before executing the command “show platform hardware qos np <np_num> profile resources” to reflect the updated values.

Example for Changed Threshold Configuration

The following sample configuration shows that the (highlighted) threshold configuration can be changed to have the same threshold. Having the same threshold results in reduction WRED profile usage.

```plaintext
interface Gig10/3
    service-policy out WRED_DEMO
policy-map WRED_DEMO
    class routing
        bandwidth percent 1
    class bph
        bandwidth percent 39
        random-detect dscp-based aggregate
        random-detect dscp values 18 minimum-thresh 96 maximum-thresh 192 mark-prob 5
        random-detect dscp values 20 minimum-thresh 128 maximum-thresh 192 mark-prob 10
        random-detect dscp values 10 12 minimum-thresh 150 maximum-thresh 200 mark-prob 5
    class bp1
        bandwidth percent 20
        random-detect dscp-based aggregate
        random-detect dscp values 18 minimum-thresh 96 maximum-thresh 192 mark-prob 5
        random-detect dscp values 20 minimum-thresh 128 maximum-thresh 192 mark-prob 10
        random-detect dscp values 10 12 minimum-thresh 130 maximum-thresh 200 mark-prob 5
    class class-default
        bandwidth percent 10
        random-detect dscp-based aggregate
        random-detect dscp values 0 minimum-thresh 48 maximum-thresh 96 mark-prob 5
        random-detect dscp values 8 minimum-thresh 64 maximum-thresh 96 mark-prob 10
```

Example for Using Queue-limit in the Parent Policy to Reduce WRED Profile Utilization

The following sample configuration shows that the same (highlighted) queue-limit configuration is being used by the 2 parent policies that have different shaper rates applied. This ensures that the WRED profile resources of the child policy are shared by the 2 parent policies.

```plaintext
policy-map hqosparent_1
    class class-default
        shape average 6328000
        queue-limit 100000 packets
        service-policy output hqoschild
    !
policy-map hqosparent_2
    class class-default
        shape average 200000000
        queue-limit 100000 packets
        service-policy output hqoschild
    !
policy-map hqoschild
    class class1
        bandwidth remaining percent 1
        random-detect dscp-based aggregate minimum-thresh 800 maximum-thresh 1600 mark-prob 1
```
class class2
police 64000 8000 8000 conform-action transmit exceed-action transmit violate-action transmit
bandwidth remaining percent 1
random-detect dscp-based aggregate minimum-thresh 800 maximum-thresh 1600 mark-prob 1
class class3
police cir 1000000000 bc 125000000 be 125000000 conform-action set-dscp-transmit ef
exceed-action drop violate-action drop
priority
class class4
police cir 900000000 bc 112500000 be 112500000 conform-action set-dscp-transmit af31
exceed-action set-dscp-transmit af32 violate-action set-dscp-transmit af32
bandwidth remaining percent 59
random-detect dscp-based aggregate minimum-thresh 800 maximum-thresh 1600 mark-prob 1
random-detect exponential-weighting-constant 1
random-detect dscp values 26 minimum-thresh 3200 maximum-thresh 4800 mark-prob 1
random-detect dscp values 28 minimum-thresh 2400 maximum-thresh 3200 mark-prob 1
class class5
police cir 450000000 bc 56250000 be 56250000 conform-action set-dscp-transmit af21
exceed-action set-dscp-transmit af22 violate-action set-dscp-transmit af22
bandwidth remaining percent 30
random-detect dscp-based aggregate minimum-thresh 800 maximum-thresh 1600 mark-prob 1
random-detect exponential-weighting-constant 1
random-detect dscp values 18 minimum-thresh 3200 maximum-thresh 4800 mark-prob 1
random-detect dscp values 20 minimum-thresh 2400 maximum-thresh 3200 mark-prob 1
class class6
police cir 150000000 bc 187500000 be 187500000 conform-action set-dscp-transmit default
exceed-action set-dscp-transmit default violate-action set-dscp-transmit default
bandwidth remaining percent 9
random-detect dscp-based aggregate minimum-thresh 800 maximum-thresh 1600 mark-prob 1
random-detect exponential-weighting-constant 1

! interface GigabitEthernet8/12.1
service-policy output hqosparent_1
!
interface GigabitEthernet8/12.2
service-policy output hqosparent_2
!

**TM - Port Mapping**

Traffic Manager (TM) is a queuing application-specific integrated circuit (ASIC) of the network processor (NP). TM ensures that critical traffic get preferential treatment through a scheduler.

For different versions of an ES+ line card, some interfaces that are mapped to the same NP share the same TM. As the 12 unique profile limit works per TM, you may also overcome the limit by spreading the interface across different TMs.

**TM-Port Mapping** tabulates TM to port mapping.

<table>
<thead>
<tr>
<th>Table 7-10</th>
<th>TM-Port Mapping</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>4x10G</td>
</tr>
<tr>
<td>NP0, TMb</td>
<td>1</td>
</tr>
<tr>
<td>NP0, TMc</td>
<td>5</td>
</tr>
<tr>
<td>NP1, TMb</td>
<td>2</td>
</tr>
<tr>
<td>NP1, TMc</td>
<td>6</td>
</tr>
</tbody>
</table>
Chapter 7  Configuring QoS

Configuring QoS Queue Scheduling

Note
TMb is used for one set-up of ports, and TMc is used for another set-up of ports depending on the line card used, as shown in the table. When a line card uses both TMb and TMc, the two TMs share the 12 WRED profiles.

<table>
<thead>
<tr>
<th></th>
<th>4x10G</th>
<th>8x10G</th>
<th>2x10G</th>
<th>40x1G</th>
<th>20x1G</th>
<th>20x1G_2x10G</th>
<th>10x1G_1x10G</th>
</tr>
</thead>
<tbody>
<tr>
<td>NP2</td>
<td>TMb</td>
<td>3</td>
<td>3</td>
<td>21-25</td>
<td>1-5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NP2</td>
<td>TMc</td>
<td>7</td>
<td></td>
<td>26-30</td>
<td>6-10</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NP3</td>
<td>TMb</td>
<td>4</td>
<td>4</td>
<td>31-35</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NP3</td>
<td>TMc</td>
<td>8</td>
<td></td>
<td>36-40</td>
<td>22</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Details on WRED Resource Usage Shared TM Usage

In case of 10G ES+, both TMb and TMc uses shared mode for profile allocation in egress direction.

TM selection criteria in shared mode are as follows:

- Without 'group <service-group-id>' under interface configuration, always TMb is selected
- With 'group <service-group-id>' under interface configuration, lowest used (in terms of 'group' and 'service-policy' configs) TM is selected.
- All service-policies under same service-group are allocated resources in the one TM. So, the same WRED profile parameters configured under two service-groups if allocated in different TMs would use distinct resources.

Order of sub-interface configuration at the time of router boot-up/reload is in ascending order of sub-interface number. For instance, if user configures sub-interfaces in order Te1/1.9, Te1/1.2, Te1/1.4, Te1/1.10, and after reload, router configures sub-interfaces in ascending order i.e. Te1/1.2, Te1/1.4, Te1/1.9, Te1/1.10. Since the TM selection for new service-group depends on the current usage, the resources used may differ before and after reload depending upon the configuration.

So, for 10G ES+, it's recommended for user to configure to consume maximum 12 WRED profiles per NP.

Configuring Bandwidth and CBWFQ

Class-based weighted fair queuing (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 the following interfaces:

- Main Layer 3 interface
- Layer 3 subinterface
- Switchport interfaces
- Service instances
- Port-channel service instances
Port-channel Layer 3 member link

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.

Effective from Cisco IOS Release 15.1(1)S, the layer 3 and layer 4 level WFQ profiles belong to one hardware pool and can be commonly used among the layers.

**Calculating commit-weight and excess-weight**

Use the following formula to calculate weight for bandwidth:

Commit weight = (Bandwidth of the class) x (Maximum weight allowed at the level) / (Parent bandwidth).

Commit weight is then rounded to integer value based on optimizations allowed by hardware.

Excess weight = Commit weight (at layer 4 level).

---

**Note**

At layer 4 level, if no truncation error appears for (Bandwidth of class) x 100 / (Parent bandwidth), for all child-classes, then the maximum weight used for calculation would be 100 instead of 1020.

Use the following formula to calculate weight for bandwidth percent:

Commit weight = (Bandwidth percent of class) x (Maximum weight allowed at the level).

Commit weight is then rounded to integer value based on optimizations as allowed by hardware.

Excess weight = Commit weight (at layer 4 level).

---

**Note**

At layer 4 level, if no truncation error appears for (Bandwidth of class) x 100 / (Parent bandwidth), for all child-classes, then the maximum weight used for calculation would be 100 instead of 1020.

Use the following formula to calculate weight for remaining bandwidth percent:

Calculate weights for the remaining bandwidth percent by first calculating the remaining bandwidth under a policy-map and then allotting this bandwidth for each class based on its remaining bandwidth percent. Once this remaining bandwidth for a class is known, the excess weight is calculated as:

Excess weight = (Bandwidth remaining allotted to the class) x (Maximum weight allowed at the level) / (Parent bandwidth).

Excess weight is then rounded to integer value based on optimizations as allowed by hardware.

Commit weight = Excess weight (at layer 4 level).

---

**Note**

At layer 4 level, if no truncation error appears for (Bandwidth of class) x 100 / (Parent bandwidth), for all child-classes, then the maximum weight used for calculation would be 100 instead of 1020.

Use the following formula to calculate weight for Bandwidth Remaining Ratio (BRR):

Excess weight = (BRR of class) subject to maximum weight at the level.

Excess weight is then rounded to integer value based as allowed by hardware.
Commit weight = Excess weight (at layer 4 level).

Table 7-11 lists the maximum and allowed weights at various levels:

<table>
<thead>
<tr>
<th>TM Entity Level</th>
<th>Maximum Weight</th>
<th>Allowed Weights</th>
</tr>
</thead>
<tbody>
<tr>
<td>L4</td>
<td>1020</td>
<td>1.. 255, 256, 260, 264.. 1020</td>
</tr>
<tr>
<td>L3</td>
<td>1020</td>
<td>1.. 255, 256, 260, 264.. 1020</td>
</tr>
<tr>
<td>L2</td>
<td>255</td>
<td>1.. 255</td>
</tr>
<tr>
<td>L1</td>
<td>255</td>
<td>1.. 255</td>
</tr>
</tbody>
</table>

Restrictions and Usage Guidelines

When configuring Bandwidth and CBWFQ on Cisco 7600 Series ES+ line cards, follow these restrictions and usage guidelines:

- The `bandwidth kbps` and `bandwidth percent x%` commands are supported.
- On ingress, the `bandwidth kbps`, `bandwidth remaining ratio`, `bandwidth remaining percent`, and `bandwidth percent x%` commands are supported on the main Layer 3 interface, the Layer 3 subinterface, and on service instances.
- The `bandwidth remaining percent` command is supported at the child level. The `bandwidth remaining ratio` command is supported at the parent and child level.
- Excluding port channel service instances, bandwidth is supported on the input for H-QoS only. Ingress queuing is not supported for port channel service instances.
- The `bandwidth` command used within a QoS policy-map must be consistent across classes. For example, class1 with `bandwidth kbps` and class2 with `bandwidth remaining ratio` in the same policy-map is not supported.
- The total unique bandwidth profiles used across layer 3 and layer 4 cannot exceed 64.

```
Note
The consistency need not be maintained between parent and child policy-maps. For example, parent with `bandwidth remaining ratio` and child with `bandwidth kbps` is supported.
```

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `policy-map policy-name`
4. `class {class-name | class-default}`
5. `bandwidth {bandwidth-kbps | percent percent | remaining {ratio ratio | percent percent}}`
## Detailed Steps

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><strong>enable</strong>&lt;br&gt;Enables privileged EXEC mode.  &lt;br&gt;• Enter your password if prompted.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router# enable</td>
</tr>
<tr>
<td>Step 2</td>
<td><strong>configure terminal</strong>&lt;br&gt;Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router# configure terminal</td>
</tr>
<tr>
<td>Step 3</td>
<td><strong>policy-map policy-map-name</strong>&lt;br&gt;Creates or modifies a traffic policy and enters policy-map configuration mode, where:&lt;br&gt;• <em>policy-map-name</em>—Specifies the name of the traffic policy to configure. Names can be a maximum of 40 alphanumeric characters.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config)# policy-map policy1</td>
</tr>
<tr>
<td>Step 4</td>
<td>**class (class-name</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config)# class c3</td>
</tr>
<tr>
<td>Step 5</td>
<td>**bandwidth (bandwidth-kbps</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-pmap-c)# bandwidth 20000</td>
</tr>
</tbody>
</table>

## Examples

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
```
Configuring QoS

Queue Scheduling

Chapter 7

Configuring QoS

Queue Scheduling

Chapter 7

Configuring QoS

Queue Scheduling

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)# class class2
Router(config-pmap-c)# bandwidth 20000
Router(config-pmap-c)# exit
Router(config-pmap)# class class3
Router(config-pmap-c)# exit
Router(config)#
Router(config)# interface gigabit ethernet 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
```

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

```
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)# interface gigabit ethernet 2/1
Router(config-if)# service-policy output policy1
```

Use the following commands to verify CBWFQ:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router# show policy-map policy-map</td>
<td>Displays the configuration of all classes that make up the specified policy-map.</td>
</tr>
<tr>
<td>Router# show policy-map policy-map class class-name</td>
<td>Displays the configuration of the specified class of the specified policy-map.</td>
</tr>
</tbody>
</table>
Configuring LLQ

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
- Switchport interfaces
- Service instances
- Port-channel service instances
- Port-channel Layer 3 member link

Restrictions and Usage Guidelines

When configuring LLQ on Cisco 7600 Series ES+ line cards, follow these restrictions and usage guidelines:

- **Ingress LLQ**
  - Dual Priority Queues (High, Medium and Data)
  - 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.
  - Flat policy map with LLQ is not supported.

- **Egress LLQ**
  - Dual Priority Queues
  - 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.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router# <code>show policy-map interface interface-name</code></td>
<td>Displays the configuration of all classes configured for all policy-maps on the specified interface.</td>
</tr>
<tr>
<td>Router# <code>show queue interface-type interface-number</code></td>
<td>Displays queueing configuration and statistics for a particular interface.</td>
</tr>
</tbody>
</table>
• Egress LLQ
  – Dual Priority Queues (High, Medium and Data)
  – LLQ configuration is allowed only at the leaf policy-map.
  – The `priority` and `priority level` commands are supported but you cannot use both in the same policy-map.
  – Basic Priority/Low Latency Queue with percent is not supported.
  – Basic Low Latency Queue with percent is not supported.
  – Priority queue with bit rates is not supported.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `policy-map policy-name`
4. `class {class-name | class-default}`
5. `police bps-value conform-action action exceed-action action`
   or
   `police cir percent % conform-action action exceed-action action`
   or
   `police cir bps-value pir bps-value conform-action action exceed-action action violate-action action`
   or
   `police cir percent % pir percent % conform-action action exceed-action action violate-action action`
6. `priority`
   or
   `priority level`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 <code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: <code>Router# enable</code></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Step 2 <code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: <code>Router# configure terminal</code></td>
<td></td>
</tr>
</tbody>
</table>
### Chapter 7 Configuring QoS

#### Configuring QoS Queue Scheduling

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>policy-map policy-name</strong>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Router(config)# policy-map silver</td>
</tr>
<tr>
<td>Specifies the name of the policy-map to configure.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>**class (class-name</td>
</tr>
<tr>
<td>Specifies the name of a predefined class included in the service policy.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><strong>police bps-value conform-action action exceed-action action</strong>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Router(config-pmap-c)# police 5000000 conform-action set-dscp-transmit 0 exceed-action drop</td>
</tr>
<tr>
<td>Specifies a maximum bandwidth usage by a traffic class through the use of a token bucket algorithm, where:&lt;br&gt;• <strong>bps-value</strong>—Specifies the average rate in bits per second. Valid values are 64000 to 200000000.&lt;br&gt;• <strong>action</strong>—Specifies the he actions that are taken on a packet when it conforms or exceeds. The possible actions are shown in Table 7-5.</td>
<td></td>
</tr>
</tbody>
</table>

Or

| **police cir percent conform-action action exceed-action action**<br>**Example:**<br>Router(config-pmap-c)# police cir percent 20 conform-action transmit exceed-action set-prec-transmit 1 |
| Configures traffic policing on the basis of a percentage of bandwidth available on an interface, where:<br>• **cir**—Specifies the committed information rate. Indicates that the CIR will be used for policing traffic.<br>• **percent**—Specifies that a percentage of bandwidth will be used for calculating the CIR.<br>• **%**—Specifies the CIR bandwidth percentage. Valid values are 1 to 100.<br>• **action**—Specifies the he actions that are taken on a packet when it conforms or exceeds. The possible actions are shown in Table 7-5. |

Or

| **police cir bps-value pir bps-value conform-action action exceed-action action violate-action action**<br>**Example:**<br>Router(config-pmap-c)# police cir 1000000 pir 2000000 conform-action set-cos-transmit 3 exceed-action set-cos-transmit 1 violate-action drop |
| Configures traffic policing using two rates, the CIR and the PIR, where:<br>• **cir**—Specifies the committed information rate. Indicates that the CIR will be used for policing traffic.<br>• **pir**—Specifies the peak information rate. Indicates that the PIR will be used for policing traffic.<br>• **bps-value**—Specifies the average rate in bits per second. Valid values are 64000 to 200000000.<br>• **action**—Specifies the he actions that are taken on a packet when it conforms or exceeds. The possible actions are shown in Table 7-5. |
Chapter 7 Configuring QoS

Configuring QoS Queue Scheduling

Examples

The following example configures an output LLQ policy on a switchport interface that matches on a CoS value queuing defined in the classes.

Router# enable
Router# configure terminal
Router(config)# policy map switchport-llq-policy
Router(config-pmap)# class cos0
Router(config-pmap-c)# police 500000000
Router(config-pmap-c)# priority

Now the policy is applied to the interface.

Router# enable
Router# configure terminal
Router(config)# interface TenGigabitEthernet9/1
Router(config-if)# switchport
Router(config-if)# switchport access vlan 2000
Router(config-if)# switchport mode access
Router(config-if)# service-policy output switchport-llq-policy

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 50000000
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 DBUS CoS Queuing

This feature allows you to configure which DBUS CoS values are mapped to the high-priority queue. The `hw-module slot slot queue priority switch-fpga output cos values|none` command is used on the Routing Processor (RP) to configure the priority values. You can change the priority by changing the CoS values. The system allows you to configure eight class-of-service values. The default CoS values are 5, 6, and 7.

Configuring Bandwidth Remaining Ratio (BRR)

Bandwidth Remaining Ratio (BRR) specifies the ratio that bandwidth is split between users when the link is congested (oversubscribed). This feature allows the link rate to be prorated out to logical interfaces such as EVCs and L3 subinterfaces. This feature is needed by the user since it provides the ability to oversubscribe the shape rate so logical interfaces can utilize unused bandwidth of other logical interfaces.

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

Restrictions and Usage Guidelines

When configuring BRR on the Cisco 7600 Series ES+ line card, follow these restrictions and usage guidelines:

- You can configure Bandwidth Remaining Ratio as an action in the policy-map of a parent or a child class. BRR can be configured to a minimum ratio of 1 and maximum of 1000 on a logical interface.
- Because there is no support for an implicit BRR of 1, you must explicitly configure a BRR of 1 on policies. This does not mean that a BRR of 1 is required in an LLQ class (LLQ and CBWFQ configurations in the same class will be rejected by the CLI). A child level BRR automatically excludes LLQ classes from participating in bandwidth sharing because LLQ classes have bandwidth guarantees.
- Use the `bandwidth remaining ratio number` command to configure BRR. The larger the number, the more bandwidth the logical interface that the QoS policy-map is applied to receives when the link is congested.
• BRR at the parent level of an HQoS policy-map will functions if the port is congested with traffic. If the total traffic on the port is lower than the link bandwidth, then all the traffic that comes in has sufficient bandwidth to go out, and there is no necessity for BRR.

• For BRR on the ES+ line cards, the bandwidth sharing calculation is dynamic. BRR calculations are updated regularly so that as the traffic profile changes, the bandwidth sharing changes.

• BRR between flat and H-QoS policy-maps is not supported.

• BRR configurations for a child policy-map and a parent policy-map are similar. However, at the child level the congestion level that initiates BRR calculations are shifted from the physical port level to the parent shaper level.

• At parent level, you must configure the shaper along with BRR for BRR to work.

• BRR is supported on port channel service instances and port-channel member links (Layer 3). The ratios are maintained between all service instances load balanced on a member link. For example, if service instances 1, 2, and 3 were load balanced to link Gi1/1 and service instances 4 and 5 to link Gi1/2, then BRR ratios would be maintained between service instances 1, 2, and 3 on Gi1/1 and between 4 and 5 on link Gi1/2.

• The ES+ line card supports service propagation. When a port is congested in egress, service propagation splits the bandwidth remaining on the link between users in the configured ratio after all LLQ traffic has been serviced.
  - Service propagation is always on.
  - Service propagation is turned on automatically when there is no bandwidth guarantee in the parent.

• In order to avoid running out of buffer space on an ES+ line card, it is strongly recommended that the queue-limit num of pkts command is configured for each child class queue, where num of pkts is a number reasonable for the queue. Failure to configure the queue-limit command can result in distorted BRR ratios on sending traffic.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. policy-map policy-name
4. class {class-name | class-default}
5. shape average cir [bc] [be]
6. bandwidth remaining ratio ratio
7. service-policy policy-map
## Chapter 7  Configuring QoS

### Configuring QoS Queue Scheduling

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| 1    | enable  | Enables privileged EXEC mode.  
• Enter your password if prompted. |
|      | Example: | Router# enable |
| 2    | configure terminal | Enters global configuration mode. |
|      | Example: | Router# configure terminal |
| 3    | policy-map policy-name | Specifies the name of the policy-map to configure. |
|      | Example: | Router(config)# policy-map silver |
| 4    | class (class-name | class-default) | Specifies the name of a predefined class included in the service policy. |
|      | Example: | Router(config-pmap)# class classcos0 |
| 5    | shape average cir [bc] [be] | Specifies average or peak rate traffic shaping. |
|      | Example: | Router(config-pmap-c)# shape average 10000000 |
| 6    | bandwidth remaining ratio ratio | Specifies a bandwidth-remaining ratio for class-level or subinterface-level queues to be used during congestion to determine the amount of excess bandwidth (unused by priority traffic) to allocate to non-priority queues.  
**Note**  The value of ratio is between 1 to 1000. |
|      | Example: | Router(config-pmap-c)# bandwidth remaining ratio 2 |
| 7    | service-policy policy-map | Attaches a policy-map to a class. |
|      | Example: | Router(config-pmap-c)# service-policy cust2-classes |

### Examples

In the following configuration, three policy-maps are applied in egress on three service instances. If gold, silver, and bronze service instances send their full quota of 300, 300, and 100 Mb/s of priority traffic, then because PRP/service propagation is ON, the remaining (1 Gb/s - 700 Mb/s) 300 Mb/s of link bandwidth is shared between users in the ratio 1 : 2 : 3 where:

- User A gets: \(1 / (1+2+3) \times 300 \text{ Mb/s} = 50 \text{ Mb/s} \) of non-LLQ traffic
- User B gets: \(2 / (1+2+3) \times 300 \text{ Mb/s} = 100 \text{ Mb/s} \) of non-LLQ traffic
- User C gets: \(3 / (1+2+3) \times 300 \text{ Mb/s} = 150 \text{ Mb/s} \) of non-LLQ traffic

Router# enable  
Router# configure terminal  
Router(config)# policy-map data_gold_child_out
Configuring PFC QoS on a Cisco 7600 Series Ethernet Services Plus Line Card

The Cisco 7600 Series ES+ line card supports most of the same QoS features as those supported by the Policy Feature Card (PFC) on the Cisco 7600 series routers.

This section describes those QoS features that have Cisco 7600 Series ES+ line card-specific configuration guidelines. After you review the Cisco 7600 Series ES+ line card-specific guidelines described in this document, then refer to the Cisco 7600 Series Router Cisco IOS Software Configuration Guide, Release 15.0SR located at the following URL:


Router(config-pmap)# class video
Router(config-pmap-c)# priority
Router(config-pmap-c)# police 300000000
Router(config-pmap-c)# set cos 4
Router(config-pmap)# class class-default
Router(config-pmap-c)# set cos 3

Router(config)# policy-map data_gold_parent_out
Router(config-pmap)# class class-default
Router(config-pmap-c)# shape average 500000000
Router(config-pmap-c)# bandwidth remaining ratio 3
Router(config-pmap-c)# service-policy data_gold_child_out

Router(config)# policy-map data_silver_child_out
Router(config-pmap)# class video
Router(config-pmap-c)# priority
Router(config-pmap-c)# police 300000000
Router(config-pmap-c)# set cos 4
Router(config-pmap)# class class-default
Router(config-pmap-c)# set cos 1

Router(config)# policy-map data_silver_parent_out
Router(config-pmap)# class class-default
Router(config-pmap-c)# shape average 500000000
Router(config-pmap-c)# bandwidth remaining ratio 2
Router(config-pmap-c)# service-policy data_silver_child_out

Router(config)# policy-map data_bronze_child_out
Router(config-pmap)# class video
Router(config-pmap-c)# priority
Router(config-pmap-c)# police 100000000
Router(config-pmap-c)# set cos 4
Router(config-pmap)# class class-default
Router(config-pmap-c)# set cos 1

Router(config)# policy-map data_bronze_parent_out
Router(config-pmap)# class class-default
Router(config-pmap-c)# shape average 500000000
Router(config-pmap-c)# bandwidth remaining ratio 1
Router(config-pmap-c)# service-policy data_bronze_child_out
PFC QoS on a Cisco 7600 Series Ethernet Services Plus Line Card Configuration Guidelines

The Cisco 7600 Series ES+ line card supports Policy Feature Card (PFC) QoS for SVI interfaces only in the case of ingress cos-to-exp marking and micro flow policing. For supported interfaces, see “Supported Interfaces” section on page 7-3.

Configuring Hierarchical QoS

The Cisco 7600 Series ES+ line cards support hierarchical QoS (H-QoS) that you configure using Cisco Modular QoS CLI (MQC). The following H-QoS capabilities are supported:

- Four-level H-QoS (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.)
- 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 not supported

- Ingress and egress classification
- Subinterface/Switch port QoS for Ethernet
- 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
- Hierarchical policing
- Input shaping
- Scaling for ES+ line cards
  - 128,000 queues
  - 16,000 traffic shapers
  - 48,000 policers per NPE
  - 8,000 H-QoS policy-maps per NPE in egress. (On the 20xGE and 40xGE port line cards, the first five ports on the NPE support a maximum of 4,000 H-QoS policy-map applications. Similarly, the next 5 ports on the NPE also support a maximum of 4000 H-QoS policy-map applications, giving a total of 4000 + 4000 = 8000 H-QoS policy-maps per NPE in egress). In ingress, a maximum of 3904 HQoS policy-maps can be applied across the 10 ports of the NPE. Note that unlike egress, there is no limit in ingress on a per-5-port basis.

- Scaling for ES+T line cards
  - 16 Child Queues for each port only for lowq cards.
  - 24000 policers per ES+T-20G/ES+T-2TG.

Follow these restrictions while configuring Hierarchical QoS for the Cisco 7600 series ES+ line cards:

- The Cisco 7600 series ES+ line cards support up to 128,000 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 for the Cisco 7600 series ES+T line cards:

- The Cisco 7600 series ES+T line cards support up to 16 queues for each port.
- The Cisco 7600 series ES+T line cards support up to 16 queues per port channel.
- Cisco 76-ES+T-2TG3CXL and Cisco 76-ES+T-20G3CXL line cards support up to 24000 policers per line card.
- Cisco 76-ES+T-4TG3CXL and Cisco 76-ES+T-40G3CXL line cards support up to 48000 policers per line card.
- If QoS is configured on a port channel and also on the member links of the port channel, then the sum of queues on the port channel and the largest value of queues among all member links of that port channel should not exceed 16.
- Applying QoS shape or police on L3 port channel (main interface or sub-interface) on ES+ line cards results in replication of QoS on each member link. For example, when there are two member links in port channel, shaper of 20 Mbps is replicated on both the links resulting in an aggregate of 40 Mbps (20 Mbps x 2).
- 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.

In IOS hierarchical levels are represented as follows and current support is up to five levels:

- Physical or main interface
- Subinterface or logical layer
- Grandparent class
- Parent class
- Child class

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.

A policy-map with three levels has four levels of hierarchy when attached on the main interface, and five levels of hierarchy when attached on a subinterface.
On the ingress, three level H-QOS is supported (port, parent, child).

Shape only services must be deployed using H-QoS policies to ensure that the parent scheduler is installed at L3 in the scheduler. This applies from Release 12.2(33)SRD5, 12.2(33)SRE2 and 15.0(1)S to all future releases where QoS profile enhancement is supported.

Table 7-12 provides information about supported H-QoS features.

### Table 7-12  Hierarchical QoS Feature Support

<table>
<thead>
<tr>
<th>Interface Type</th>
<th>Marking</th>
<th>Policing</th>
<th>Shaping</th>
<th>Bandwidth</th>
<th>Priority and Priority</th>
<th>Priority and Policing</th>
<th>WRED</th>
</tr>
</thead>
<tbody>
<tr>
<td>Main Layer 3 interface</td>
<td>CoS, prec/dscp, EXP</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Layer 3 subinterface</td>
<td>CoS, prec/dscp, EXP</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Service instances</td>
<td>outer CoS, prec/dscp, inner CoS</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SVI interface</td>
<td>Yes</td>
<td>No(^1)</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Switchport interfaces</td>
<td>Outer CoS</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Port-channel service instances</td>
<td>outer CoS, inner CoS</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Port-channel Layer 3 member link</td>
<td>CoS, prec/dscp, EXP</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

1. Earl Policing is not supported post 12.2(33)SRE release.

### Examples

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

```bash
! 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:

```bash
! Router# enable
```
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)# class prec2
Router(config-pmap-c)# priority level 2
Router(config-pmap-c)# class class-default
Router(config-pmap-c)# Police 100kbps

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 an EVC interface:

```
Router(config)# policy-map child_1
Router(config-pmap)# class cos1
Router(config-pmap-c)# priority level 1
Router(config-pmap-c)# class cos 2
Router(config-pmap-c)# priority 2
Router(config-pmap-c)# class class-default
Router(config-pmap-c)# Police 100kbps

Router(config)# policy-map HQoSParent
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 3-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)# class prec456
Router(config-pmap-c)# shape average 10M
Router(config-pmap-c)# class class-default

Router(config)# policy-map HQoS_parent
Router(config-pmap)# class ACL_c1
Router(config-pmap-c)# Police 100kbps
Router(config-pmap-c)# priority 1
Router(config-pmap-c)# service policy child_1
Router(config-pmap-c)# class ACL_c2
Router(config-pmap-c)# Police 100kbps
Router(config-pmap-c)# priority level 2
Router(config-pmap-c)# service policy child_2
Router(config-pmap-c)# class class-default
Router(config-pmap-c)# Police 100kbps
Router(config-pmap-c)# service policy child_3

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

This example configures an egress 3 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)# class prec456
Router(config-pmap-c)# shape average 10M
Router(config-pmap)# class class-default
!
Router(config)# policy-map HQoS_parent
Router(config-pmap)# class ACL_c1
Router(config-pmap-c)# Police 100kbps
Router(config-pmap-c)# priority level 1
Router(config-pmap-c)# service policy child_1
Router(config-pmap)# class ACL_c2
Router(config-pmap-c)# Police 100kbps
Router(config-pmap-c)# priority level 2
Router(config-pmap-c)# service policy child_2
Router(config-pmap)# class class-default
Router(config-pmap-c)# service policy child_3
!
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
!

EVCS QoS Support

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

EVC QoS works with the following EVC combinations:
- One TAG case
- Two TAG case
- One TAG to one TAG
- One TAG to two TAG
- Two TAG to one TAG
- Two TAG to two TAG
- One TAG termination
- Two TAG termination
- Tag to Tag Translation

For information on how to configure EVC QoS, refer to the following sections to see how service instances and port channel service instances are handled:
- Configuring Classification, page 7-8
- Configuring Policing, page 7-14
- Configuring Marking, page 7-23
Restrictions and Usage Guidelines

When configuring QoS with EVCS on the Cisco 7600 Series ES+ line card, follow these restrictions and usage guidelines:

- Service instances use MQC.
- QoS supports 16,000 service instances.
- H-QoS supports up to 2000 policies.
- Ingress QoS supports H-QoS and flat policy-maps.
- Ingress shaping is supported.
- For egress QoS, both hierarchical and flat policy-maps are supported.
- Before creating a service instance, remove any policy-maps on the main interface.
- Any policy-map can exist in a parent policy.
- When QoS is applied on a port channel service instances with member links, the router verifies QoS compatibility with the ES+ line card. However, if the QoS policy-map is applied when the port channel service instances does not have member links, the router assumes ES+ line card capability and allows the policy-map to be attached.
- For service instances configured on port channels:
  - Member links of the port channel can span multiple line cards, but the line cards must be of the same type. For example, you cannot have an ESM20 and an ES+ member link in the same port channel.
  - Ingress QoS is limited to marking and policing.
  - Ingress queuing is not supported.
  - The `bandwidth percent` and `police percent` commands are not supported in flat policy-maps or parents of H-QoS policy-maps. Both commands are supported in child policy-maps.
  - Five-minute load intervals are recommended (30 second load intervals cause higher fluctuations in rates).
- BRR is supported on port-channel service instances.
- Bandwidth (kbps, percent) in parent and flat on EVCs is not supported.

EVC Configuration Examples

This example shows ingress QoS on scalable EoMPLS.

```
Router# enable
Router# configure terminal
Router(config)# interface GE 1/2
Router(config-if)# service instance 1 ethernet
Router(config-if-srv)# encapsulation dot1q 100
Router(config-if-srv)# rewrite ingress tag pop 1 symmetric
Router(config-if)# xconnect 2.2.2.2 100 pw-class vlan-xconnect
```
Router(config-pmap-c)# service-policy input mark-it-in
Router(config)# policy-map mark-it-in
Router(config-pmap)# class cos0
Router(config-pmap-c)# police
Router(config-pmap-c)# set mpls exp imposition 5

In this example of a single tag VLAN configuration, because the encapsulation dot1q 10 is already classified, only the inner VLAN and CoS values are configured.

Router# enable
Router# configure terminal
Router(config)# interface GE 1/2
Router(config-if)# service instance 1
Router(config-if-srv)# encapsulation dot1q 10 second-dot1q any
Router(config-if-srv)# rewrite ingress tag pop 1 symmetric
Router(config-if-srv)# bridge domain 200
Router(config-pmap-c)# service-policy input mark-it-in
Router(config)# policy-map mark-it-in
Router(config-pmap)# class innervlan20
Router(config-pmap-c)# police 10000000
Router(config-pmap-c)# set cos 0
Router(config-pmap-c)# set cos-inner 0

This is an example of a single tag VLAN connect ingress policy.

Router# enable
Router# configure terminal
Router(config)# interface GigabitEthernet1/1
Router(config-if)# service instance 100 ethernet
Router(config-if-srv)# encapsulation dot1q 10 second-dot1q any
Router(config-if-srv)# rewrite ingress tag pop 1 symmetric
Router(config-pmap-c)# service-policy in mark-it-in
Router(config)# interface GigabitEthernet 1/2
Router(config-if)# service instance 101 ethernet
Router(config-if-srv)# encapsulation dot1q 11 second-dot1q any
Router(config-if-srv)# rewrite ingress tag pop 1 symmetric
Router(config-pmap-c)# service-policy in mark-it-in
Router(config-if-srv)# connect EVC1 GigabitEthernet 1/1 100 GigabitEthernet 1/2 101
Router(config)# policy-map mark-it-in
Router(config-pmap)# class vlaninner20cosinner5
Router(config-pmap-c)# set cos 0

This is an example of an egress double tag VLAN connect hierarchical configuration.

Router# enable
Router# configure terminal
Router(config)# interface GigabitEthernet1/1
Router(config-if)# service instance 100 ethernet
Router(config-if-srv)# encapsulation dot1q 10 second-dot1q 20
Router(config-if-srv)# rewrite ingress tag pop 2 symmetric
Router(config-pmap-c)# service-policy out parent-out-100
Router(config)# interface GigabitEthernet 1/2
Router(config-if)# service instance 101 ethernet
Router(config-if-srv)# encapsulation dot1q 11 second-dot1q 21
Router(config-if-srv)# rewrite ingress tag pop 2 symmetric
Router(config-pmap-c)# service-policy out parent-out-101
Router(config-if-srv)# connect EVC1 GigabitEthernet 1/1 100 GigabitEthernet 1/2 101
Router(config)# policy-map child-out-100
Router(config-pmap)# class cos5
Router(config-pmap-c)# bandwidth percent 10
Router(config-pmap-c)# set cos 0
Router(config-pmap-c)# set cos-inner 0
Router(config)# policy-map parent-out-100
QoS on Port-Channel Member-Link

The QoS on Port-Channel Member-Link feature provides support to apply QoS service-policies in ingress and egress traffic on the following interfaces:

- Layer 3 Port-channel main interface
- Layer 3 Port-channel subinterface
- Port-channel member links with per port queuing
- Layer 2 Port-channel interface

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

- Policy-map attached to the EVC or subinterface through which the traffic is flowing.
- Policy-map attached to member link in the absence of above case.

For more information, see Table 7-13.

QoS policy-maps cannot co-exist on a port-channel main interface, subinterface, and EVC. However, member-link policy-map can co-exist with policy-map on L3 port-channel main interface, subinterface, or EVC. In case of L2 port-channels, you can configure QoS on either port-channel main-interface or on the member-link. QoS on both the L2 port-channel main-interface and member-link is not supported.
Note Starting with Cisco IOS Release 12.2(33)SRD1, these interfaces support QoS:
- Port-channel subinterface (supported in input direction only).
- Port-channel Layer 3 member-link (supported in output direction only).

Note Starting with Cisco IOS Release 15.1 (01)S, these interfaces support QoS:
- Port-channel Layer 2 main interface
- Port-channel Layer 3 main interface
- Port-channel Layer 2 member link

Supported Egress QoS Configurations

Table 7-13 lists the QoS configurations supported on ingress and egress.

<table>
<thead>
<tr>
<th>QoS Configurations</th>
<th>Comments</th>
</tr>
</thead>
</table>
| Policy-map attached to layer 3 port-channel interface (input and output) | • Traffic ingress from any member link and egress to any member link will be subject to policy-map attached to port-channel main interface.  
• Classification is supported on port-channel interface  
• Policing is supported on port-channel interface (aggregated policing for each Network Process [NP]).  
• Policing-microflow (EARL Policing) is not supported.  
• Marking is supported on port-channel interface.  
• Queuing is not supported on port-channel interface. |
| Policy-map attached to layer 3 port-channel subinterface (input and output) | • Marking is supported on port-channel subinterface.  
• Policing is supported on port-channel subinterface (aggregated policing for each NP).  
• Queuing is not supported on port-channel subinterface.  
• Policing-microflow (EARL Policing) is supported for ingress only. |
| Policy-map attached on the member-link with no policy-map configured on port-channel interface, port-channel subinterface, and portchannel EVC. | • Classification is supported.  
• All traffic flowing through port-channel Layer 3 member is subject to policy-map attached to port-channel Layer 3 member link.  
• Policing-microflow (EARL Policing) is not supported.  
• Marking is supported on member-link.  
• Queuing is supported on member-link. |
| Policy-map attached to port-channel member link and policy-map configured on port-channel interface. | • Policy-map on port-channel main interface will take precedence over policy-map configured on member links. |
Table 7-13  Supported QoS Configurations

<table>
<thead>
<tr>
<th>QoS Configurations</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy-map attached to port-channel member link and policy-map configured on port-channel subinterface.</td>
<td>• Policy-map on port-channel subinterface will take precedence over policy-map configured on port-channel member link for that subinterface traffic.</td>
</tr>
</tbody>
</table>
| Policy-map attached to port-channel member link and policy-map configured on port-channel EVC service instance. | • Policy-map on port-channel EVC will take precedence over the policy-map configured on the member-link.  
• All the traffic flowing through port-channel service instance is subject to policy-map attached to port-channel service instance.  
• Traffic flowing through the member link configured with QoS policy-map but not through port-channel EVC is subject to the policy-map attached to member link. |

1. For more information on classification, see Table 7-4  
2. For more information on policing, see Table 7-5  
3. For more information on marking, see Table 7-6

Note  
If a policy-map is not applied on an EVC or subinterface, the traffic from such subinterfaces and EVCs is subjected to the member QoS policy. For the traffic flowing through a subinterface or EVC with policy-map, corresponding policy-map is applied on the traffic.

Restrictions and Usage Guidelines

When configuring the QoS on Port-Channel Member-Link feature on the Cisco 7600 Series ES+ line card, follow these restrictions and usage guidelines:

• Any traffic that belongs to a port-channel subinterface or port-channel service instance will go through the member link policy only if there is no policy directly attached on that port-channel subinterface or port-channel service instance.

If the port-channel subinterface or port-channel service instance has its own policy, traffic is subjected to the policy applied on that port-channel subinterface or port-channel service instance.

It is not recommended to configure member link policy on the ingress if there is a micro-flow policing policy configured on the port-channel main interface or port-channel subinterface. If a member link policy and a micro-flow policing policy exist together, traffic is subjected to both policies, first by the member link policy on the NP and then the micro-flow policing policy on the PFC.

Having Layer 3 port-channel member links with user defined classes in the parent introduces an additional queuing hierarchy. The interface bandwidth is shared equally between all the user defined classes.

To protect and guarantee the port channel service instance bandwidth, the member link policy should have a grand-parent class-default with shape configured to restrict the maximum interface bandwidth given to non port-channel service instance traffic (if there is more than one class at the parent level in the member link policy).

• Queuing features on Port-Channel main and subinterface are not supported.

• Police percent on flat policy-map is not supported on port-channel main and subinterfaces.
• Egress microflow policing is not supported on member links, port-channel, and port-channel subinterface.
• If there is a policy-map attached to the main interface, you cannot attach a policy-map the EVC or sub-interface of the main interface.

**QoS on Port-Channel Member-Link Configuration Examples**

The following example shows a sample policy-map configuration:

```plaintext
Router# enable
Router# configure terminal
Router(config)# policy-map port-channel-egress_qos
Router(config-pmap)# class prec0
Router(config-pmap-c)# police cir 100000000
Router(config-pmap-c)# set ip precedence 3
Router# enable

Router(config)# policy-map subint_egress
Router(config-pmap-c)#class prec1 <match on precedence 1
Router(config-pmap-c)# police 20000 conform-action set-prec-transmit 3 exceed-action drop
Router(config-pmap-c)#class class-default
Router(config-pmap-c)#police 400000
Router#

Router(config)# policy-map memlink_child
Router(config-pmap-c)# class cos0 <match on cos 0
Router(config-pmap-c)# shape average 50000000
Router(config-pmap-c)# priority
Router(config-pmap-c)# class cos1
Router(config-pmap-c)# bandwidth 100000
Router(config-pmap-c)# class class-default
Router(config-pmap-c)# shape average 100000000

Router(config)# policy-map memlink_parent_ingress
Router(config-pmap-c)# class vlan11
Router(config-pmap-c)# shape average 300000000
Router(config-if)# service-policy child
Router(config-pmap-c)# class vlan12
Router(config-pmap-c)# shape average 300000000
Router(config-if)# service-policy child
Router(config-pmap-c)# class class-default
```

The following example illustrates how to configure the service-policy under a router port-channel Layer 3 member link.

```plaintext
Router# enable
Router# configure terminal
Router(config)# interface Port-channel 1
Router(config-if)# ip address
Router(config-if)# mpls ip

Router(config)# interface gi1/0
Router(config-if)# channel-group 1
Router(config-if)# service-policy output port-qos

Router(config)# interface gi1/1
Router(config-if)# channel-group 1
Router(config-if)# service-policy output port-qos
```

The following example includes a bandwidth remaining ratio:
Router# enable
Router# configure terminal
Router(config)# policy-map port-qos
Router(config-pmap)# class cos0 match on cos 0
Router(config-pmap-c)# police cir 100000000
Router(config-pmap-c)# priority
Router(config-pmap-c)# class cos1
Router(config-pmap-c)# bandwidth remaining ratio 2
Router(config-pmap-c)# class class-default
Router(config-pmap-c)# bandwidth remaining ratio 1

The following are four examples of Layer 3 service policies:

Router# enable
Router# configure terminal
Router(config)# policy-map port-qos
Router(config-pmap)# class prec1 match on ip prec 1
Router(config-pmap-c)# police cir 100000000
Router(config-pmap-c)# priority
Router(config-pmap-c)# class prec2
Router(config-pmap-c)# bandwidth 100000
Router(config-pmap-c)# class class-default
Router(config-pmap-c)# shape average 100000000
Router(config-pmap-c)# random-detect aggregate
Router(config-pmap-c)# random-detect precedence values 3 minimum-thresh 40 maximum-thresh 60 mark-prob 1
Router(config-pmap-c)# random-detect precedence values 4 minimum-thresh 70 maximum-thresh 90 mark-prob 1
Router(config-pmap-c)# random-detect precedence values 5 minimum-thresh 100 maximum-thresh 120 mark-prob 1

Router# enable
Router# configure terminal
Router(config)# policy-map port-qos
Router(config-pmap)# class exp1 match on exp 1
Router(config-pmap-c)# police cir 100000000
Router(config-pmap-c)# priority
Router(config-pmap-c)# class exp2
Router(config-pmap-c)# bandwidth 100000
Router(config-pmap-c)# class class-default
Router(config-pmap-c)# shape average 100000000

Router# enable
Router# configure terminal
Router(config)# policy-map port-qos
Router(config-pmap)# class ip-expl match on ip prec1, or exp 1
Router(config-pmap-c)# police cir 100000000
Router(config-pmap-c)# priority
Router(config-pmap-c)# class ip-exp2
Router(config-pmap-c)# bandwidth 100000
Router(config-pmap-c)# class class-default
Router(config-pmap-c)# shape average 100000000

Router# enable
Router# configure terminal
Router(config)# policy-map port-qos
Router(config-pmap)# class exp1 match on exp 1
Router(config-pmap-c)# police cir 100000000
Router(config-pmap-c)# priority
Router(config-pmap-c)# class exp2
Router(config-pmap-c)# bandwidth remaining ratio 5
Chapter 7 Configuring QoS

QoS on Port-Channel Member-Link

Router(config-pmap)# class class-default
Router(config-pmap-c)# bandwidth remaining ratio 2

The following example shows the flat service-policies that can be configured under member-links:

Router# enable
Router# configure terminal
Router(config)# policy-map port-qos
Router(config-pmap)# class vlan11
Router(config-pmap-c)# match on vlan 11
Router(config-pmap-c)# police cir 100000000
Router(config-pmap-c)# priority
Router(config-pmap-c)# class vlan12
Router(config-pmap-c)# bandwidth 100000
Router(config-pmap-c)# class class-default
Router(config-pmap-c)# shape average 100000000

Router(config)# policy-map child
Router(config-pmap-c)# class cos0
Router(config-pmap-c)# match on cos 0
Router(config-pmap-c)# police cir 100000000
Router(config-pmap-c)# priority
Router(config-pmap-c)# class cos1
Router(config-pmap-c)# bandwidth 100000
Router(config-pmap-c)# class class-default
Router(config-pmap-c)# shape average 100000000

Router(config)# policy-map parent
Router(config-pmap-c)# class class-default
Router(config-pmap-c)# shape average 300000000
Router(config-if)# service-policy child

Router(config)# policy-map parent
Router(config-pmap-c)# class vlan11
Router(config-pmap-c)# shape average 300000000
Router(config-if)# service-policy child

The following example shows how to configure QoS on port-channel subinterface in egress:

Router# enable
Router# configure terminal
Router(config)# interface Port-channel 1.1
Router(config-if)# encapsulation dot1q 1001
Router(config-if)# service-policy input subint-egress
The following examples show service-policy combination on various interfaces.

The first example shows an egress service-policy attached to a port-channel member-link. There is no service-policy on the port-channel service instance.

```
Router# enable
Router# configure terminal
Router(config)# interface Port-channel 1
Router(config-if)# ip address
Router(config-if)# service instance 1 ethernet
Router(config-if-srv)# encapsulation dot1q 100
Router(config-if-srv)# bridge-domain 200
Router(config-if)# service instance 2 ethernet
Router(config-if-srv)# encapsulation dot1q 101
Router(config-if-srv)# bridge-domain 200

interface gi1/0
Router(config-if)# channel-group 1
Router(config-if)# service-policy output port-qos
Router(config)# interface gi1/1
Router(config-if)# channel-group 1
Router(config-if)# service-policy output port-qos
```

In the next example, an egress service-policy is attached to a port-channel member-link. An egress and an ingress service-policy are applied on the port-channel service instance.

```
Router# enable
Router# configure terminal
Router(config)# interface Port-channel 1
Router(config-if)# ip address
Router(config-if)# service instance 1 ethernet
Router(config-if-srv)# encapsulation dot1q 100
Router(config-if-srv)# bridge-domain 200
Router(config-if)# service-policy output evc-egress
Router(config-if)# service-policy input evc-ingress
Router(config-if)# service instance 2 ethernet
Router(config-if-srv)# encapsulation dot1q 101
Router(config-if-srv)# bridge-domain 200
Router(config-if)# service-policy output evc-egress
Router(config-if)# service-policy input evc-ingress

Router(config)# interface gi1/0
Router(config-if)# channel-group 1
Router(config-if)# service-policy output port-qos
Router(config)# interface gi1/1
Router(config-if)# channel-group 1
Router(config-if)# service-policy output port-qos
```

In the following example, an egress service-policy is attached to a port-channel member-link. An egress and an ingress service-policy are applied on the port-channel service instance. An ingress service-policy is applied on the port-channel subinterface.

```
Router# enable
Router# configure terminal
Router(config)# interface Port-channel 1
Router(config-if)# ip address
Router(config-if)# service instance 1 ethernet
Router(config-if-srv)# encapsulation dot1q 100
Router(config-if-srv)# bridge-domain 200
Router(config-if)# service-policy output evc-egress
Router(config-if)# service-policy input evc-ingress

Router(config)# interface gi1/0
Router(config-if)# channel-group 1
Router(config-if)# service-policy output port-qos
Router(config)# interface gi1/1
Router(config-if)# channel-group 1
Router(config-if)# service-policy output port-qos
```

Router(config-if)# service-policy output evc-egress
Router(config-if)# service-policy input evc-ingress
Router(config-if)# service instance 2 ethernet
Router(config-if-srv)# encapsulation dot1q 101
Router(config-if-srv)# bridge-domain 200
Router(config-if)# service-policy output evc-egress
Router(config-if)# service-policy input evc-ingress

Router(config)# interface Port-channel 1.1
Router(config-if-srv)# encapsulation dot1q 1000
Router(config-if)# service-policy input subint-ingress
Router(config-if)# service-policy output subint-egress

Router(config)# interface gi1/0
Router(config-if)# channel-group 1
Router(config-if)# service-policy output port-qos
Router(config)# interface gi1/1
Router(config-if)# channel-group 1
Router(config-if)# service-policy output port-qos

The following example shows how to configure QoS on member-link for Ingress
Router# enable
Router# configure terminal
Router(config)# interface gi1/1
Router(config-if)# channel-group 1
Router(config-if)# service-policy input memlink-Parent_ingress

The following examples shows the policy that can be configured under Port channel main interface:
Router# enable
Router# configure terminal
Router(config)# policy-map port-channel-egress_qos
Router(config-pmap)# class dscp0
Router(config-pmap-c)# police cir 100000000
Router(config-pmap)# set ip precedence 3
Router# enable

Router# configure terminal
Router(config)# policy-map port-channel-ingress_qos
Router(config-pmap-c)# class cos1
Router(config-pmap-c)# police cir 80000 pir 160000 conform-action set-dscp-transmit 5 exceed-action set-dscp-transmit 6 violate-action drop
Router# enable

Router# configure terminal
Router(config)# interface Port-channel 1
Router(config-if)# service-policy output port-channel-egress-qos
Router(config-if)# service-policy input port-channel-ingress-qos

The following examples shows how to configure QoS on port-channel main interface:
Router# enable
Router# configure terminal
Router(config)# policy-map port-channel-ingress_qos
Router(config-pmap-c)# class cos1
Router(config-pmap-c)# police cir 80000 pir 160000 conform-action set-dscp-transmit 5 exceed-action set-dscp-transmit 6 violate-action drop
Router# enable

Router# configure terminal
Router(config)# interface Port-channel 1
Router(config-if)# service-policy output port-channel-egress-qos
Router(config-if)# service-policy input port-channel-ingress-qos
Troubleshooting QoS on Port-Channel Member-Link

This section describes how to troubleshoot QoS on a Port-Channel Member-Link.

- The `show policy-map interface inf-name` command shows service policy in suspended mode.
  
  An example output:
  
  ```
  PE2#sh policy-map int port-ch 51
  Port-channel51
  Service-policy output: abc
  Service policy abc is in suspended mode
  ```

  A policy is suspended when there are no member-links attached to it. Use the `show etherchannel summary` command to check the member-links attached to a policy and the corresponding status. The following example shows the output of the `show etherchannel summary` command:

  ```
  PE2#show etherchannel summary
  Flags:  D - down        P - bundled in port-channel
          I - stand-alone s - suspended
          H - Hot-standby (LACP only)
          R - Layer3      S - Layer2
          U - in use      f - failed to allocate aggregator
          m - not in use, minimum links not met
          u - unsuitable for bundling
          w - waiting to be aggregated
          d - default port
  Number of channel-groups in use: 4
  Number of aggregators:           4
  Group  Port-channel  Protocol    Ports
  -----------------------------------------------
  1      Po1(RU)          -        Gi2/12(P)
  2      Po2(SD)          -
  3      Po3(SD)          -
  4      Po4(RU)          -        Gi2/1(P)    Gi2/2(P)    Gi2/22(P)
  ```

- The QoS policy-map configured on a port-channel or member-links is not working. Run the following commands on the route processor:

  - `show interface interface-type slot/port` command to check the interface statistics and ensure that the traffic is flowing.
  - `run policy-map policy-map-name` command to verify the policy-map definitions.
  - `show run class-map class-map-name` command to verify the class-map definitions.
  - `show run interface port-channel pc-num` to check the interface configurations.
  - `show etherchannel summary` command to check member-link bundling information.

  - Verify the support matrix available at:

  Run the following commands on the line card:

  - `show platform npc qos sp pc all` command to check the number of policies applied on port-channel main interface, subinterface, and EVC interfaces. The following example shows an output of the `show platform` command:

    ```
    PE2-dfc2#
    Port-Channel 3 : No policies attached
    Port-Channel 4 :
    mp port  dir pc-type count
    -----------------------------------------------
    0 0   Input   PC-L3    2
    0 0   Output  PC-L3    2
    0 0   Input   PC-EVC    1
    ```
Chapter 7 Configuring QoS

IPv6 - Hop by Hop Rate Limiter

The IPv6 Hop-by-Hop (HBH) extension header is part of the original specification of the IPv6 protocol (RFC 2460). It is identified by header type 0 and when present, this extension header must always be the first extension header (EH) to follow the main header. Because a node must process any received packet that has an HBH extension header, forwarding of packets containing the HBH header can represent or be used as a security threat.

The IPv6 - Hop by Hop Rate Limiter feature provides protection from Denial of Service (DoS) attacks by allowing you to rate limit IPv6 HBH packets.

Restrictions and Usage Guidelines

When rate limiting IPv6 HBH packets on the Cisco 7600 Series ES+ line card, follow these restrictions and usage guidelines:

- Supported with the following supervisor engines:

Note

To check the policy-map statistics on EVC and SG targets under a port-channel, run these commands:

show policy-map interface intf service instance efp
show policy-map interface intf service group group.
Chapter 7  Configuring QoS

IPV6 - Hop by Hop Rate Limiter

- Route Switching Processor 720-1GE
- Route Switching Processor 720-10GE
- Supervisor Engine 32
- Supervisor Engine 720

- Setting the police rate to 0 drops all the IPv6 HBH packets.
- After setting the police rate, the setting will remain on the line card even if the line card is moved to another chassis running Cisco IOS Release 12.2(33)SRD1 or later.
- IPv6 packets with HBH and EH will bypass other QoS configured on the Cisco 7600 Series ES+ line card.

Configuring IPv6 - Hop by Hop Rate Limiter

To connect to a specific line card for the purpose of executing the `test platform police ipv6 set` command, `test platform police ipv6 get` command or the `test platform police ipv6 disable` command, use the `attach` command in privileged EXEC mode.

You can then set the IPv6 internal police rate by using the `test platform police ipv6 set` command in privileged EXEC mode from the line card console:

**SUMMARY STEPS**

1. `attach module-number`
2. `enable`
3. `test platform police ipv6 set rate`
4. `test platform police ipv6 get`
5. `test platform police ipv6 disable`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>attach module-number</code></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router# attach 9</td>
</tr>
<tr>
<td><strong>Step 1</strong></td>
<td><code>enable</code></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router-dfc3# enable</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>test platform police ipv6 set rate</code></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router-dfc3# test platform police ipv6 set 1234</td>
</tr>
</tbody>
</table>
Chapter 7 Configuring QoS

Port Level Shaping Concurrent with 4HQoS on ES+

Example

This example shows how to set the rate.

```
Console# attach 3
Trying Switch ... 
Entering CONSOLE for Switch
Type "^C^C^C" to end this session
osr3-dfc3#
Router-dfc3# enable
```

```
Router-dfc3# test platform police ipv6 get
```

Example:

```
Router-dfc3# test platform police ipv6 get
```

```
You can obtain IPv6 internal police rate by using the test platform police get command in privileged EXEC mode from the line card console:
```

```
Router-dfc3# test platform police ipv6 set 1234
```

```
You can disable the IPv6 internal policer by using the test platform police ipv6 disable command in privileged EXEC mode from the line card console:
```

```
Router-dfc3# test platform police ipv6 disable
```

```
Router-dfc3# test platform police ipv6 get
```

```
IPv6 with HBH header is not policed.
```

Note

On an ES+ line card, rate=65535 indicates that the policer is disabled.

Command Purpose

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>test platform police ipv6 get</td>
<td>Gets the IPv6 internal police rate.</td>
</tr>
<tr>
<td>test platform police ipv6 disable</td>
<td>Disables the IPv6 internal policer.</td>
</tr>
</tbody>
</table>

Post 15.3(01)S IOS release, IPv6 HbH Rate limiter can be configured through a CLI instead of using test command. Command that needs to be configured is "hw-module slot slot-number ipv6-hbh-rl kbps_value". Configured value can be validated using CLI "show hw-module slot slot-number ipv6-hbh-rl"

Port Level Shaping Concurrent with 4HQoS on ES+

In a network having a PE router connected to a low level device with lesser line rate capability, you can configure the traffic shaping QoS on the output direction of the PE port. Until Cisco IOS release 15.0(1), QoS on main interface is not supported to co-exist with the QoS policy on any other target on the same physical port. This feature allows class-default shaping only QoS policy on a main interface to co-exist with QoS policy on the sub targets. You can also use this feature to apply a shaping policy on the main interface and a HQoS policy on the sub targets such as sub-interfaces, EVCs, sessions, and service groups.
Furthermore, this feature also enables you to control the bandwidth assigned to a node directly connected to a port as per the service agreement.

Restrictions and Usage Guidelines

Follow these restrictions and usage guidelines while configuring port level shaping concurrent with 4HQoS on an ES+ line card:

- To allow coexistence, apply policy-map on the main interface before applying the policy-map on the sub targets.
- You can remove the policy-map on the main interface only after removing policy-maps from all the corresponding sub targets.
- You can configure port level shaping with these policy-maps:
  - Flat policy-map or HQoS policy-map on a service group
  - Flat policy-map or HQoS policy-map on an EFP
  - Flat policy-map or HQoS policy-map on a subinterface
  - Flat policy-map or HQoS policy-map on an Intelligent services Gateway (ISG) session
  - Flat policy-map on service group with HQoS on the member EFP, subinterface, or session
  - Port channel Member link HQoS

- For co-existence with sub target QoS, only a flat policy-map with no user defined classes is allowed and only the shape action is allowed.
- Sub target QoS is not allowed for user defined classes on the main interface policy-map, or if there is a HQoS policy-map on the main interface.
- A change in the installed policy-map on the main interface resulting in unsupported configuration is rejected.
- Port level shaping is supported in the egress direction on the main interface and the port-channel main interface.
- The coexistence of port level shaping with sub target QoS is not supported in ingress direction.
- On ES+ LowQ interfaces, co-existence of port-shaper with queuing on subtargets like subinterface, EVC, and service-groups are not supported.

**Note**

Use the `hw-module slot slotnum allow-coexist np npnum` command to configure port level shaping on a 10G interface, else the port level shaper installation fails on the line card.

Configuring Port Level Shaping Concurrent with 4HQoS on ES+

Complete these steps to configure port level shaping concurrent with 4HQoS on an ES+ line card:

- Attach the default-class to a policy-map
- Configure shape rate for the class
- Attach the configured policy-map on egress of an interface.
Summary Steps

1. `enable`
2. `configure terminal`
3. `policy-map policy-map-name`
4. `class {class-name | class-default}`
5. `shape average cir [bc] [be]`
6. `interface gigabitethernet slot/port or interface tengigabitethernet slot/port or interface port-channel number`
7. `service-policy output policy-map-name`
8. `end`

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>enable</code>&lt;br&gt;Enables the privileged EXEC mode.&lt;br&gt;• Enter the password if prompted.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router&gt; enable</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>configure terminal</code>&lt;br&gt;Enters the global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router# configure terminal</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>policy-map policy-map-name</code>&lt;br&gt;Specifies the name of the policy-map.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config)# Policy-map subrate</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>`class {class-name</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-pmap)# Class class-default</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><code>shape average cir [bc] [be]</code>&lt;br&gt;Specifies the average or peak rate traffic shaping.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-pmap-c)# Shape average 100000000</td>
</tr>
</tbody>
</table>
### Example

This example displays port level shaping configuration on ES+ line card.

```plaintext
Router# enable
Router# conf t
  Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# policy-map subrate
Router(config-pmap)# class class-default
Router(config-pmap-c)# Shape average 1000000
Router(config-pmap-c)# interface gigabitethernet 3/1
Router(config-if)# Service-policy out subrate
Router(config-if)# end
```

### Verification

Use these commands to verify port level shaping configuration on ES+ line card:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router# show policy-map</td>
<td>Displays all the configured policy-maps.</td>
</tr>
<tr>
<td>Router# show policy-map policy-map-name</td>
<td>Displays the user-specified policy-map.</td>
</tr>
</tbody>
</table>
Minimum Bandwidth Guarantee Plus Multiple Policy

The minimum bandwidth guarantee on the service groups plus multiple policy feature enables a user to configure a guaranteed minimum bandwidth at the service group level. This feature allows you to explicitly guarantee a minimum bandwidth for the subscribers in the service groups and implicitly for the subscribers without any service group on the same interface. Until release 15.0(1), absolute bandwidth is not supported for the policies applied on the service groups. Using this feature a user can configure a minimum bandwidth on a policy-map applied on the service groups. The remaining bandwidth is computed on each physical port by subtracting the sum of guaranteed bandwidths from the link rate. This remaining bandwidth is then allocated to the port-default entity that manages those service groups with no Quality of Service (QoS), and all the members that do not belong to any service group. Thus, providing a way to configure minimum bandwidth on the default node.
You can configure the minimum bandwidth guarantee feature in terms of: bandwidth rate (Kb/s) or bandwidth percent. You can configure this feature on the class-default in the flat policy-map or the class-default in the parent of a Hierarchical QoS (HQoS) policy-map and apply it to a service group.

Furthermore, this feature allows you to allocate a bandwidth share for these targets:
- Targets without any service group configuration.
- Targets with service groups where the service group is not configured explicitly for the bandwidth.

A target can be an EVC, subinterface, or a session.

Port Channel QoS Considerations

The QoS configuration is based on the load balancing mechanism configured on the port channel. If a port-channel is configured with non flow-based load-balancing, the sum of bandwidth of all the active links is considered as the total available bandwidth on the port-channel. In non flow-based load balancing, the service group QoS is installed on the link where the group is load balanced. When a port-channel is configured with flow-based load balancing, the service group QoS is replicated on all the active member links and the maximum bandwidth that can be guaranteed on a port channel is equal to the single link bandwidth.

Restrictions and Usage Guidelines

Follow these restrictions and usage guidelines when configuring minimum bandwidth guarantee on ES+ line cards:
- You can configure bandwidth as bandwidth kbps or bandwidth percent on the class-default of flat policy-map or HQoS parent policy-map.
- Minimum bandwidth guarantee feature is not supported on user defined classes at any level.
- Minimum bandwidth guarantee feature is supported only on an egress interface.
- For a service group on a port-channel, the service group bandwidth is replicated to all the active member links if the port-channel is configured with flow-based load balancing. Else, the specified service group is installed on one of the active member links and the QoS is configured on the same member link.
- If the port-channel has flow-based load balancing mechanism, limit the interface bandwidth on the port-channel equivalent to the bandwidth of a single member link using the bandwidth command.
- If Bandwidth Remaining Ratio (BRR) is configured on HQoS service groups, the sum of excess weights of all the HQoS service groups is computed and allocated to the new default service group HQoS node. However, the maximum weight that can be configured at the Layer 2 level is 255.
- Bandwidth Remaining Percent (BRP) is not supported on the service groups.
- You can configure each HQoS service group with a maximum weight of 255. The sum of all the HQoS service groups is applied on the Layer 2 node. If the sum is greater than 255, it is rounded off to 255 and applied on the Layer 2 node and the bandwidth allocated is shared between all the HQoS service groups on the port.
You can bundle ES+ T (LowQ ports) with other types of LC ports only if QoS is not applied. After you bundle the mixed ports, do not allow the QoS Service policy.

When QoS is applied, only ES+T (lowQ ports) should be bundled and should not allow mixed mode.

### Configuring Bandwidth Guarantee on a Service Group

You can configure minimum bandwidth guarantee on a service group on an ES+ line card in two ways:

- Configuring minimum bandwidth guarantee by Rate (Kb/s)
- Configuring minimum bandwidth guarantee by Percentage

**Summary Steps**

1. enable
2. configure terminal
3. policy-map policy-map-name
4. class {class-name | class-default}
5. bandwidth {kbps | percent percent_value}
6. exit
7. exit
8. service-group id_number
9. service-policy [{input | output} policy-map-name]
10. interface gigabitethernet slot/port or interface tengigabitethernet slot/port or interface port-channel number
11. service instance id {Ethernet [service-name]}
12. encapsulation dot1q id
13. group id_number
14. end

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>enable</td>
<td>Enables the privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router&gt; enable</td>
<td></td>
</tr>
</tbody>
</table>

| Step 2 | configure terminal       | Enters the global configuration mode.       |
| Example: | Router# configure terminal |                                            |
### Chapter 7  Configuring QoS

#### Minimum Bandwidth Guarantee Plus Multiple Policy

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 3</strong></td>
<td>Policy-map policy-map-name&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Router(config)# Policy-map subrate</td>
</tr>
<tr>
<td>Specifies the name of the policy-map to configure.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Class (class-name</td>
</tr>
<tr>
<td>Specifies the name of a predefined class included in the service policy.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Bandwidth (kbps</td>
</tr>
<tr>
<td>Configures the minimum bandwidth guarantee.&lt;br&gt;In the first example, bandwidth is configured in Kb/s.&lt;br&gt;In the second example, bandwidth is configured in percent value.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Exit&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Router(config-pmap-c)# exit</td>
</tr>
<tr>
<td>Exits the class bandwidth configuration session.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>Exit&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Router(config-pmap)# exit</td>
</tr>
<tr>
<td>Exits the policy-map configuration session.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>Service-group id-number&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Router(config)# service group 1</td>
</tr>
<tr>
<td>Assigns a service group identification number. The acceptable range is between 1 and 32768.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td>Service-policy [(input</td>
</tr>
<tr>
<td>Attaches a traffic policy to the egress interface, where:&lt;br&gt;• <strong>policy-map-name</strong>—Specifies the name of the traffic policy to configure.</td>
<td></td>
</tr>
</tbody>
</table>
Example

This example displays minimum bandwidth guarantee configuration by bandwidth rate:

```
Router> enable
Router# config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# policy-map 4g-bandwidth-policy
Router(config-pmap)# class class-default
Router(config-pmap-c)# bandwidth 4000000
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# service-group 100
Router(config-service-group)# service-policy output 4g-bandwidth-policy
Router(config-service-group)# int teng2/1
Router(config-if)# service instance 1 ethernet
Router(config-if-srv)# encaps dot1q 200
```
Verification

Use these commands to verify minimum bandwidth guarantee on service groups configuration:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show policy-map</td>
<td>Displays all the configured policy-maps.</td>
</tr>
<tr>
<td>show policy-map policy-map-name</td>
<td>Displays the user-specified policy-map.</td>
</tr>
<tr>
<td>show policy-map interface</td>
<td>Displays statistics and configurations of all input and output</td>
</tr>
<tr>
<td>interface_Id service group</td>
<td>policies that are attached to the corresponding service group.</td>
</tr>
<tr>
<td>group_Id</td>
<td></td>
</tr>
<tr>
<td>Router#show policy-map interface</td>
<td>sample output:</td>
</tr>
<tr>
<td>teng2/1 service group 100</td>
<td></td>
</tr>
<tr>
<td>TenGigabitEthernet2/1: Service Group 100</td>
<td>Service-policy output: 4g-bandwidth-policy</td>
</tr>
<tr>
<td>Counters last updated 00:01:57</td>
<td></td>
</tr>
<tr>
<td>ago</td>
<td></td>
</tr>
<tr>
<td>Class-map: class-default (match-any)</td>
<td>0 packets, 0 bytes</td>
</tr>
<tr>
<td>5 minute offered rate 0000 bps, drop rate 0000 bps</td>
<td>Match: any</td>
</tr>
<tr>
<td>Queueing</td>
<td></td>
</tr>
<tr>
<td>queue limit 131072 packets</td>
<td></td>
</tr>
<tr>
<td>(queue depth/total drops/no-buffer drops) 0/0/0</td>
<td></td>
</tr>
<tr>
<td>(pkts output/bytes output) 0/0</td>
<td></td>
</tr>
<tr>
<td>bandwidth 40000000 kbps</td>
<td></td>
</tr>
</tbody>
</table>

Troubleshooting the Minimum Bandwidth Guarantee Configuration

For information on troubleshooting, see Troubleshooting QoS on a ES+ Line Card.
Service Group QoS Support on the Cisco 7600 Series Router

A service group is a logical entity that allows you to group different interface types and apply features as a whole to the group. The interface types can be grouped under a service group and you can apply QoS policies on an aggregate basis for a number of interface types grouped under the service group.

In Cisco releases prior to 15.1(1)S, only Ethernet Virtual Circuits (EVCs) were supported as members of service groups. Effective from Cisco IOS release 15.1(1)S, sub interfaces and sessions on those sub interfaces are supported as members of a service group and you can group all these under the same service group. Service groups also support port channels with EVCs, sub interfaces or sessions.

Restrictions and Usage Guidelines

Follow these restrictions and guidelines while configuring a QoS service group on the Cisco 7600 series:

- An interface type can have a hierarchical policy, but the corresponding group can have only a policy with class-default.
- A service group with HQoS policy can have a hierarchical policy, but the members of the service group cannot have any QoS policies.
- In a service group only shape, BRR, bandwidth, and policing features are supported at the parent level.
- On service groups with HQoS policy, WRED and queue limit features are also supported on child classes.
- On service groups with flat policy, WRED and queue limit features are not supported.
- A service group number is global and you cannot assign a service group number that is already assigned to another interface.
- An interface can only belong to one service group at a time.
- QoS on a service group or member and QoS on main interface cannot co-exist except for the port-level shaper.
- QoS on both sessions and sub interfaces of those sessions is not supported.
- Service groups only support sessions on sub-interfaces, and not sessions on the main interfaces.
- Grouping of main interfaces is not supported. Only grouping of sub interfaces or EVCs on a main interface is supported.
- Queuing features on non-access subinterfaces of port-channel interfaces are not supported.
- In ingress direction, HQoS queuing policies on service groups, EVCs, sub interfaces or sessions are not supported on a port channel.
- In ingress direction, flat queuing policy on service group and HQoS policy on EVC, sub interface or session is not supported on a port channel.
- When multiple interface types are part of a service group on a port-channel interface, all interface types of that group on the port channel should be configured for a common load balancing scheme.
- If sub interfaces and EVCs are part of the same service group, then the port channel should have only flow based load balancing scheme. Only a single type of load balancing scheme is supported at a time for flow based load balancing.
- An access sub interface or sessions supports only 1:1 active or standby redundancy load balancing scheme. Normal subinterfaces (non-access) support only flow based or 1:1 active or standby redundancy load balancing schemes.
When a load balancing scheme on a port channel is flow based, QoS on the service groups as well as QoS on members is replicated on all the member links of the port channel.

When a load balancing scheme on a port channel is service based (manual, automatic, weighted or 1:1 model), QoS on the service group as well as member link is configured only on one member link based on the specific load balancing scheme.

On a port channel when access subinterface or sessions are part of a service group, flow based, manual, weighted, or automatic load balancing schemes are not supported.

On a port channel when normal subinterfaces are part of a service group, manual, weighted, or automatic load balancing schemes are not supported.

For ES+T (76-ES+T-40G3CXL and 76-ES+T-20G3CXL) 1GE line cards:
- In ingress direction, support for six service groups with flat policy.
- In egress direction, support for 11 service groups with flat policy.

For ES+T (76-ES+T-2TG3CXL and 76-ES+T-4TG3CXL) 10GE line cards:
- In ingress and egress direction, support for 15 service groups with flat policy per port.

For ES+ line cards with 10 GE ports:
- In ingress direction, support for 239 service groups with flat policy per port.
- In egress direction, support for 510 service groups with flat policy per port.
- In ingress direction, support for 4000 service groups with HQoS policy per port.
- In egress direction, support for 8000 service groups with HQoS policy per port.

For ES+ line cards with a single gigabit ethernet port:
- In ingress direction, support up to 15 service groups with flat policy per port.
- In egress direction, support up to 31 service groups with flat policy per port.
- In ingress direction, support up to 3856 service groups with HQoS policy for a group of 10 ports (the ports should be grouped as 1-10, 11-20 and so on).
- In egress direction, support up to 4000 service groups with HQoS policy for a group of 5 ports (the ports should be grouped as 1-5, 6-10 and so on).

Since hardware programming is sensitive to order of configuration and potential for non-persistent scale, in case of HQoS with service-group, while applying service-group at the interface level, apply "group <service-group-id>" configuration prior to "service-policy <direction> <service_policy_name>". This is to ensure that child level queue-limits are calculated as per hierarchy which in-turn influence WRED profile usage.

---

**Note**

If you receive an error message while configuring QoS or QoS service groups on an interface, sub interface, service instance, or session on an ES+ line card, use the `show platform npc qos sp np al hw_qos` command to troubleshoot.
Configuring Service Group QoS

Perform these steps to configure service group QoS.

**Summary Steps**

1. `enable`
2. `configure terminal`
3. `policy-map policy-map-name`
4. `class {class-name | class-default}`
5. `shape average cir [bc] [be]`
6. `service-group id`
7. `service-policy [input | output] policy-map-name`
8. `interface gigabitethernet slot/port [subinterface] [access]` or `interface tengigabitethernet slot/port [subinterface] [access]` or `interface port-channel number [subinterface] [access]`
9. `service-instance id {ethernet [service-name]}
10. `group id`
11. `end`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>enable</code></td>
</tr>
<tr>
<td>Example:</td>
<td><code>Router&gt; enable</code></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>configure terminal</code></td>
</tr>
<tr>
<td>Example:</td>
<td><code>Router# configure terminal</code></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>policy-map policy-name</code></td>
</tr>
<tr>
<td>Example:</td>
<td><code>Router(config)# policy-map qos-service group-in</code></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>`class {class-name</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Router(config-pmap)# class cos</code></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><code>shape average cir [bc] [be]</code></td>
</tr>
<tr>
<td>Example:</td>
<td><code>Router(config-pmap-c)# shape average 10000000</code></td>
</tr>
<tr>
<td>Command</td>
<td>Purpose</td>
</tr>
<tr>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Assigns a service group ID. The acceptable range is 1 to 32768.</td>
</tr>
<tr>
<td><em>service-group id number</em></td>
<td>Example: Router(config)# service-group 1</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>Creates a service policy within the service group and attaches it to the ingress or egress of a service group.</td>
</tr>
<tr>
<td>*service-policy [{input</td>
<td>output} policy-map-name]*</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>Specifies the interface to configure service group:</td>
</tr>
<tr>
<td><em>interface gigabitethernet slot/port[.subinterface] [access]</em></td>
<td>- <code>slot/port[.subinterface]</code> — Specifies the location of the interface. If you are configuring a sub interface, you should also specify the sub interface.</td>
</tr>
<tr>
<td>or</td>
<td>- <code>number[.subinterface]</code> — Specifies the port-channel interface.</td>
</tr>
<tr>
<td><em>interface tengigabitethernet slot/port[.subinterface] [access]</em></td>
<td>- <code>access</code> - Specifies the keyword if the interface is an access sub interface.</td>
</tr>
<tr>
<td>or</td>
<td>Example: Router(config)# interface gigabitethernet 4/1 or Router(config)# interface gigabitethernet 4/1.1 access</td>
</tr>
<tr>
<td><em>interface port-channel number[.subinterface] [access]</em></td>
<td><strong>Step 9</strong></td>
</tr>
<tr>
<td></td>
<td>Note: Perform this step only if the targeted interface type is EVC.</td>
</tr>
<tr>
<td><em>service instance id {ethernet [service-name]}</em></td>
<td>Example: Router(config-if)# service instance 1 ethernet</td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td>Adds the interface type to the service group.</td>
</tr>
<tr>
<td><em>group id</em></td>
<td>Example: Router(config-if-subif)# group 1000 or Router(config-if-srv)# group 1000</td>
</tr>
<tr>
<td><strong>Step 11</strong></td>
<td>Exits the interface configuration mode and returns to the privileged EXEC mode.</td>
</tr>
<tr>
<td><em>end</em></td>
<td>Example: Router(config-if-subif)# end</td>
</tr>
</tbody>
</table>
Examples

This example shows how to configure a service group with output service policy and attach a service instance to the service group.

Router# enable
Router# configure terminal
Router# policy-map p1
Router(config-pmap)# class class-default
Router(config-pmap-c)# shape average 100000000
Router(config)# service-group 1
Router(config-service-group)# service-policy output p1
Router(config)# interface gigabitethernet 1/1
Router(config-if)# service instance 101 ethernet
Router(config-if-srv)# group 1

This example shows how to configure a service policy in egress direction and attach the access sub interface to the service group.

Router# enable
Router# configure terminal
Router# policy-map p2
Router(config-pmap)# class class-default
Router(config-pmap-c)# shape average 100000000
Router(config)# service-group 2
Router(config-service-group)# service-policy output p2
Router(config)# interface gigabitethernet 1/1.1 access
Router(config-subif)# group 2
Router(config-subif)# exit

This example shows how to apply a QoS policy to sessions and attach the service group to a sub interface where sessions are brought up.

Router# enable
Router# configure terminal
Router(config)# policy-map p3
Router(config-pmap)# class class-default
Router(config-pmap-c)# shape average 100000000
Router(config)# service-group 3
Router(config-service-group)# service-policy output p3
Router(config)# policy-map p4
Router(config-pmap)# class class-default
Router(config-pmap-c)# shape average 100000000
Router(config)# policy-map type service hqos_dynamic
Router(config-service-policy-map)# service-policy output p4
Router(config)# policy-map type control hqos_dynamic_control
Router(config-control-policy-map)# class type control always event session-start
Router(config-control-policy-map-class-control)# 1 service-policy type service name hqos_dynamic
Router(config)# interface gigabit ethernet 1/1.1 access
Router(config-subif)# service-policy type control hqos_dynamic_control
Router(config-subif)# group 3
Router(config-subif)# ip subscriber routed
Router(config-subscriber)# initiator unclassified ip-address

This example shows how to configure a service group with an output service policy and attaches the service group to a port-channel EVC interface:

Router# enable
Router# configure terminal
Router# policy-map p5
Router(config-pmap)# class class-default
Router(config-pmap-c)# shape average 100000000
Router(config)# service-group 5
Router(config-service-group)# service-policy output p5
Router(config)# interface Port-channel 1
Router(config-if)# service instance 1 ethernet
Router(config-if-srv)# group 5
Router(config-if-srv)# exit

This example shows how to apply a QoS policy to sessions and attach the service group to a port-channel access sub interface where sessions are brought up.

Router# enable
Router# configure terminal
Router(config)# policy-map p3
Router(config-pmap)# class class-default
Router(config-pmap-c)# shape average 100000000
Router(config)# service-group 3
Router(config-service-group)# service-policy output p3
Router(config)# policy-map p4
Router(config-pmap)# class class-default
Router(config-pmap-c)# shape average 100000000
Router(config)# policy-map type service hqos_dynamic
Router(config-service-policy-map)# service-policy output p4
Router(config)# policy-map type control hqos_dynamic_control
Router(config-control-policy-map)# class type control always event session-start
Router(config-control-policy-map-class-control)# 1 service-policy type service name hqos_dynamic
Router(config)# interface port-channel 1.1 access
Router(config-subif)# service-policy type control hqos_dynamic_control
Router(config-subif)# group 3
Router(config-subif)# ip subscriber routed
Router(config-subscriber)# initiator unclassified ip-address
Router(config-if-srv)# end

### Verification

Use these commands to verify the configuration.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router# Show class-map</td>
<td>Displays class maps and their matching criteria.</td>
</tr>
<tr>
<td>Router# Show policy-map</td>
<td>Displays the configuration of all classes for all existing policy maps.</td>
</tr>
<tr>
<td>Router# Show policy-map interface</td>
<td>Displays the statistics and the configuration of the input and output policies attached to an interface.</td>
</tr>
<tr>
<td>Router# Show policy-map interface service instance</td>
<td>Displays the policy-map information for a given service instance on a port channel.</td>
</tr>
<tr>
<td>Router# Show policy-map target service-group group-id</td>
<td>Displays policy-map information about a service group with members that are attached to an interface or port-channel.</td>
</tr>
</tbody>
</table>
Configuring Flexible Service Mapping Based on CoS and Ethertype

The Flexible Service Mapping based on CoS and Ethertype feature enhances the current capability of mapping packets to service instance by allowing you to use CoS and Ethertypes to classify traffic into different service instances, thereby consuming a lesser number of VLANs on the module.

This feature adds the following capabilities for mapping to service instances:

- For QinQ, match on a single CoS value (either inner CoS or outer CoS, but not both simultaneously)
- Match on a range or list of CoS values when a single VLAN or QinQ is specified in the match criteria
- Match support for a single CoS value for a range or list of VLANs
- Match on the following supported payload ether types
  - IPv4 (etype 0x0800)
  - IPv6 (etype 0x086dd)
  - **pppoe-all** (0x8863 and 0x8864)
- In the case of QinQ, inner VLAN can have a range when the outer VLAN is a single VLAN.
- Match on range or list of CoS values when both outer and inner VLANs are single.
- Match on etype is supported both in the case of a single VLAN or in QinQ.
- The pppoe-all CLI option is supported (matches both 0x8863 and 0x8864). The pppoe-session CLI option is not supported.

Restrictions and Usage Guidelines

When configuring Flexible Service Mapping based on CoS and Ethertype, follow these restrictions and guidelines:

- This feature supports both Dot1Q and QinQ.
- Egress behavior implemented for mismatched CoS and Ethertype forwards the packet without re-write and there is no filtering on egress based on the CoS or Layer 3 Ethertype. (Even if CoS or Ethertype mismatches, if egress VLAN information matches, then the frames are forwarded.)
- Neither **pppoe-discovery** or **pppoe-session** are supported individually as ethertypes. Cisco IOS release 12.2(33)SRD3 only supports pppoe-all.
- Service instances on port-channels are supported.
- Matching on both Ethertype and CoS for the same service instance is not allowed.
• OuterCoS or inner CoS can be specified under the same service instance, but not at the same time.
• Specifying a range or list of outer VLANs in double tag cases is not supported.
• MAC learning occurs with bridge-domain, but does not occur with xconnect and connect.
• Egress checking of VLAN matching does not occur with xconnect and local connect.
• Rewrites are supported.

Summary Steps

1. enable
2. configure terminal
3. interface gigabitethernet slot/port or interface tengigabitethernet slot/port or interface port-channel number
4. [no] shut
5. service instance id [Ethernet [service-name]]
6. encapsulation dot1q vlan-id [cos | comma | hyphen | etype] or encapsulation dot1q vlan-id second-dot1q [any | vlan-id[:vlan-id[:vlan-id]]] or encapsulation dot1q vlan-id cos [0-7] or encapsulation dot1q vlan-id etype [IPv4|IPv6|pppoe-all]

DETAILED STEPS

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 1 | enable   | Enables privileged EXEC mode.  
   |         | • Enter your password if prompted. |
| Example: | Router> enable |

| Step 2 | configure terminal  | Enters global configuration mode. |
| Example: | Router# configure terminal |

| Step 3 | interface gigabitethernet slot/port  | Specifies the Gigabit Ethernet or the Ten Gigabit Ethernet interface to configure, where:  
   | or interface tengigabitethernet slot/port  | • slot/port—Specifies the location of the interface.  
   | or interface port-channel number  | Creates the port-channel interface. |
| Example: | Router(config)# interface gigabitethernet 4/1 |

| Step 4 | [no] shut  | Initiates the selected interface. |
| Example: | Router(config-if)# no shut |
### Supported Configurations

The following are the supported Ethertype and CoS configurations:

- Supported payload ether type configurations for a single tag:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 5</strong></td>
<td></td>
</tr>
<tr>
<td><code>service instance id (Ethernet {service-name})</code></td>
<td>Creates a service instance on the selected ethernet interface.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router(config-if)# service instance 1 ethernet</code></td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>The commands that follow are used for Dot1q or QinQ configurations. Read the purpose of each command to determine which to use.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td></td>
</tr>
<tr>
<td>`encapsulation dot1q vlan-id {cos</td>
<td>comma</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router(config-if-srv)# encapsulation dot1q 100</code></td>
<td></td>
</tr>
<tr>
<td>or</td>
<td></td>
</tr>
<tr>
<td>`encapsulation dot1q vlan-id second-dot1q {any</td>
<td>vlan-id[,vlan-id[-vlan-id]]}`</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router(config-if-srv)# encapsulation dot1q second-dot1q 20</code></td>
<td></td>
</tr>
<tr>
<td>or</td>
<td></td>
</tr>
<tr>
<td><code>encapsulation dot1q vlan-id cos [0-7]</code></td>
<td>Specifies the CoS value in the match criteria for the ingress frames on the service instance.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router(config-if-srv)# encapsulation dot1q 100 cos 5-6</code></td>
<td></td>
</tr>
<tr>
<td>or</td>
<td></td>
</tr>
<tr>
<td>`encapsulation dot1q vlan-id etype [IPv4</td>
<td>IPv6</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router(config-if-srv)# encapsulation dot1q 100 etype ipv4</code></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>encapsulation dot1q 100 cos 5-7 second-dot1q 500</code></td>
<td>Specifies cos value in the match criteria based on the outer tag</td>
</tr>
</tbody>
</table>
Configuring Flexible Service Mapping Based on CoS and Ethertype

Router(config)# interface gigabitethernet 1/1
Router(config-if)# service instance 1 ethernet
Router(config-if-srv)# encapsulation dot1q vlan_id etype etype string

- Supported payload Ethertype configurations for a double tag:
  Router(config)# interface gigabitethernet 1/1
  Router(config-if)# service instance 1 ethernet
  Router(config-if-srv)# encapsulation dot1q vlan id second-dot1q vlan id etype etype string

- Supported payload Ethertype configurations for single tag with single VLAN:

  - Supported payload Ethertype configurations for single tag with range of VLANs:
    Router(config)# interface gigabitethernet 1/1
    Router(config-if)# service instance 1 ethernet
    Router(config-if-srv)# encapsulation dot1q 11-15 etype ipv4
    Router(config-if-srv)# exit
    Router(config-if-srv)# encapsulation dot1q 11-15 etype ipv6
    Router(config-if-srv)# exit
    Router(config-if-srv)# encapsulation dot1q 11-15 etype pppoe-all

  - Supported payload Ethertype configurations for double tag with no range:
    Router(config)# interface gigabitethernet 1/1
    Router(config-if)# service instance 1 ethernet
    Router(config-if-srv)# encapsulation dot1q 10 second-dot1q 1001 etype ipv4
    Router(config-if-srv)# exit
    Router(config-if-srv)# encapsulation dot1q 10 second-dot1q 1001 etype ipv6
    Router(config-if-srv)# exit
    Router(config-if-srv)# encapsulation dot1q 10 second-dot1q 1001 etype pppoe-all

- Supported payload Ethertype configurations for double tag with range on inner VLANs:

- Supported CoS configurations for a single tag:
  Router(config)# interface gigabitethernet 1/1
  Router(config-if)# service instance 1 ethernet
  Router(config-if-srv)# encapsulation dot1q single vlan_id cos single cos value
  Router(config)# interface gigabitethernet 1/1
  Router(config-if)# service instance 1 ethernet
  Router(config-if-srv)# encapsulation dot1q single vlan_id cos list/range of cos values
Chapter 7      Configuring QoS

Configuring Flexible Service Mapping Based on CoS and Ethertype

```
Router(config)# interface gigabitethernet 1/1
Router(config-if)# service instance 1 ethernet
Router(config-if-srv)# encapsulation dot1q list/range of vlan ids cos single cos value
```

- Supported CoS configurations for a double tag:

```
Router(config)# interface gigabitethernet 1/1
Router(config-if)# service instance 1 ethernet
Router(config-if-srv)# encapsulation dot1q single vlan_id second-dot1q single vlan_id cos single cos value
Router(config)# interface gigabitethernet 1/1
Router(config-if)# service instance 1 ethernet
Router(config-if-srv)# encapsulation dot1q single vlan_id second-dot1q single vlan_id cos list/range of cos_values
Router(config)# interface gigabitethernet 1/1
Router(config-if)# service instance 1 ethernet
Router(config-if-srv)# encapsulation dot1q single vlan_id cos single cos_value second-dot1q single vlan_id
Router(config)# interface gigabitethernet 1/1
Router(config-if)# service instance 1 ethernet
Router(config-if-srv)# encapsulation dot1q single vlan_id cos list/range of cos_values second-dot1q single vlan_id
Router(config)# interface gigabitethernet 1/1
Router(config-if)# service instance 1 ethernet
Router(config-if-srv)# encapsulation dot1q single vlan_id cos single cos_value second-dot1q list/range of vlan_ids
```

Examples

The following example displays EVCs with encap dot1q and CoS under bridge-domain.

```
Router# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface gigabitethernet 3/1
Router(config-if)# no shut
Router(config-if)# service instance 1 ethernet
Router(config-if-srv)# encapsulation dot1q 100 cos 5
Router(config-if-srv)# bridge-domain 202
Router(config-if-srv)# interface gigabitethernet 3/2
Router(config-if)# no shut
Router(config-if)# service instance 1 ethernet
Router(config-if-srv)# encapsulation dot1q 100 cos 5
Router(config-if-srv)# bridge-domain 202
Router(config-if-srv)# end
Router#
Router# show bridge-domain 202
Bridge-domain 202 (2 ports in all)
State: UP     Mac learning: Enabled
    GigabitEthernet3/1 service instance 1
    GigabitEthernet3/2 service instance 1
```

The following example shows EVC with encap dot1q and ethertype ipv4 with bridge-domain.

```
Router(config)# interface gigabitethernet 3/1
Router(config-if)# service instance 1 ethernet
Router(config-if-srv)# encapsulation dot1q 100 etype ipv4
Router(config-if-srv)# bridge-domain 202
```
Router(config-if-srv)# interface gigabitethernet 3/2
Router(config-if-srv)# service instance 1 ethernet
Router(config-if-srv)# encapsulation dot1q 100 etype ipv4
Router(config-if-srv)# bridge-domain 202
Router(config-if-srv)#
Router(config-if-srv)# end
Router#

Router# show bridge-domain 202
Bridge-domain 202 (2 ports in all)
State: UP        Mac learning: Enabled
GigabitEthernet3/1 service instance 1
GigabitEthernet3/2 service instance 1

The following is an example of local connect.
Router(config)# interface TenGigabitEthernet2/3
Router(config-if)# no ip address
Router(config-if)# service instance 1 ethernet
Router(config-if-srv)# encapsulation dot1q 2 second-dot1q 2-3 cos 5

Router(config)# interface TenGigabitEthernet2/4
Router(config-if)# no ip address
Router(config-if)# service instance 1 ethernet
Router(config-if-srv)# encapsulation dot1q 2 second-dot1q 2-3 cos 5

Router(config-if-srv)# connect local1 te2/3 1 te2/4 1

The following is an example of xconnect.
Router(config)# interface TenGigabitEthernet2/3
Router(config-if)# no ip address
Router(config-if)# service instance 1 ethernet
Router(config-if-srv)# encapsulation dot1q 2 second-dot1q 2-3 cos 5
Router(config-if-srv)# xconnect 75.1.1.5 10000 encapsulation mpls
!
Router(config-if-srv)# end

The peer side router configuration is below:
Router(config)# interface GigabitEthernet3/0/14
Router(config-if)# no ip address
Router(config-if)# service instance 1 ethernet
Router(config-if-srv)# encapsulation dot1q 2 second-dot1q 2-3 cos 5
Router(config-if-srv)# xconnect 75.1.1.1 10000 encapsulation mpls
!
Router(config-if-srv)# end

Verification

Use the following commands to verify operation.
Egress QoS Scheduling on Port Channel Interfaces

A port channel is an aggregation of individual ethernet links to form a single logical link. Queuing and scheduling is used as a congestion management technique to prioritize selected data traffic while implementing QoS. In Cisco IOS releases prior to 15.1(2)S, queuing and scheduling in egress on a port channel interface or subinterface was not supported, and port channel QoS was implemented using port-channel member link QoS. Effective from Cisco IOS release 15.1(2)S, egress queuing on port channel interfaces or subinterfaces is supported on the Cisco 7600 ES+ line cards.

Restrictions and Usage Guidelines

Follow these restrictions and guidelines while configuring Egress QoS scheduling on port channel interfaces:

- These queuing functions are supported:
  - Traffic Shaping
  - Priority Queuing
  - Bandwidth Remaining Ratio (BRR)
  - Weighted Random Early Detection (WRED)
  - Queue limit

- Minimum bandwidth guarantee is not supported for EVCs and sessions at the parent level of an HQoS policy map.

- If the port channel subinterface is a member of a service group, the minimum bandwidth guarantee can be configured at the service group level, even though the port channel subinterface does not support absolute bandwidth at the parent level.

- WRED and queue limit are supported only at the child level in a policy map.

- QoS service policy cannot be simultaneously configured on a port channel main interface and subinterface except for the port sub-rate shaper.
- QoS service policy can be configured simultaneously on port channel main interface and member link or port channel subinterface and member link. But, port channel member link QoS will be effective only when main interface or sub interface QoS is removed.

- By default a port channel main interface or subinterface follows the flow based load balancing model.

- A 3-level HQoS policy with queuing can be applied only on the port channel interface and not on the subinterface. When a port channel is configured as a layer 2 interface, the 2-level or 3-level queuing policies can be applied in the same way as on a normal layer 3 port-channel main interface.

- Load balancing on a port channel with an access subinterface or sessions is limited to the 1:1 active standby redundancy model. This applies to the QoS on this port channel as well.
Configuring Egress QoS Scheduling on Port Channel Interfaces

Complete these steps to configure Egress QoS scheduling.

**Summary Steps**

1. `enable`
2. `configure terminal`
3. `policy map policy-map-name`
4. `class {class-name | class-default}`
5. `shape average cir [bc] [be]`
6. `interface port-channel number [subinterface] [access]`
7. `encapsulation dot1q vlan-id`
8. `ip address ip-address mask`
9. `service-policy output policy-map-name`
10. `end`
## Detailed Steps

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>enable</td>
<td>Enables the privileged EXEC mode. If prompted, enter the password.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong>&lt;br&gt;Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>configure terminal</td>
<td>Enters the global configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong>&lt;br&gt;Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>policy-map policy-map-name</td>
<td>Specifies the name of the policy map.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong>&lt;br&gt;Router(config)# policy-map policy1</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>class (class-name</td>
<td>class-default)</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong>&lt;br&gt;Router(config-pmap)# class class-default</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>shape average cir [bc] [be]</td>
<td>Specifies the average or peak rate traffic shaping.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong>&lt;br&gt;Router(config-pmap-c)# shape average 100000000</td>
<td></td>
</tr>
</tbody>
</table>
| 6    | interface port-channel number [.subinterface] [access] | Specifies the port channel interface.  
  - `number` - port channel number assigned to an interface.  
  - `subinterface` - Specifies the port channel subinterface. |
|      | **Example:**<br>Router(config)# interface port-channel 1 | |
| 7    | encapsulation dot1q vlan-id | Defines the matching criteria to map dot1Q ingress frames on a sub interface to the appropriate service instance.  
  **vlan-id** - This is an integer in the range of 1 to 4094.  
  **Note** Perform this step only if you configure egress QoS scheduling on a port-channel sub interface or access sub interface. |
|      | **Example:**<br>Router(config-if)# encapsulation dot1q 200 | |
Egress QoS Scheduling on Port Channel Interfaces

### Examples

This example shows how to configure egress QoS scheduling on a port channel main interface.

```plaintext
Router# enable
Router# configure terminal
Router# policy-map p1
Router(config-pmap)# class class-default
Router(config-pmap-c)# shape average 100000000
Router(config)# interface Port-channel 1
Router(config-if)# no ip address
Router(config-if)# service-policy output p1
Router(config)# exit
```

This example shows how to configure egress QoS scheduling on a port channel subinterface.

```plaintext
Router# enable
Router# configure terminal
Router# policy-map p2
Router(config-pmap)# class class-default
Router(config-pmap-c)# shape average 100000000
Router(config)# interface Port-channel 200.1
Router(config-subif)# encapsulation dot1q 200
Router(config-subif)# ip address 100.1.1.1 255.0.0.0
Router(config-if)# service-policy output p2
Router(config)# exit
```

This example shows how to configure egress QoS scheduling on a port channel access subinterface.

```plaintext
Router# enable
Router# configure terminal
Router# policy-map p3
Router(config-pmap)# class class-default
Router(config-pmap-c)# shape average 100000000
Router(config)# interface Port-channel 200.1 access
Router(config-subif)# encapsulation dot1q 200
Router(config-subif)# ip address 100.1.1.1 255.0.0.0
Router(config-if)# service-policy output p3
Router(config)# exit
```
This example shows how to configure egress QoS scheduling on a port channel subinterface with service group.

Router# enable
Router# configure terminal
Router# policy-map p4
Router(config-pmap)# class class-default
Router(config-pmap-c)# shape average 100000000
Router(config)# service-group 2
Router(config-service-group)# service-policy output p4
Router(config)# interface Port-channel 200.1
Router(config-subif)# encapsulation dot1q 200
Router(config-subif)# ip address 100.1.1.1 255.0.0.0
Router(config-subif)# group 2
Router(config)# exit

Verification

Use these commands to verify the egress QoS scheduling on a port channel interface.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show policy-map interface</td>
<td>Displays the configuration of all classes for all policy maps attached to all interfaces.</td>
</tr>
<tr>
<td>show policy-map interface port-channel number</td>
<td>Displays the configuration of all classes for all inbound or outbound policy maps attached to the specified interface.</td>
</tr>
<tr>
<td>show policy-map target service-group</td>
<td>Displays policy map information for service groups.</td>
</tr>
</tbody>
</table>

Troubleshooting Egress QoS Scheduling on a Port Channel Interface

For information on troubleshooting, see Troubleshooting QoS on a ES+ Line Card.
Layer 2 and Layer 3 QoS ACL Classification for EVC

Classification is the separation of packets into traffic classes. Using classification, you can partition network traffic into multiple priority levels or classes of service. Once the classification criteria is defined, the traffic that matches the classification criteria is then subjected to the QoS service policy you apply to the interface. The QoS policy specifies the actions and rules to apply to packets belonging to a particular traffic class.

Ethernet Virtual Connection (EVC) is the primary component used in the deployment of the carrier ethernet technology. Before Cisco IOS release 15.1(2)S, service policies configured under EVCs were classified only using layer 2 MAC access control lists (ACL). Effective from Cisco IOS release 15.1(2)S, applying service policies with layer 2, layer 3 or layer 4 ACLs to EVCs are supported.

Restrictions and Usage Guidelines

Follow these restrictions and guidelines while configuring layer 2 and layer 3 QoS ACL classification:

- Layer 2 ACL QoS classification is supported in both input and output direction on the switchport and EVCs of the main and port channel interfaces that include:
  - ACL matching destination MAC address with address mask.
  - ACL matching source or destination MAC address and COS value.
  - ACL matching source or destination MAC address and VLAN ID.

- If both source and destination MAC addresses are configured in an ACE, the destination address is ignored.

- Neither source nor destination MAC ACL classification is not supported in the same policy.

- COS inner and VLAN inner ACL classifications are not supported.

- Numbered MAC ACL is not supported.

- Layer 3 QoS ACL classification support under EVCs on physical and port channel interface includes:
  - ACL matching an IP source address and an IP protocol
  - ACL matching an IP source and destination address with wild cards
  - ACL matching an IP source address and an IP protocol
  - ACL matching an IP source address and a TCP source port
  - ACL matching an IP source address and a TCP destination port
  - ACL matching an IP source address and the TCP FIN bit
  - ACL matching an IP source address and the TCP SYN bit
  - ACL matching an IP source address and the TCP URG bit
  - ACL matching an IP source address and a UDP source port

- ACL options such as time range, dynamic range and log is not supported.

- IP standard ACL classification is supported.

- Both named and numbered IP ACL classification are supported.

- IPV6 ACL classification is supported.
Configuring Layer 2 and Layer 3 QoS ACL Classification

Complete these steps to configure the layer 2 and layer 3 QoS ACL classification feature.

**Summary Steps**

1. `enable`
2. `configure terminal`
3. `class-map class-map-name`
4. `match access-group access-list-name`
5. `policy-map policy-map-name`
6. `class class-name`
7. `interface type number`
8. `no ip address`
9. `service instance identifier ethernet`
10. `service-policy {input | output} policy-map-name`
11. `end`

**Detailed Steps**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><code>enable</code></td>
<td>Enables the privileged EXEC mode. If prompted, enter the password.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>enable</code></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td><code>configure terminal</code></td>
<td>Enters the global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td><code>class-map class-map-name</code></td>
<td>Specifies the class map name.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>class-map class-map-name</code></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td><code>match access-group access-list-name</code></td>
<td>Configure the match criteria for a class map based on the specified ACL name.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>match access-group access-list-name</code></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td><code>policy-map policy-map-name</code></td>
<td>Specifies the name of the policy map.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>policy-map policy-map-name</code></td>
<td></td>
</tr>
</tbody>
</table>
### Step 6

**Command:**

```text
class (class-name | class-default)
```

**Example:**

```text
Router(config-pmap)# class class-default
```

**Purpose:** Specifies the name of a predefined class included in the service policy.

### Step 7

**Command:**

```text
interface gigabitethernet slot/port
or
interface tengigabitethernet slot/port
or
interface port-channel number
```

**Example:**

```text
Router(config)# interface port-channel 1
```

**Purpose:** Specifies the interface.

- `slot/port` - Specifies the location of the interface.
- `number` - Specifies the port channel interface.

### Step 8

**Command:**

```text
no ip address
```

**Example:**

```text
Router(config-if)# no ip address
```

**Purpose:** Removes an IP address from the interface.

### Step 9

**Command:**

```text
service instance id ethernet
```

**Example:**

```text
Router(config-if)# service instance 1 ethernet
```

**Purpose:** Specifies the ethernet service instance.

### Step 10

**Command:**

```text
service-policy {input | output} policy-map-name
```

**Example:**

```text
Router(config-if)# service-policy output pl
```

**Purpose:** Attaches a traffic policy to the interface.

- `policy-map-name` — Specifies the name of the traffic policy to configure.

### Step 11

**Command:**

```text
end
```

**Example:**

```text
Router(config-if)# end
```

**Purpose:** Closes the configuration session.
Examples

This example shows how to configure the layer 2 and layer 3 QoS ACL classification on a gigabit ethernet interface using a named layer 3 or 4 access control list.

Router# enable
Router# configure terminal
Router(config)# ip access-list extended l3_l4acl
Router(config-ext-nl3-l4acl)# 10 permit ip 0.0.0.1 255.255.0.0 any dscp 32
Router# class-map l3_l4acl
Router(config-cmap)# match access-group name l3_l4acl
Router# policy-map p1
Router(config-pmap)# class l3_l4acl
Router(config)# interface gigabitethernet 1/2
Router(config-if)# no ip address
Router(config-if)# service-instance 1 ethernet
Router(config-if-srv)# service-policy output p1
Router(config)# exit

This example shows how to configure layer 2 and layer 3 QoS ACL classification using a numbered layer 3 or 4 access control list.

Router# enable
Router# configure terminal
Router(config)# ip access-list extended 121
Router(config-ext-nacl)# 10 permit ip 0.0.0.1 255.255.0.0 any dscp 32
Router# class-map 121
Router(config-cmap)# match access-group 121
Router# policy-map p2
Router(config-pmap)# class 121
Router(config)# interface gigabitethernet 1/3
Router(config-if)# no ip address
Router(config-if)# service-instance 1 ethernet
Router(config-if-srv)# service-policy output p2
Router(config)# exit

This example shows how to configure layer 2 and layer 3 QoS ACL classification using a named layer 2 access control list.

Router# enable
Router# configure terminal
Router(config)# MAC access-list extended l2acl
Router(config-ext-nacl)# permit 2222.33ef.0000.0000 any cos 2
Router# class-map l2acl
Router(config-cmap)# match access-group name l2acl
Router# policy-map p3
Router(config-pmap)# class l2acl
Router(config)# interface gigabitethernet 1/2
Router(config-if)# no ip address
Router(config-if)# service-instance 1 ethernet
Router(config-if-srv)# service-policy output p3
Router(config)# exit

Verification

Use these commands to verify the layer 2 and layer 3 QoS ACL classification feature.
Deny ACL QoS Classification

Access Control Lists (ACL) are used to filter data traffic based on a filtering criteria configured on the router interface. Data packets are matched to the criteria specified in the ACLs and traffic is either allowed or denied. When deny ACLs are configured under a class map, the packets that match the ACLs are not classified under that class but classified in the remaining classes depending on the class-map configuration.

Effective from Cisco IOS release 15.1(3)S, deny ACL QoS classification is supported on the Cisco 7600 ES+ line cards, and Access Control Entries (ACEs) configured with a deny action are considered for traffic classification.

Restrictions and Usage Guidelines

Follow these restrictions and guidelines while configuring deny ACL QoS classification:

- You can configure a QoS policy map with deny ACLs for classification on ES+ main interface, sub-interfaces, EVCs, service groups, and sessions.
- The following ACL options are not supported:
  - Time range
  - Dynamic range
  - ACL log
- Deny ACL configuration in the parent policy is supported only on the main interface.
- The number of ACEs per ACL is limited to 8000.
- The maximum number of unique ACLs is 8000.

Configuring Deny ACL QoS Classification

Complete these steps to configure the deny ACL QoS classification feature.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show policy-map interface</td>
<td>Displays the configuration of all classes configured for all policy maps attached to all the interfaces.</td>
</tr>
<tr>
<td>show access-list [access-list-number</td>
<td>Displays the configured ACLs.</td>
</tr>
<tr>
<td>access-list-name]</td>
<td></td>
</tr>
</tbody>
</table>
### Summary Steps

1. enable
2. configure terminal
3. ip access-list extended \{acl-name | acl-num\}
4. \{deny | permit\} protocol \{source source-wildcard\} \{destination destination-wildcard | any\}
5. class-map class-map-name
6. match access-group acl-name
7. policy-map policy-map-name
8. class class-name
9. interface type slot/port
10. no ip address
11. service instance id ethernet
12. service-policy \{input | output\} policy-map-name
13. encapsulation dot1q vlan-id
14. bridge-domain bridge-id
15. end

### Detailed Steps

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>enable</td>
<td>Enables the privileged EXEC mode. If prompted, enter the password.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Example: Router&gt; enable</td>
</tr>
<tr>
<td>2</td>
<td>configure terminal</td>
<td>Enters the global configuration mode.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Example: Router# configure terminal</td>
</tr>
<tr>
<td>3</td>
<td>ip access-list extended {acl-name</td>
<td>acl-num}</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Example: Router(config)# ip access-list extended 101</td>
</tr>
<tr>
<td>4</td>
<td>{deny</td>
<td>permit} protocol {source source-wildcard} {destination destination-wildcard</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Example: Router(config-ext-nacl)# deny ip 200.1.1.0 0.0.0.255 any</td>
</tr>
<tr>
<td>Step</td>
<td>Command</td>
<td>Purpose</td>
</tr>
<tr>
<td>------</td>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td>5</td>
<td><code>class-map class-map-name</code></td>
<td>Specifies the class map name.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config)# class-map c1</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>`match access-group {acl-name</td>
<td>acl-num}`</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config-cmap)# match access-group 101</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td><code>policy-map policy-map-name</code></td>
<td>Specifies the name of the policy map.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config)# policy-map p1</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>`class {class-name</td>
<td>class-default}`</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config-pmap)# class c1</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td><code>interface gigabitethernet slot/port</code> or <code>interface tengigabitethernet slot/port</code> or <code>interface port-channel number</code></td>
<td>Specifies the interface.</td>
</tr>
<tr>
<td></td>
<td>• <code>slot/port</code> - Specifies the location of the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <code>number</code> - Specifies the port channel interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config)# interface gigabitethernet 1/2</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td><code>no ip address</code></td>
<td>Removes an IP address from the interface.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config-if)# no ip address</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td><code>service instance id ethernet</code></td>
<td>Specifies the ethernet service instance.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config-if)# service instance 1 ethernet</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>`service-policy {input</td>
<td>output} policy-map-name`</td>
</tr>
<tr>
<td></td>
<td><code>policy-map-name</code> - Specifies the name of the traffic policy to configure.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config-if-srv)# service-policy output p1</td>
<td></td>
</tr>
</tbody>
</table>
### Deny ACL QoS Classification

**Examples**

This example shows how to configure deny ACL QoS classification on an EVC interface using a numbered access control list.

```
Router# enable
Router# configure terminal
Router(config)# ip access-list extended 102
Router(config-ext-nacl)# deny ip 200.1.1.0 0.0.0.255 any
Router(config)# class-map c1
Router(config-cmap)# match access-group 102
Router(config)# policy-map p1
Router(config-pmap)# class c1
Router(config)# interface gigabitethernet 1/2
Router(config-if)# no ip address
Router(config-if)# service-instance 1 ethernet
Router(config-if-srv)# service-policy output p1
Router(config-if-srv)# encapsulation dot1q 100
Router(config-if-srv)# bridge-domain 10
Router(config-if-srv)# end
```

### Verification

Use these commands to verify the deny ACL QoS classification feature.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show running-config class-map class-map</code></td>
<td>Displays the configuration of a specified class map.</td>
</tr>
<tr>
<td><code>show running-config policy-map policy-map</code></td>
<td>Displays the configuration of a specified policy map.</td>
</tr>
</tbody>
</table>
**Troubleshooting Deny ACL QoS Classification**

For troubleshooting information, see Troubleshooting QoS on a ES+ Line Card.
Ingress HQoS for Port Channel Interfaces

A port channel is an aggregation of individual ethernet links to form a single logical link. Queuing and scheduling is used as a congestion management method to prioritize the selected data traffic while implementing QoS. Effective with Cisco IOS release 15.3(1)S, ingress queuing and scheduling is supported on port channel interfaces of the Cisco 7600 ES+ line cards.

Restrictions

Following restrictions apply to ingress QoS on port channel interfaces:

- These queuing functions are supported:
  - Traffic Shaping
  - Priority Queuing
  - Bandwidth
  - Bandwidth Remaining Ratio (BRR)
  - Queue Limit
- QoS service policy cannot be simultaneously configured on a port channel main interface and subinterface.
- Weighted Random Early Detection (WRED) is not supported.
- QoS service policy can be configured simultaneously on port channel main interface and member link or port channel subinterface and port channel member link. But, port channel member link QoS will be effective only when main interface or sub interface QoS is removed.
- A 3-level HQoS policy can be applied only on the port channel interface and not on the subinterface. When a port channel is configured as a layer 2 interface, the 2-level or 3-level queuing policies can be applied in the same way as on a normal layer 3 port-channel main interface.
- A 2-level HQoS policy can be applied on the port-channel main or sub interface.
- Queuing action with flat policy is not supported in ingress direction on port channel main interface or sub interface.
Configuring Ingress HQoS on Port Channel Interfaces

Complete these steps to configure ingress QoS on a port channel interface.

**Summary Steps**

1. `enable`
2. `configure terminal`
3. `policy map policy-map-child`
4. `class {class-name | class-default}`
5. `bandwidth bandwidth`
6. `exit`
7. `exit`
8. `policy map policy-map-parent`
9. `class {class-name | class-default}`
10. `shape average cir [bc] [be]`
11. `service-policy policy-map-child`
12. `exit`
13. `exit`
14. `interface port-channel number [subinterface]`
15. `service-policy input policy-map-parent`
16. `end`
## Ingress HQoS for Port Channel Interfaces

### Chapter 7      Configuring QoS

#### Ingress HQoS for Port Channel Interfaces

### Detailed Steps

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>enable</td>
<td>Enables the privileged EXEC mode. If prompted, enter the password.</td>
</tr>
</tbody>
</table>
|      |         | **Example:**
|      |         | Router> enable |
| 2    | configure terminal | Enters the global configuration mode. |
|      |         | **Example:**
|      |         | Router# configure terminal |
| 3    | policy-map policy-map-child | Specifies the name of the child policy map. |
|      |         | **Example:**
|      |         | Router(config)# policy-map child |
| 4    | class (class-name | class-default) | Specifies the name of a predefined class included in the service policy. |
|      |         | **Example:**
|      |         | Router(config-pmap)# class class1 |
| 5    | bandwidth bandwidth | Specifies the bandwidth allocated for a class belonging to a policy map. |
|      |         | **Example:**
|      |         | Router(config-pmap-c)# bandwidth 2000 |
| 6    | Exit    | Exits from the class configuration mode. |
|      |         | **Example:**
|      |         | Router(config-pmap-c)# exit |
| 7    | Exit    | Exits from the policy map configuration mode. |
|      |         | **Example:**
|      |         | Router(config-pmap)# exit |
| 8    | policy-map policy-map-parent | Specifies the name of the parent policy map. |
|      |         | **Example:**
|      |         | Router(config)# policy-map parent |
Ingress HQoS for Port Channel Interfaces

### Chapter 7
Configuring QoS

#### Step 9

**Command:**
```
class (class-name | class-default)
```

**Example:**
```
Router(config-pmap)# class class-default
```

**Purpose:** Specifies the name of a predefined parent class included in the service policy.

#### Step 10

**Command:**
```
shape average cir [bc] [be]
```

**Example:**
```
Router(config-pmap-c)# shape average 100000000
```

**Purpose:** Specifies the average or peak rate traffic shaping.
- **cir** - Specifies the committed information rate (CIR), in bits per second (bps).
- **bc** - (Optional) Specifies the committed burst size, in bits.
- **be** - (Optional) Specifies the excess burst size, in bits.

#### Step 11

**Command:**
```
service-policy policy-map-child
```

**Example:**
```
Router(config-pmap-c)# service-policy child
```

**Purpose:** Applies the child service policy to the parent class.
- **policy-map-child** — Name of the configured child service policy.

#### Step 12

**Command:**
```
exit
```

**Example:**
```
Router(config-pmap-c)# exit
```

**Purpose:** Exits from the class configuration mode.

#### Step 13

**Command:**
```
exit
```

**Example:**
```
Router(config-pmap)# exit
```

**Purpose:** Exits from the policy map configuration mode.

#### Step 14

**Command:**
```
interface port-channel number [
subinterface]
```

**Example:**
```
Router(config)# interface port-channel 1
```

**Purpose:** Specifies the port channel interface.
- **number** - port channel number assigned to an interface.
- **subinterface** - port channel subinterface.

#### Step 15

**Command:**
```
service-policy input policy-map-parent
```

**Example:**
```
Router(config-if)# service-policy input parent
```

**Purpose:** Attaches a traffic policy to the input direction of an interface.
- **policy-map-parent** — Specifies the name of the configured parent policy.

#### Step 16

**Command:**
```
end
```

**Example:**
```
Router(config-if)# end
```

**Purpose:** Closes the configuration session.

---

**Command Purpose**

- **class (class-name | class-default)**: Specifies the name of a predefined parent class included in the service policy.
- **shape average cir [bc] [be]**: Specifies the average or peak rate traffic shaping.
  - **cir**: Specifies the committed information rate (CIR), in bits per second (bps).
  - **bc** (Optional): Specifies the committed burst size, in bits.
  - **be** (Optional): Specifies the excess burst size, in bits.
- **service-policy policy-map-child**: Applies the child service policy to the parent class.
- **service-policy input policy-map-parent**: Attaches a traffic policy to the input direction of an interface.
- **end**: Closes the configuration session.
Configuration Examples

This example shows how to configure ingress HQoS on a port channel main interface.

Router# enable
Router# configure terminal
Router# policy-map child
Router(config-pmap)# class class1
Router(config-pmap-c)# bandwidth 2000
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router# policy-map parent
Router(config-pmap)# class class-default
Router(config-pmap-c)# shape average 100000000
Router(config-pmap-c)# service-policy child
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface Port-channel 1
Router(config-if)# service-policy input parent
Router(config)# end

This example shows how to configure ingress HQoS on a port channel subinterface.

Router# enable
Router# configure terminal
Router# policy-map child
Router(config-pmap)# class class1
Router(config-pmap-c)# bandwidth 3000
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router# policy-map parent
Router(config-pmap)# class class-default
Router(config-pmap-c)# shape average 100000000
Router(config-pmap-c)# service-policy child
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface Port-channel 200.1
Router(config-subif)# service-policy input parent
Router(config)# end

Verifying Ingress HQoS

Use these commands to verify the ingress HQoS on a port channel interface.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show policy-map interface</td>
<td>Displays the configuration of policy maps attached to all interfaces.</td>
</tr>
<tr>
<td>show policy-map interface port-channel number</td>
<td>Displays the configuration of all inbound or outbound policy maps attached to the specified interface.</td>
</tr>
</tbody>
</table>
Troubleshooting QoS on a ES+ Line Card

Table 7-14 lists some of the troubleshooting scenarios for a ES+ line card.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show policy-map interface port-channel number service group [service-group-identifier]</code></td>
<td>Displays the policy-map information for service groups that have members attached to a port channel.</td>
</tr>
<tr>
<td><code>show policy-map interface port-channel number service instance service-instance-number</code></td>
<td>Displays the policy-map information for a given service instance under a port channel.</td>
</tr>
</tbody>
</table>
### Troubleshooting Scenarios for QoS in a ES+ Line Card

<table>
<thead>
<tr>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non-functional classification and marking on an ES+ interface.</td>
<td>Use the <code>show tcam interface interface qos type1/type2 ip detail</code> (type1 is for input policy, type2 for output policy) command to verify that the classification hardware parameters are configured correctly and packets are relayed to the right class as shown in this example:</td>
</tr>
</tbody>
</table>

```plaintext
Router#sh tcam interface gig10/1 qos type1 ip detail
* Global Defaults not shared
DPort - Destination Port SPort - Source Port TCP-F
- U -URG          Pro - Protocol
I - Inverted LOU  TOS - TOS Value   -
A -ACK           rtr - Router
MRFM - M -MPLS Packet TN - T -Tcp Control -
P -PSH           COD - C -Bank Care Flag
    - R -Recirc. Flag   - N -Non-cachable
    - R -RST           - I -OrdIndep. Flag
    - F -Fragment Flag CAP - Capture Flag -
S -SYN                - D -Dynamic Flag
    - M -More Fragments F-P - FlowMask-Prior. -
F -FIN              T - V(Value)/M(Mask)/R(Result)
X - XTAG            (*) - Bank Priority
-----------------------------
Interface: 1104  label: 1537  lookup_type: 1
protocol: IP  packet-type: 0
+----------+-------------------+-------------------+-------------------+-------------------+
|T|Index| Dest Ip Addr | Source Ip Addr | DPort | SPort | TCP-F | Pro|MRFM|X|TOS|TN|COD|F-P|
+----------+-------------------+-------------------+-------------------+-------------------+
M 36836 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 <-
0 ------- 0 X--- 0 0
```
Chapter 7 Configuring QoS

Troubleshooting QoS on a ES+ Line Card

<table>
<thead>
<tr>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Result: 1D29C700 &lt;-</td>
<td>{ in the above output, &quot;&lt;-&quot; indicates which class the packets being classified to. }</td>
</tr>
<tr>
<td>2) Do do an elam capture and check the the QoS values received and re-written to.</td>
<td></td>
</tr>
<tr>
<td>Elam can capture data coming from the Constellation Data Bus interface (DBUS), partial results coming from the L3 Forwarding Engine (Tycho), and final results transmitted on the Constellation Result Bus (RBUS).</td>
<td></td>
</tr>
<tr>
<td>Following are the commands to use the elam.</td>
<td></td>
</tr>
<tr>
<td>1. Select slot on which to run elam: show platform capture elamasic &lt;sup/tyco&gt; slot &lt;slot no&gt;</td>
<td></td>
</tr>
<tr>
<td>2. Set the trigger for packets of interest: show platform capture elam trigger &lt;intersted fields of the packets such as vlan id, source and destination IP, source index, etc&gt;</td>
<td></td>
</tr>
<tr>
<td>3. Start the Elam capture: show platform capture elam start</td>
<td></td>
</tr>
<tr>
<td>4. Show the status of Elam: show platform capture elam status</td>
<td></td>
</tr>
<tr>
<td>5. Show the captured Elam data: show platform capture elam data</td>
<td></td>
</tr>
<tr>
<td>Weneed to repeat the above steps for both dbus as well as rbus captures .</td>
<td></td>
</tr>
<tr>
<td>show platform capture elam help</td>
<td></td>
</tr>
<tr>
<td>* Return a brief help that reminds how to use the ELAM commands</td>
<td></td>
</tr>
</tbody>
</table>
7-124

Cisco 7600 Series Ethernet Services Plus (ES+) and Ethernet Services Plus T (ES+T) Line Card Configuration Guide

Chapter 7 Configuring QoS

Troubleshooting QoS on a ES+ Line Card

Note

“<->” indicates the class where the packets are being classified.

- Perform an ELAM (Embedded Logic Analyzer Module) capture and check the QoS values received and re-written. ELAM can capture data from the Constellation Data Bus interface (DBUS), partial results coming from the L3 Forwarding Engine, and final results transmitted on the Constellation Result Bus (RBUS).

- Use these commands to capture ELAM data on Dbus and Rbus:
  - Use the `show platform capture elam help` to use the ELAM commands.
  - Select the slot to use the ELAM `show platform capture elam asic sup/tyco slot slot no` command.
  - Use the `show platform capture elam trigger` command to trigger the packets.
  - Use the `show platform capture elam start` command to start the Elam capture.
  - Use the `show platform capture elam status` command to show the status of Elam.
  - Use the `show the captured Elam data` command to show the platform capture elam data.
  - If the issue persists, contact TAC.

Service group issues

Use the `show run service-group, show service group details, show service group statistics` command to display the policy-map applied to service-group, policy-map applied on service-group along with the members of the service-group, and the output of the number of service-groups configured. Share the output with TAC for troubleshooting.

QoS policy map configured on port-channel interface is non-functional

Check the following commands on the route processor:

- Use the `show interface interface-type slot/port` command check the interface statistics to confirm the traffic flow.
- Verify the policy-map and the class map definitions:
  - `show run policy-map <policy-map name>`
  - `show run class-map <class-map name>`
  - `show run interface <interface>`
- If the issue persists, contact TAC.
<table>
<thead>
<tr>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traffic statistic issues in service instances and service groups</td>
<td>Use the <code>show ethernet service instance stat</code> and <code>show service-group traffic-stats</code> commands to troubleshoot traffic issues in service instances and groups. If the issue persists, contact TAC.</td>
</tr>
<tr>
<td>Service-group traffic statistics issue</td>
<td>Use the <code>clear service-group traffic-stats</code> command to clear redundant traffic statistics. If the issue persists, contact TAC.</td>
</tr>
<tr>
<td>Incorrect QoS rates on EVCs and service group issues</td>
<td>• Use the <code>show policy-map interface &lt;intf&gt; service instance efp#</code> and <code>show policy-map interface intf service group group#</code> commands to confirm the policy map information. If the issue persists, contact TAC.</td>
</tr>
<tr>
<td></td>
<td>• Use the <code>clear counters</code> command from the route processor and derive the output of <code>show policy-map interface intf service instance efp</code> and <code>show policy-map interface intf service group group statistics</code> and study the conformed and drop rates. If the issue persists, contact TAC.</td>
</tr>
<tr>
<td>QoS service policy on a suspend mode</td>
<td>The policy moves to a suspension mode when there are no member links attached to it. Use the <code>show etherchannel summary</code> command to check member links attached to it and their status. If the issue persists, contact TAC.</td>
</tr>
<tr>
<td></td>
<td>PE2#show etherchannel summary</td>
</tr>
<tr>
<td></td>
<td>Flags: D - down P - bundled in port-channel</td>
</tr>
<tr>
<td></td>
<td>I - stand-alone s - suspended</td>
</tr>
<tr>
<td></td>
<td>H - Hot-standby (LACP only)</td>
</tr>
<tr>
<td></td>
<td>R - Layer3 S - Layer2</td>
</tr>
<tr>
<td></td>
<td>U - in use f - failed to allocate aggregator</td>
</tr>
<tr>
<td></td>
<td>M - not in use, minimum links not met</td>
</tr>
<tr>
<td></td>
<td>u - unsuitable for bundling</td>
</tr>
<tr>
<td></td>
<td>w - waiting to be aggregated</td>
</tr>
<tr>
<td></td>
<td>d - default port</td>
</tr>
<tr>
<td></td>
<td>Number of channel-groups in use: 4</td>
</tr>
<tr>
<td></td>
<td>Number of aggregators: 4</td>
</tr>
<tr>
<td></td>
<td>Group Port-channel Protocol Ports</td>
</tr>
<tr>
<td></td>
<td>1 Po1(RU) - Gi2/12(P)</td>
</tr>
<tr>
<td></td>
<td>2 Po2(SD) -</td>
</tr>
<tr>
<td></td>
<td>3 Po3(SD) -</td>
</tr>
<tr>
<td></td>
<td>4 Po4(RU) - Gi2/1(P) Gi2/2(P) Gi2/22(P)</td>
</tr>
<tr>
<td>Troubleshooting policing issues on the port-channel for member links</td>
<td>On the ES+ line card, policing is performed per NP (Network Processor) aggregate basis. For example, if 100M policer is configured on PC sub-targets and if there are 2 member-links spread across 2 different Network Processors (NPs), traffic from both the member-links are policed to 200M and not 100M. If the issue persists, contact TAC.</td>
</tr>
<tr>
<td>across a network processor</td>
<td></td>
</tr>
</tbody>
</table>
### Troubleshooting QoS on a ES+ Line Card

#### Queuing issues

Use the `show policy map interface` command to view the queuing details, shaping, bandwidth, queue limit and WRED values, that has all these and highlight the queuing, bandwidth parameters.

#### Rate counters are not accurate

- Rate counters are updated in fixed intervals. Use the `load-interval seconds` command to increase the load interval for accurate rate counter values.

#### Traffic classified incorrectly

- Use the `show run class-map` command to check the class-map definition.
- Use the `show policy-map interface` command to check the classification statistics.
- Use the `show tcam interface interface qos type1/type2 ip detail` (type1 is for input policy, type2 for output policy) command to verify that the classification hardware parameters are configured correctly and packets are relayed to the right class as shown in the example:

```
Router#sh tcam interface gig10/1 qos type1 ip detail
* Global Defaults shared
DPort - Destination Port  SPort - Source Port TCP-F - U
-URG       Pro  - Protocol
I  - Inverted LOU  TOS  - TOS Value
- A -ACK     rtr  - Router
MRFM  - M -MPLS Packet  TN  - T -Tcp Control
- P -PSH   COD  - C -Bank Care Flag
  - R -Recirc. Flag  - N -Non-cachable
  - R -RST  - I -OrdIndep. Flag
  - F -Fragment Flag  CAP  - Capture Flag
  - S -SYN  - D -Dynamic Flag
  - M -More Fragments  F-P  - FlowMask-Prior.
  - F -FIN  T  - V(Value)/M(Mask)/R(Result)
  X  - XTAG  (*)  - Bank Priority

Interface: 1018  label: 513 lookup_type: 1
protocol: IP packet-type: 0
|T|Index| Dest Ip Addr | Source Ip Addr| DPort |

V 36828 0.0.0.0 0.0.0.0 P=0
P=0 ------ 0 ---- 0 0 -- ---- 0-0 <-
M 36836 0.0.0.0 0.0.0.0 0
0 ------ 0 X--- 0 0 <-

R rslt: 142811A8 <-
V 36829 0.0.0.0 0.0.0.0 P=0
P=0 ------ 0 M--- 0 0 -- ---- 0-0
M 36836 0.0.0.0 0.0.0.0 0
0 ------ 0 X--- 0 0
R rslt: 142811A8
```

**Note**

<- indicates the class where the packets are classified.
### Problem
Excessive drops in packets

### Solution
- Use the `show policy map interface` command to check if the offered rate exceeds the configured policer shape rate.
- Queuing on ES20/SIP-600 is performed on the L1 frame with an overhead of 24 bytes. The ES20 supports user-defined overhead accounting for shape/wfq classes.
- Drops also occur due to low queue-limit configured. Increase the queue-limits value if unaccounted drops are seen.
- In case of excessive drops, check if WRED can be used as, illustrated in this example.

```bash
Router#sh run policy-map queuing
Building configuration...

Current configuration : 276 bytes

! policy-map queuing
  class prec1
    bandwidth 200000
  class prec2
    shape average 100000000
    random-detect
    random-detect precedence 1 100 1000
    random-detect precedence 2 150 1500
    random-detect precedence 3 200 800
  class class-default
    shape average 100000000

! end
```

```
Router#
Router#sh pol
Router#sh policy-map int gig10/6
GigabitEthernet10/6
  Service-policy output: queuing
  Counters last updated 00:00:27 ago

  Class-map: prec1 (match-all)
  0 packets, 0 bytes
  5 minute offered rate 0000 bps, drop rate 0000 bps
  Match: ip precedence 1
  Queueing
  queue limit 65536 packets
  (queue depth/total drops/no-buffer drops) 0/0/0
```
Chapter 7  Configuring QoS

Troubleshooting QoS on a ES+ Line Card

<<< drops due to bandwidth over subscription

(pkts output/bytes output) 0/0
bandwidth 200000 kbps  <<< bandwidth
configured in the policy-map

Class-map: prec2 (match-all)
0 packets, 0 bytes
5 minute offered rate 0000 bps, drop rate 0000 bps
Match: ip precedence 2
Match: precedence 2
Queueing
queue limit 32768 packets

(queue depth/total drops/no-buffer drops) 0/0/0

<<< drops due to shaper

(pkts output/bytes output) 0/0
shape (average) cir 100000000, bc 400000, be 400000

target shape rate 100000000  <<< shaper
configured in the policy-map by the user
Exp-weight-constant: 9 (1/512)
Mean queue depth: 0 packets

class Random drop Tail drop Minimum
Maximum Mark
pkt/s bytes pkt/s bytes thresh prob
0 3457/5687000 0/0
8192 16384 1/10  <<< wred packet/bytes counts
and threshold values

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0/0</td>
<td>0/0</td>
<td>100</td>
</tr>
<tr>
<td>1000</td>
<td>1/10</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>0/0</td>
<td>0/0</td>
<td>150</td>
</tr>
<tr>
<td>1500</td>
<td>1/10</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>1408/4508780</td>
<td>0/0</td>
<td></td>
</tr>
<tr>
<td>200</td>
<td>800</td>
<td>1/10</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>0/0</td>
<td>0/0</td>
<td>12288</td>
</tr>
<tr>
<td>16384</td>
<td>1/10</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>0/0</td>
<td>0/0</td>
<td>13312</td>
</tr>
<tr>
<td>16384</td>
<td>1/10</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>0/0</td>
<td>0/0</td>
<td>14336</td>
</tr>
<tr>
<td>16384</td>
<td>1/10</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>0/0</td>
<td>0/0</td>
<td>15360</td>
</tr>
<tr>
<td>16384</td>
<td>1/10</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Problem</td>
<td>Solution</td>
<td></td>
<td></td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Class-map: class-default (match-any)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0 packets, 0 bytes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5 minute offered rate 0000 bps, drop rate 0000 bps</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Match: any</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Queuing</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>queue limit 32768 packets</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(queue depth/total drops/no-buffer drops) 0/0/0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(pkts output/bytes output) 0/0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>shape (average) cir 100000000, bc 400000, be 400000</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>target shape rate 100000000 &lt;&lt;&lt; shaper configured in the policy-map by the user</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Problem: Bandwidth not met

Solution:
Check if the queue limits are configured right.

Based on this example, check if the bandwidth and priority class has been configured correctly.

Router#sh run policy-map queuing
Building configuration...

Current configuration : 276 bytes
!
policy-map queuing
 class prec1
  bandwidth 200000
class prec2
  shape average 100000000
  random-detect
  random-detect precedence 1 100 1000
  random-detect precedence 2 150 1500
  random-detect precedence 3 200 800
class class-default
  shape average 100000000
!
end

Router#

Router#sh pol
Router#sh policy-map int gig10/6
GigabitEthernet10/6

Service-policy output: queuing

Counters last updated 00:00:27 ago

Class-map: prec1 (match-all)
  0 packets, 0 bytes
  5 minute offered rate 0000 bps, drop rate 0000 bps
  Match: ip precedence 1
  Queueing
  queue limit 65536 packets
  (queue depth/total drops/no-buffer drops) 0/0/0
<<< drops due to bandwidth over subscription
  (pkts output/bytes output) 0/0
  bandwidth 200000 kbps <<< bandwidth
configured in the policy-map
### Problem
Debug QoS policing traffic issues in EARL

<table>
<thead>
<tr>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Check the policer configured on the hardware. For aggregate policer and microflow policer, check the aggregate Id value using the `sh mls qos [ip</td>
</tr>
<tr>
<td>• Use the <code>show tcam interface</code> command to check whether or not the TCAM is programmed correctly for the interface. The result from the output can be used to find different fields in the QoS hardware on that interface.</td>
</tr>
</tbody>
</table>

### Warning
Use the `show tcam interface` command with the module option to view the tcam programming on the DFCs.

| • Check the rate and burst configured on the policer. |
| • Use Elam (Embedded Logical Analyzer Module) Capture tool (captures the packets routed internally) to view the packet details. Share the output information with TAC for further troubleshooting. |

### Problem
Microflow policing issues

<table>
<thead>
<tr>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Use the <code>sh fm int xxx</code> and <code>sh mls netflow ip detail</code> commands to view the output. Share the information with TAC for troubleshooting.</td>
</tr>
<tr>
<td>• Validation of microflow policing: Use the <code>show mls netflow ip qos module module</code> command to validate the microflow policing. In this output, <code>Pkts/Bytes</code> indicates total forwarded packets/bytes, and the police count column indicates the drop count.</td>
</tr>
</tbody>
</table>

```
Router#sh mls netflow ip qos module 10
Displaying Netflow entries in module 10
DstIP           SrcIP           Prot:SrcPort:DstPort Src i/f         :AdjPtr
------------------------------------------------------
------------------------------------------------------
Pkts         Bytes         LastSeen   QoS    PoliceCount
Threshold   Leak
------------------------------------------------------
------------------------------------------------------
Drop  Bucket
--------------------------
20.1.1.2        10.1.1.2        255 :0      :0       --
0x0
12857116     591427336     17:35:40   0x80   5117484352
0           0
NO    3145792
```

### Problem
Policer not receiving the packets

<table>
<thead>
<tr>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use the `sh mls qos [ip</td>
</tr>
</tbody>
</table>
### Troubleshooting QoS on a ES+ Line Card

<table>
<thead>
<tr>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incorrect QoS ACLs in TCAM</td>
<td>• Use the <code>sh qm int xxx</code> and `sh tcam int xx qos [type1</td>
</tr>
</tbody>
</table>
| Expected CIR/PIR rate not reached | 1. TCP traffic displays rates below the CIR due to the slow-start algorithms and retransmissions.  
2. To increase the CIR/PIR rates, use a traffic generator or UDP traffic.  
3. Use large burst values to police TCP traffic. |
| Egress packet drop issues         | • Check the traffic type.  
• Raise the bandwidth. E.g: old 10M users – gig link in a 10 gig backbone network.  
• Modify the queue limit or introduce WRED. |
### Problem
Non-functional classification and marking on an ES+ interface.

### Solution
Use the `show tcam interface interface qos type1/type2 ip detail` (type1 is for input policy, type2 for output policy) command to verify that the classification hardware parameters are configured correctly and packets are relayed to the right class as shown in this example:

```
Router#sh tcam interface gig10/1 qos type1 ip detail
```

* Global Defaults not shared

<table>
<thead>
<tr>
<th>DPort - Destination Port</th>
<th>SPort - Source Port</th>
<th>TCP-F</th>
</tr>
</thead>
<tbody>
<tr>
<td>- U -URG</td>
<td>Pro - Protocol</td>
<td></td>
</tr>
<tr>
<td>I - Inverted LOU</td>
<td>TOS - TOS Value</td>
<td></td>
</tr>
<tr>
<td>A -ACK</td>
<td>rtr - Router</td>
<td></td>
</tr>
<tr>
<td>MRFM - M -MPLS Packet</td>
<td>TN - T -Tcp Control</td>
<td></td>
</tr>
<tr>
<td>P -PSH</td>
<td>COD - C -Bank Care Flag</td>
<td></td>
</tr>
<tr>
<td>- R -Recirc. Flag</td>
<td>- N -Non-cachable</td>
<td></td>
</tr>
<tr>
<td>- R -RST</td>
<td>I -OrdIndep. Flag</td>
<td></td>
</tr>
<tr>
<td>- F -Fragment Flag</td>
<td>CAP - Capture Flag</td>
<td></td>
</tr>
<tr>
<td>S -SYN</td>
<td>- D -Dynamic Flag</td>
<td></td>
</tr>
<tr>
<td>- M -More Fragments</td>
<td>F-P - FlowMask-Prior.</td>
<td></td>
</tr>
<tr>
<td>F -FIN</td>
<td>T - V(Value)/M(Mask)/R(Result)</td>
<td></td>
</tr>
<tr>
<td>X - XTAG</td>
<td>(*) - Bank Priority</td>
<td></td>
</tr>
</tbody>
</table>

-----------------------------------------
Interface: 1104  label: 1537  lookup_type: 1
protocol: IP  packet-type: 0

<table>
<thead>
<tr>
<th>T</th>
<th>Index</th>
<th>Dest Ip Addr</th>
<th>Source Ip Addr</th>
<th>DPort</th>
<th>SPort</th>
<th>TCP-F</th>
<th>Pro</th>
<th>MRFM</th>
<th>X</th>
<th>TOS</th>
<th>TN</th>
<th>COD</th>
<th>F-P</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0</td>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
<td>0</td>
<td>0.0.0.0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0 ---- 0</td>
<td>0 ---- 0-0</td>
<td>&lt;=</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>M 36836</td>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>------ 0</td>
<td>X--- 0</td>
<td>&lt;=</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**result: 1D29C700**  
{ in the above output, "<" indicates which class the packets being classified to. }

2) Do do an elam capture and check the QoS values received and re-written to.

Elam can capture data coming from the Constellation Data Bus interface (DBUS), partial results coming from the L3 Forwarding Engine (Tycho), and final results transmitted on the Constellation Result Bus (RBUS).
Troubleshooting QoS on a ES+ Line Card

Problem |
---|
Following are the commands to use the elam. 
1. Select slot on which to run elam: show platform capture elam asic <sup/tyco> slot <slot no>
2. Set the trigger for packets of interest: show platform capture elam trigger <intersted fields of the packets such as vlan id, source and destination IP, source index, etc>
3. Start the Elam capture: show platform capture elam start
4. Show the status of Elam: show platform capture elam status
5. Show the captured Elam data: show platform capture elam data

We need to repeat the above steps for both dbus as well as rbus captures.

cmd = show platform capture elam help

* Return a brief help that reminds how to use the ELAM commands

Note: "<-" indicates the class where the packets are being classified.

- Perform an ELAM (Embedded Logic Analyzer Module) capture and check the QoS values received and re-written. ELAM can capture data from the Constellation Data Bus interface (DBUS), partial results coming from the L3 Forwarding Engine, and final results transmitted on the Constellation Result Bus (RBUS).

- Use these commands to capture ELAM data on Dbus and Rbus:
  - Use the show platform capture elam help to use the ELAM commands.
  - Select the slot to use the ELAM show platform capture elam asic sup/tyco slot <slot no> command.
  - Use the show platform capture elam trigger command to trigger the packets.
  - Use the show platform capture elam start command to start the Elam capture.
  - Use the show platform capture elam status command to show the status of Elam.
  - Use the show the captured Elam data command to show the platform capture elam data.
  - If the issue persists, contact TAC.
<table>
<thead>
<tr>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service group issues</td>
<td>Use the <code>show run service-group</code>, <code>show service group details</code>, <code>show service group statistics</code> command to display the policy-map applied to service-group, policy-map applied on service-group along with the members of the service-group, and the output of the number of service-groups configured. Share the output with TAC for troubleshooting.</td>
</tr>
</tbody>
</table>
| QoS policy map configured on port-channel interface is non-functional | Check the following commands on the route processor:  
  - Use the `show interface interface-type slot/port` command check the interface statistics to confirm the traffic flow.  
  - Verify the policy-map and the class map definitions:  
    - `show run policy-map <polic-map name>`  
    - `show run class-map <class-map name>`  
    - `show run interface <interface>`  
  - If the issue persists, contact TAC. |
| Traffic statistic issues in service instances and service groups | Use the `show ethernet service instance stat` and `show service-group traffic-stats` commands to troubleshoot traffic issues in service instances and groups. If the issue persists, contact TAC. |
| Service-group traffic statistics issue | Use the `clear service-group traffic-stats` command to clear redundant traffic statistics. If the issue persists, contact TAC. |
| Incorrect QoS rates on EVCs and service group issues | • Use the `show policy-map interface <intf> service instance efp#` and `show policy-map interface intf service group group#` commands to confirm the policy map information. If the issue persists, contact TAC.  
  • Use the `clear counters` command from the route processor and derive the output of `show policy-map interface intf service instance efp` and `show policy-map interface intf service group group statistics` and study the conformed and drop rates. If the issue persists, contact TAC. |
### Troubleshooting QoS on a ES+ Line Card

<table>
<thead>
<tr>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>QoS service policy on a suspend mode</td>
<td>The policy moves to a suspension mode when there are no member links attached to it. Use the <code>show etherchannel summary</code> command to check member links attached to it and their status. If the issue persists, contact TAC.</td>
</tr>
</tbody>
</table>

```plaintext
PE2#show etherchannel summary
Flags:  D - down        P - bundled in port-channel
        I - stand-alone  s - suspended
        H - Hot-standby  L - LACP only
        R - Layer3       S - Layer2
        U - in use       f - failed to allocate aggregator
        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port

Number of channel-groups in use: 4
Number of aggregators: 4

<table>
<thead>
<tr>
<th>Group</th>
<th>Port-channel</th>
<th>Protocol</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Po1(RU)</td>
<td>-</td>
<td>Gi2/12(P)</td>
</tr>
<tr>
<td>2</td>
<td>Po2(SD)</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Po3(SD)</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Po4(RU)</td>
<td>-</td>
<td>Gi2/1(P)  Gi2/2(P) Gi2/22(P)</td>
</tr>
</tbody>
</table>
```

### Troubleshooting policing issues on the port-channel for member links across a network processor

On the ES+ line card, policing is performed per NP (Network Processor) aggregate basis. For example, if 100M policer is configured on PC sub-targets and if there are two member-links spread across two different NPs, traffic from both the member-links are policed to 200M and not 100M. If the issue persists, contact TAC.

### Queuing issues

Use the `show policy map interface` command to view the queuing details, shaping, bandwidth, queue limit and WRED values that has all these and highlight the queuing, bandwidth parameters.