Classification, Marking, and Policing

- Information About Classification, Marking, and Policing Policies, page 34-1
- How to Configure Classification, Marking, and Policing Policies, page 34-7

Note
- For complete syntax and usage information for the commands used in this chapter, see these publications:
- Cisco IOS Release 15.1SY supports only Ethernet interfaces. Cisco IOS Release 15.1SY does not support any WAN features or commands.

Tip
For additional information about Cisco Catalyst 6500 Series Switches (including configuration examples and troubleshooting information), see the documents listed on this page:
  Participate in the Technical Documentation Ideas forum

Information About Classification, Marking, and Policing Policies

- Classification, Marking, and Policing Policy Overview, page 34-1
- Traffic Classification, page 34-2
- Traffic Marking, page 34-3
- Information about Policing, page 34-4

Classification, Marking, and Policing Policy Overview

The classification, marking, and policing configuration is defined by the policies attached to an interface. Classification, marking, and policing are unaffected by any QoS commands configured on ingress interfaces or by queueing policies.
Traffic Classification

Traffic classification allows the network to recognize traffic as it falls into classes that you have configured. Network traffic must be classified to apply specific QoS to it.

Classification can be inclusive (for example, all of the traffic in a Layer 2 VLAN or all of the traffic passing through an interface) or classification can be very specific (for example, you can use a class map with match commands that recognize specific aspects of the traffic).

You can classify and apply QoS (for example, marking) and then, on another interface or network device, classify again based on the marked value and apply other QoS.

The PFC and any DFCs supports a single match command in class-map match-all class maps, except that the match protocol command can be configured in a class map with the match dscp or match precedence command.

The PFC and any DFCs supports multiple match commands in class-map match-any class maps.

Note

PFC QoS supports a maximum of 9 commands that match DSCP or IP precedence values in class maps and ACLs.

Class maps can use the match commands listed in Table 34-1 to configure a traffic class that is based on the match criteria.

<table>
<thead>
<tr>
<th>match Commands</th>
<th>Direction</th>
<th>Match Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>match access-group {access_list_number</td>
<td>Both</td>
<td>Access control list (ACL).</td>
</tr>
<tr>
<td>name access_list_name}</td>
<td></td>
<td>Note: Use ACLs to match the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>—CoS value</td>
</tr>
<tr>
<td></td>
<td></td>
<td>—VLAN ID</td>
</tr>
<tr>
<td></td>
<td></td>
<td>—Packet length</td>
</tr>
<tr>
<td>match any</td>
<td>Both</td>
<td>Any match criteria.</td>
</tr>
<tr>
<td>match cos</td>
<td>Ingress</td>
<td>CoS value.</td>
</tr>
<tr>
<td>match discard-class</td>
<td>Both</td>
<td>Discard class value.</td>
</tr>
<tr>
<td>match dscp</td>
<td>Both</td>
<td>DSCP value.</td>
</tr>
<tr>
<td>Note: The match protocol</td>
<td></td>
<td>command can be configured in a class map with the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>match dscp command.</td>
</tr>
<tr>
<td>match l2 miss</td>
<td>Ingress</td>
<td>Layer 2 traffic flooded in a VLAN because it is</td>
</tr>
<tr>
<td></td>
<td></td>
<td>addressed to a currently unlearned MAC-Layer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>destination address.</td>
</tr>
<tr>
<td>match mpls experimental topmost</td>
<td>Both</td>
<td>MPLS EXP value in the topmost label.</td>
</tr>
<tr>
<td>match precedence</td>
<td>Both</td>
<td>IP precedence values.</td>
</tr>
<tr>
<td>Note: The match protocol</td>
<td></td>
<td>command can be configured in a class map with the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>match precedence command.</td>
</tr>
</tbody>
</table>
### Information About Classification, Marking, and Policing Policies

#### Chapter 34  Classification, Marking, and Policing

#### Chapter 34  Classification, Marking, and Policing

#### Information About Classification, Marking, and Policing Policies

**Table 34-1  Traffic Classification Class Map match Commands and Match Criteria (continued)**

<table>
<thead>
<tr>
<th>match Commands</th>
<th>Direction</th>
<th>Match Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>`match protocol {arp</td>
<td>ip</td>
<td>ipv6}`</td>
</tr>
<tr>
<td><strong>Note</strong> The <code>match protocol</code> command can be configured in a class map with the <code>match dscp</code> or <code>match precedence</code> command.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>match qos-group</code></td>
<td>Both</td>
<td>QoS group ID.</td>
</tr>
</tbody>
</table>

The PFC and any DFCs supports these ACL types for use with the **match access group** command:

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Numbered ACLs</th>
<th>Extended ACLs</th>
<th>Named ACLs</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4</td>
<td>Yes: 1 to 99, 1300 to 1999</td>
<td>Yes: 100 to 199, 2000 to 2699</td>
<td>Yes</td>
</tr>
<tr>
<td>IPv6</td>
<td>Not applicable</td>
<td>Yes (named)</td>
<td>Yes</td>
</tr>
<tr>
<td>MAC Layer</td>
<td>Not applicable</td>
<td>Not applicable</td>
<td>Yes</td>
</tr>
<tr>
<td>ARP</td>
<td>Not applicable</td>
<td>Not applicable</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Traffic Marking

**Note** Policing can also mark traffic.

Marking network traffic allows you to set or modify the attributes for a specific class of traffic, which allows class-based QoS features to recognize traffic classes based on the marking. There are two traffic marking methods:

- You can apply a configured value with a policy-map `set` command. **Table 34-2** lists the available policy-map `set` commands and the corresponding attribute.

#### Table 34-2  Configured-Value Policy-Map Commands

<table>
<thead>
<tr>
<th>set Commands</th>
<th>Traffic Attribute</th>
<th>Ingress?</th>
<th>Egress?</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>set cos cos_value</code></td>
<td>Layer 2 CoS value</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td><code>set dscp dscp_value</code></td>
<td>Layer 3 DSCP value</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td><code>set precedence precedence_value</code></td>
<td>Layer 3 IP precedence value</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td><code>set dscp tunnel dscp_value</code></td>
<td>Layer 3 DSCP value in the tunnel header of a Generic Routing Encapsulation (GRE) tunneled packet</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td><code>set discard-class discard_value</code></td>
<td>Discard-class value</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td><code>set qos-group group_id</code></td>
<td>QoS group ID</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td><code>set mpls experimental imposition exp_value</code></td>
<td>MPLS experimental (EXP) field on all imposed label entries</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td><code>set mpls experimental topmost exp_value</code></td>
<td>MPLS experimental (EXP) field on all topmost label entries</td>
<td>Y</td>
<td>Y</td>
</tr>
</tbody>
</table>
You can apply a map to received values with a policy-map set command. Table 34-3 lists the available policy-map set commands and the corresponding attribute.

<table>
<thead>
<tr>
<th>set Commands</th>
<th>Map Name</th>
<th>Traffic Attribute</th>
<th>Ingress?</th>
<th>Egress?</th>
</tr>
</thead>
<tbody>
<tr>
<td>set dscp cos</td>
<td>dscp-cos-map</td>
<td>Layer 3 DSCP value</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>set dscp precedence</td>
<td>dscp-precedence-map</td>
<td>Layer 3 DSCP value</td>
<td>Y</td>
<td>N</td>
</tr>
</tbody>
</table>

**Information about Policing**

- **Overview of Policing**, page 34-4
- **Per-Interface Policers**, page 34-5
- **Aggregate Policers**, page 34-5
- **Microflow Policers**, page 34-6

**Overview of Policing**

You can configure policers to do the following:

- Mark traffic
- Limit bandwidth utilization and mark traffic

Policers can be applied to ingress and egress interfaces. Ingress policing is applied first, followed by egress policing.

Policing can rate limit incoming and outgoing traffic so that it adheres to the traffic forwarding rules defined by the QoS configuration. Sometimes these configured rules for how traffic should be forwarded through the system are referred to as a contract. If the traffic does not adhere to this contract, it is marked down to a lower DSCP value or dropped.

Policing does not buffer out-of-profile packets. As a result, policing does not affect transmission delay. In contrast, traffic shaping works by buffering out-of-profile traffic, which moderates traffic bursts. (PFC QoS does not support shaping.)

The PFC and DFCs support ingress and egress PFC QoS, which includes ingress and egress policing. Policers act on ingress traffic per-port or per-VLAN. For egress traffic, the policers act per-VLAN only.

Policing uses the Layer 2 frame size. You specify the bandwidth utilization limit as a committed information rate (CIR). You can also specify a higher peak information rate (PIR). Packets that exceed a rate are “out of profile” or “nonconforming.”

In each policer, you specify if out-of-profile packets are to be dropped or to have a new DSCP value applied to them (applying a new DSCP value is called “markdown”). Because out-of-profile packets do not retain their original priority, they are not counted as part of the bandwidth consumed by in-profile packets.

If you configure a PIR, the PIR out-of-profile action cannot be less severe than the CIR out-of-profile action. For example, if the CIR out-of-profile action is to mark down the traffic, then the PIR out-of-profile action cannot be to transmit the traffic.

For all policers, PFC QoS uses a configurable global table that maps the internal DSCP value to a marked-down DSCP value. When markdown occurs, PFC QoS gets the marked-down DSCP value from the table. You cannot specify marked-down DSCP values in individual policers.
Note

- By default, the markdown table is configured so that no markdown occurs: the marked-down DSCP values are equal to the original DSCP values. To enable markdown, configure the table appropriately for your network.
- When you apply both ingress policing and egress policing to the same traffic, both the input policy and the output policy must either markdown traffic or drop traffic. PFC QoS does not support ingress markdown with egress drop or ingress drop with egress markdown.

Per-Interface Policers

PFC QoS applies the bandwidth limits specified in a per-interface policer to matched traffic. For example, if you configure a per-interface policer to allow 1 Mbps for all matched TFTP traffic, it limits the TFTP traffic to 1 Mbps.

You define per-interface policers in a policy map class with the `police` command. If you attach per-interface policers to multiple ingress ports, each one polices the matched traffic on each ingress port separately.

Aggregate Policers

- Aggregate Policer Overview, page 34-5
- Distributed Aggregate Policers, page 34-5
- Nondistributed Aggregate Policers, page 34-6

Aggregate Policer Overview

PFC QoS applies the bandwidth limits specified in an aggregate policer cumulatively to all flows in matched traffic. For example, if you configure an aggregate policer to allow 1 Mbps for all TFTP traffic flows on VLAN 1 and VLAN 3, it limits the TFTP traffic for all flows combined on VLAN 1 and VLAN 3 to 1 Mbps.

You create named aggregate policers with the `platform qos aggregate-policer` command. If you attach a named aggregate policer to multiple ingress ports, it polices the matched traffic from all the ingress ports to which it is attached.

You can configure up to 1,023 aggregate policers; the configured aggregate policers can be applied to interfaces to configure up to 16,384 policer instances.

Distributed Aggregate Policers

When distributed aggregate policing is enabled, aggregate policers synchronize policing on interfaces supported by different DFC-equipped switching modules or the PFC. Distributed aggregate policing applies to the first 4,096 aggregate policer instances of these types:

- Aggregate policers applied to VLAN, tunnel, or port channel interfaces.
- Shared aggregate policers.
- Aggregate policers in egress policies.

With distributed aggregate policing enabled, aggregate policers in excess of the hardware-supported capacity function as nondistributed aggregate policers.
Information About Classification, Marking, and Policing Policies

Nondistributed Aggregate Policers

Nondistributed aggregate policing works independently on each DFC-equipped switching module and independently on the PFC, which supports any non-DFC-equipped switching modules. Aggregate policing does not combine flow statistics from different DFC-equipped switching modules. You can display aggregate policing statistics for each DFC-equipped switching module and for the PFC and any non-DFC-equipped switching modules supported by the PFC.

Each PFC or DFC polices independently, which might affect QoS features being applied to traffic that is distributed across the PFC and any DFCs. Examples of these QoS feature are:

- Policers applied to a port channel interface.
- Policers applied to a switched virtual interface.
- Egress policers applied to either a Layer 3 interface or an SVI.

Policers affected by this restriction deliver an aggregate rate that is the sum of all the independent policing rates.

Microflow Policers

PFC QoS applies the bandwidth limit specified in a microflow policer separately to each flow in matched traffic. For example, if you configure a microflow policer to limit the TFTP traffic to 1 Mbps on VLAN 1 and VLAN 3, then 1 Mbps is allowed for each flow in VLAN 1 and 1 Mbps for each flow in VLAN 3. In other words, if there are three flows in VLAN 1 and four flows in VLAN 3, the microflow policer allows each of these flows 1 Mbps.

You can configure PFC QoS to apply the bandwidth limits in a microflow policer as follows:

- You can create microflow policers with up to 127 different rate and burst parameter combinations.
- You create microflow policers in a policy map class with the `police flow` command.
- You can configure a microflow policer to use only source addresses, which applies the microflow policer to all traffic from a source address regardless of the destination addresses.
- You can configure a microflow policer to use only destination addresses, which applies the microflow policer to all traffic to a destination address regardless of the source addresses.
- For MAC-Layer microflow policing, PFC QoS considers MAC-Layer traffic with the same protocol and the same source and destination MAC-Layer addresses to be part of the same flow, including traffic with different EtherTypes. You can configure MAC ACLs to filter IPX traffic.
- You cannot apply microflow policing to ARP traffic.
- Release 15.1(1)SY1 and later releases support Egress Microflow Destination-Only Policing. Egress policing is per-VLAN, applied on either a Layer 3 interface or an SVI. With releases earlier than Release 15.1(1)SY1, policies attached with the `output` keyword do not support microflow policing.

You can include both an aggregate policer and a microflow policer in each policy map class to police a flow based on both its own bandwidth utilization and on its bandwidth utilization combined with that of other flows.

Note

If traffic is both aggregate and microflow policed, then the aggregate and microflow policers must both be in the same policy-map class and each must use the same `conform-action` and `exceed-action` keyword option: `drop`, `set-dscp-transmit`, `set-prec-transmit`, or `transmit`.
For example, you could create a microflow policer with a bandwidth limit suitable for individuals in a group, and you could create a named aggregate policer with bandwidth limits suitable for the group as a whole. You could include both policers in policy map classes that match the group’s traffic. The combination would affect individual flows separately and the group aggregately.

For policy map classes that include both an aggregate and a microflow policer, PFC QoS responds to an out-of-profile status from either policer and, as specified by the policer, applies a new DSCP value or drops the packet. If both policers return an out-of-profile status, then if either policer specifies that the packet is to be dropped, it is dropped; otherwise, PFC QoS applies a marked-down DSCP value.

### How to Configure Classification, Marking, and Policing Policies

- Enabling Distributed Aggregate Policing, page 34-7
- Configuring a Class Map, page 34-8
- Configuring a Policy Map, page 34-9
- Attaching a Policy Map to an Interface, page 34-17
- Configuring Dynamic Per-Session Attachment of a Policy Map, page 34-19

### Enabling Distributed Aggregate Policing

To enable distributed aggregate policing, perform this task:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>`Router(config)# platform qos police distributed {strict</td>
<td>loose}`</td>
</tr>
<tr>
<td><code>Router(config)# platform qos police distributed strict</code></td>
<td>The <code>strict</code> keyword prevents application of aggregate policers to interfaces that would exceed available hardware acceleration resources.</td>
</tr>
<tr>
<td><code>Router(config)# platform qos police distributed loose</code></td>
<td>The <code>loose</code> keyword allows application of aggregate policers as nondistributed to interfaces that would exceed available hardware acceleration resources.</td>
</tr>
</tbody>
</table>

This example shows how to enable strict distributed aggregate policing globally:

```
Router(config)# platform qos police distributed strict
```

This example shows how to disable distributed aggregate policing globally:

```
Router(config)# no platform qos police distributed
```
Configuring a Class Map

- Creating a Class Map, page 34-8
- Configuring Filtering in a Class Map, page 34-8
- Verifying Class Map Configuration, page 34-8

Creating a Class Map

To create a class map, perform this task:

**Command**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>`Router(config)# class-map match-all</td>
<td>match-any class_name`</td>
</tr>
<tr>
<td><strong>Note</strong>: If you do not enter a <code>match</code> keyword, the default is <code>match-all</code>.</td>
<td></td>
</tr>
</tbody>
</table>

Configuring Filtering in a Class Map

To configure filtering in a class map, enter match commands as described in Table 34-1, “Traffic Classification Class Map match Commands and Match Criteria”.

Verifying Class Map Configuration

To verify class map configuration, perform this task:

**Command**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong>: <code>Router (config-cmap)# end</code></td>
<td>Exits configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong>: <code>Router# show class-map class_name</code></td>
<td>Verifies the configuration.</td>
</tr>
</tbody>
</table>

This example shows how to create a class map named **ipp5** and how to configure filtering to match traffic with IP precedence 5:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# class-map ipp5
Router(config-cmap)# match ip precedence 5
Router(config-cmap)# end
```

This example shows how to verify the configuration:

```
Router# show class-map ipp5
Class Map match-all ipp5 (id 1)
  Match ip precedence 5
```
Configuring a Policy Map

- Policy Map Overview, page 34-9
- Creating a Policy Map, page 34-9
- Policy Map Class Configuration Guidelines and Restrictions, page 34-9
- Creating a Policy Map Class and Configuring Filtering, page 34-9
- Configuring Policy Map Class Actions, page 34-10
- Verifying Policy Map Configuration, page 34-17

Policy Map Overview

Policy maps can contain one or more policy map classes, each with different policy map commands. Configure a separate policy map class in the policy map for each type of traffic that an interface receives. Put all commands for each type of traffic in the same policy map class. PFC QoS does not attempt to apply commands from more than one policy map class to matched traffic.

Creating a Policy Map

To create a policy map, perform this task:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router(config)# policy-map policy_name</td>
<td>Creates a policy map.</td>
</tr>
</tbody>
</table>

Policy Map Class Configuration Guidelines and Restrictions

- PFC QoS does not support the class class_name destination-address, class class_name input-interface, class class_name qos-group, and class class_name source-address policy map commands.
- PFC QoS supports the class default policy map command.
- PFC QoS does not detect the use of unsupported commands until you attach a policy map to an interface.
- PFC QoS does not support multiple ACL matches per class.

Creating a Policy Map Class and Configuring Filtering

To create a policy map class and configure it to filter with a class map, perform this task:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router(config-pmap)# class class_name</td>
<td>Creates a policy map class and configures it to filter with a class map.</td>
</tr>
<tr>
<td>Note</td>
<td>PFC QoS supports class maps that contain a single match command.</td>
</tr>
</tbody>
</table>
Configuring Policy Map Class Actions

- Policy Map Class Action Restrictions, page 34-10
- Configuring Policy Map Class Marking, page 34-11
- Configuring the Policy Map Class Trust State, page 34-11
- Configuring Policy Map Class Policing, page 34-11

Policy Map Class Action Restrictions

- Policy maps can contain one or more policy map classes.
- Put all commands for each type of traffic in the same policy map class.
- PFC QoS only applies commands from one policy map class to traffic. After traffic has matched the filtering in one policy map class, QoS does not apply the filtering configured in other policy map classes.
- For hardware-switched traffic, PFC QoS does not support the bandwidth, priority, queue-limit, or random-detect policy map class commands. You can configure these commands because they can be used for software-switched traffic.
- PFC QoS does not support the set qos-group policy map class commands.
- PFC QoS supports the set ip dscp and set ip precedence policy map class commands for IPv4 traffic.
  - You can use the set ip dscp and set ip precedence commands on non-IP traffic to mark the internal DSCP value, which is the basis of the egress Layer 2 CoS value.
  - The set ip dscp and set ip precedence commands are saved in the configuration file as set dscp and set precedence commands.
- PFC QoS supports the set dscp and set precedence policy map class commands for IPv4 and IPv6 traffic.
- You cannot do all three of the following in a policy map class:
  - Mark traffic with the set commands
  - Configure the trust state
  - Configure policing

In a policy map class, you can either mark traffic with the set commands or do one or both of the following:
  - Configure the trust state
  - Configure policing

Note When configure policing, you can mark traffic with policing keywords.

- Layer 2 network control protocols - such as STP, LLDP, CDP, LACP cannot be remarked with a policy map. These protocols are automatically treated with priority in hardware and cannot be overwritten.
Configuring Policy Map Class Marking

PFC QoS supports policy map class marking for all traffic with set policy map class commands. To configure policy map class marking, perform this task:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router(config-pmap-c)# set {dscp dscp_value</td>
<td>precedence ip_precedence_value}</td>
</tr>
</tbody>
</table>

Configuring the Policy Map Class Trust State

Note

You cannot attach a policy map that configures a trust state with the service-policy output command.

To configure the policy map class trust state, perform this task:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router(config-pmap-c)# trust {cos</td>
<td>dscp</td>
</tr>
</tbody>
</table>

When configuring the policy map class trust state, note the following information:

- Enter the no trust command to use the trust state configured on the ingress port (this is the default).
- With the cos keyword, PFC QoS sets the internal DSCP value from received or ingress port CoS.
- With the dscp keyword, PFC QoS uses received DSCP.
- With the ip-precedence keyword, PFC QoS sets DSCP from received IP precedence.

Configuring Policy Map Class Policing

- Policy Map Class Policing Restrictions, page 34-12
- Using a Named Aggregate Policer, page 34-12
- Configuring a Per-Interface Policer, page 34-13
- Configuring a Per-Interface Microflow Policer, page 34-15
Policy Map Class Policing Restrictions

- PFC QoS does not support the `set-qos-transmit` policer keyword.
- PFC QoS does not support the `set-dscp-transmit` or `set-prec-transmit` keywords as arguments to the `exceed-action` keyword.
- PFC QoS does not detect the use of unsupported keywords until you attach a policy map to an interface.
- Policing with the `conform-action transmit` keywords sets the port trust state of matched traffic to trust DSCP or to the trust state configured by a `trust` command in the policy map class.

Using a Named Aggregate Policer

To use a named aggregate policer, perform this task:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>Router(config-pmap-c)# police aggregate aggregate_name</code></td>
<td>Configures the policy map class to use a previously defined named aggregate policer.</td>
</tr>
</tbody>
</table>

- When distributed aggregate policing is enabled, note the following information:
  - Distributed aggregate policers synchronize policing on interfaces supported by different DFC-equipped switching modules or the PFC. Distributed aggregate policing applies to the first 4,096 aggregate policers of these types:
    - Aggregate policers applied to VLAN, tunnel, or port channel interfaces.
    - Shared aggregate policers.
    - Aggregate policers in egress policies.
  - Distributed aggregate policers in excess of the hardware-supported capacity function as nondistributed aggregate policers.
- When distributed aggregate policing is not enabled, note the following information:
  - Aggregate policing works independently on each DFC-equipped switching module and independently on the PFC, which supports any non-DFC-equipped switching modules. Aggregate policing does not combine flow statistics from different DFC-equipped switching modules. You can display aggregate policing statistics for each DFC-equipped switching module and for the PFC and any non-DFC-equipped switching modules supported by the PFC.
  - Each PFC or DFC polices independently, which might affect QoS features being applied to traffic that is distributed across the PFC and any DFCs. Examples of these QoS feature are:
    - Policers applied to a port channel interface.
    - Policers applied to a switched virtual interface.
    - Egress policers applied to either a Layer 3 interface or an SVI.
  - Policers affected by this restriction deliver an aggregate rate that is the sum of all the independent policing rates.
Configuring a Per-Interface Policer

To configure a per-interface policer and a policy-map class to use it, perform this task:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router(config-pmap-c)# police bits_per_second [normal_burst_bytes [maximum_burst_bytes]] [pir peak_rate_bps] [[[conform-action selected_action] exceed-action selected_action] violate-action selected_action]</td>
<td>Creates a per-interface policer and configures the policy-map class to use it.</td>
</tr>
<tr>
<td>Router(config-pmap-c)# police rate units bps [burst burst_bytes] [peak-rate peak_rate_bps bps] [peak-burst peak_burst_bytes bytes] [conform-action selected_action] [exceed-action selected_action] violate-action selected_action]</td>
<td>Creates a per-interface policer with police rate configured in bits per second (bps).</td>
</tr>
<tr>
<td>Router(config-pmap-c)# police rate units pps [burst burst_packets] [conform-action selected_action] [exceed-action selected_action] violate-action selected_action]</td>
<td>Creates a per-interface policer with police rate configured in packets per second (pps).</td>
</tr>
</tbody>
</table>

- When you apply both ingress policing and egress policing to the same traffic, both the input policy and the output policy must either mark down traffic or drop traffic. PFC QoS does not support ingress markdown with egress drop or ingress drop with egress markdown.
- Policing uses the Layer 2 frame size.
- See the “Restrictions for PFC QoS” section on page 33-1 for information about rate and burst size granularity.
- The valid range of values for the CIR bits_per_second parameter is as follows:
  - Minimum—32 kilobits per second, entered as 32000
  - Maximum—256 gigabits per second, entered as 256000000000
- The normal_burst_bytes parameter sets the CIR token bucket size.
- The maximum_burst_bytes parameter sets the PIR token bucket size.
- When configuring the size of a token bucket, note the following information:
  - Because the token bucket must be large enough to hold at least one frame, configure the token bucket size to be larger than the maximum size of the traffic being policed.
  - For TCP traffic, configure the token bucket size as a multiple of the TCP window size, with a minimum value at least twice as large as the maximum size of the traffic being policed.
  - The maximum_burst_bytes parameter must be set larger than the normal_burst_bytes parameter.
  - To sustain a specific rate, set the token bucket size to be at least the rate value divided by 2000.
  - The minimum token bucket size is 1 byte, entered as 1.
  - The maximum token bucket size is 512 megabytes, entered as 512000000.
- The valid range of values for the pir bits_per_second parameter is as follows:
  - Minimum—32 kilobits per second, entered as 32000 (the value cannot be smaller than the CIR bits_per_second parameters)
  - Maximum—256 gigabits per second, entered as 256000000000
How to Configure Classification, Marking, and Policing Policies

- (Optional) You can specify a conform action for matched in-profile traffic as follows:
  - The default conform action is `transmit`, which sets the policy map class trust state to `trust DSCP` unless the policy map class contains a `trust` command.
  - To set PFC QoS labels in untrusted traffic, you can enter the `set-dscp-transmit` keyword to mark matched untrusted traffic with a new DSCP value or enter the `set-prec-transmit` keyword to mark matched untrusted traffic with a new IP precedence value. The `set-dscp-transmit` and `set-prec-transmit` keywords are only supported for IP traffic. PFC QoS sets egress ToS and CoS from the configured value.
  - You can enter the `drop` keyword to drop all matched traffic.
  - Ensure that aggregate and microflow policers that are applied to the same traffic each specify the same conform-action behavior.

- (Optional) For traffic that exceeds the CIR, you can specify an exceed action as follows:
  - For marking without policing, you can enter the `transmit` keyword to transmit all matched out-of-profile traffic.
  - The default exceed action is `drop`, except with a `maximum_burst_bytes` parameter (`drop` is not supported with a `maximum_burst_bytes` parameter).

  **Note** When the exceed action is `drop`, PFC QoS ignores any configured violate action.

  - You can enter the `policed-dscp-transmit` keyword to cause all matched out-of-profile traffic to be marked down as specified in the markdown map.

  **Note** When you create a policer that does not use the `pir` keyword and the `maximum_burst_bytes` parameter is equal to the `normal_burst_bytes` parameter (which is the case if you do not enter the `maximum_burst_bytes` parameter), the `exceed-action policed-dscp-transmit` keywords cause PFC QoS to mark traffic down as defined by the `policed-dscp max-burst` markdown map.

- (Optional) For traffic that exceeds the PIR, you can specify a violate action as follows:
  - For marking without policing, you can enter the `transmit` keyword to transmit all matched out-of-profile traffic.
  - The default violate action is equal to the exceed action.
  - You can enter the `policed-dscp-transmit` keyword to cause all matched out-of-profile traffic to be marked down as specified in the markdown map.

This example shows how to create a policy map named `max-pol-ipp5` that uses the class-map named `ipp5`, which is configured to trust received IP precedence values and is configured with a maximum-capacity aggregate policer and with a microflow policer:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# policy-map max-pol-ipp5
Router(config-pmap)# class ipp5
Router(config-pmap-c)# trust ip-precedence
Router(config-pmap-c)# police 2000000000 200000000 conform-action set-prec-transmit 6
Router(config-pmap-c)# police flow 10000000 10000 conform-action set-prec-transmit 6
Router(config-pmap-c)# end
```
This example displays information about police rate configured in bps and pps. It also displays information about the policy-map and the class-map configured.

```console
4sup-vss#sh running-config policy-map bps
Building configuration...
Current configuration : 221 bytes
! policy-map bps
  class bps
  police rate 10000 bps burst 100 bytes peak-rate 20000 bps peak-burst 2000 bytes
  conform-action set-dscp-transmit 5 exceed-action policed-dscp-transmit violate-action drop
end
```

```console
4sup-vss#sh running-config policy-map pps
Building configuration...
Current configuration : 182 bytes
! policy-map pps
  class pps
  police rate 10000 pps burst 1000 packets conform-action set-dscp-transmit 5 exceed-action policed-dscp-transmit violate-action drop
end
```

### Configuring a Per-Interface Microflow Policer

To configure a per-interface microflow policer, perform this task:

- When you apply both ingress policing and egress policing to the same traffic, both the input policy and the output policy must either mark down traffic or drop traffic. PFC QoS does not support ingress markdown with egress drop or ingress drop with egress markdown.
- Policing uses the Layer 2 frame size.
- See the “Restrictions for PFC QoS” section on page 33-1 for information about rate and burst size granularity.
- You can enter the `mask src-only` keywords to base flow identification only on source addresses, which applies the microflow policer to all traffic from each source address. PFC QoS supports the `mask src-only` keywords for both IP traffic and MAC traffic.
- You can enter the `mask dest-only` keywords to base flow identification only on destination addresses, which applies the microflow policer to all traffic to each source address. PFC QoS supports the `mask dest-only` keywords for both IP traffic and MAC traffic. Release 15.1(1)SY1 and later releases support Egress Microflow Destination-Only Policing. Egress policing is per-VLAN, applied on either a Layer 3 interface or an SVI.
- By default and with the `mask full-flow` keywords, PFC QoS bases IP flow identification on source IP address, destination IP address, the Layer 3 protocol, and Layer 4 port numbers.
• PFC QoS considers MAC-Layer traffic with the same protocol and the same source and destination MAC-Layer addresses to be part of the same flow, including traffic with different EtherTypes.

• Microflow policers do not support the maximum_burst_bytes parameter, the pir bits_per_second keyword and parameter, or the violate-action keyword.

Note: The flowmask requirements of microflow policing, NetFlow, and NetFlow data export (NDE) might conflict.

• The valid range of values for the CIR bits_per_second parameter is as follows:
  – Minimum—32 kilobits per second, entered as 32000
  – Maximum—256 gigabits per second, entered as 25600000000

• The normal_burst_bytes parameter sets the CIR token bucket size.

• When configuring the size of a token bucket, note the following information:
  – Because the token bucket must be large enough to hold at least one frame, configure the token bucket size to be larger than the maximum size of the traffic being policed.
  – For TCP traffic, configure the token bucket size as a multiple of the TCP window size, with a minimum value at least twice as large as the maximum size of the traffic being policed.
  – The maximum_burst_bytes parameter must be set larger than the normal_burst_bytes parameter.
  – To sustain a specific rate, set the token bucket size to be at least the rate value divided by 2000.
  – The minimum token bucket size is 1 byte, entered as 1.
  – The maximum token bucket size is 512 megabytes, entered as 512000000.

• (Optional) You can specify a conform action for matched in-profile traffic as follows:
  – The default conform action is transmit, which sets the policy map class trust state to trust DSCP unless the policy map class contains a trust command.
  – To set PFC QoS labels in untrusted traffic, you can enter the set-dscp-transmit keyword to mark matched untrusted traffic with a new DSCP value or enter the set-prec-transmit keyword to mark matched untrusted traffic with a new IP precedence value. The set-dscp-transmit and set-prec-transmit keywords are only supported for IP traffic. PFC QoS sets egress ToS and CoS from the configured value.
  – You can enter the drop keyword to drop all matched traffic.
  – Ensure that aggregate and microflow policers that are applied to the same traffic each specify the same conform-action behavior.

• (Optional) For traffic that exceeds the CIR, you can specify an exceed action as follows:
  – For marking without policing, you can enter the transmit keyword to transmit all matched out-of-profile traffic.
  – The default exceed action is drop, except with a maximum_burst_bytes parameter (drop is not supported with a maximum_burst_bytes parameter).

Note: When the exceed action is drop, PFC QoS ignores any configured violate action.

  – You can enter the policed-dscp-transmit keyword to cause all matched out-of-profile traffic to be marked down as specified in the markdown map.
When you create a policer that does not use the `pir` keyword and the `maximum_burst_bytes` parameter is equal to the `normal_burst_bytes` parameter (which is the case if you do not enter the `maximum_burst_bytes` parameter), the `exceed-action policed-dscp-transmit` keywords cause PFC QoS to mark traffic down as defined by the `policed-dscp max-burst` markdown map.

## Verifying Policy Map Configuration

To verify policy map configuration, perform this task:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Router(config-pmap-c)# end&lt;br&gt;Exits policy map class configuration mode. &lt;br&gt;Note Enter additional class commands to create additional classes in the policy map.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Router# show policy-map <code>policy_name</code>&lt;br&gt;Verifies the configuration.</td>
</tr>
</tbody>
</table>

This example shows how to verify the configuration:

```plaintext
Router# show policy-map max-pol-ipp5
Policy Map max-pol-ipp5
class ipp5
class ipp5
  police flow 10000000 10000 conform-action set-prec-transmit 6 exceed-action
  policed-dscp-transmit
  trust precedence
  police 2000000000 2000000000 2000000000 conform-action set-prec-transmit 6 exceed-action
  policed-dscp-transmit
Router#
```

## Attaching a Policy Map to an Interface

To attach a policy map to an interface, perform this task:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Router(config)# interface {{(vlan vlan_ID)</td>
</tr>
<tr>
<td>Step 2</td>
<td>Router(config-if)# service-policy [input</td>
</tr>
<tr>
<td>Step 3</td>
<td>Router(config-if)# end&lt;br&gt;Exits configuration mode.</td>
</tr>
</tbody>
</table>

- Do not attach a service policy to a port that is a member of an EtherChannel.
- PFC QoS supports the `output` keyword only on Layer 3 interfaces (either LAN ports configured as Layer 3 interfaces or VLAN interfaces). You can attach both an input and an output policy map to a Layer 3 interface.
- VLAN-based or port-based PFC QoS on Layer 2 ports is not relevant to policies attached to Layer 3 interfaces with the `output` keyword.

- Release 15.1(1)SY1 and later releases support Egress Microflow Destination-Only Policing. **Egress policing is per-VLAN**, applied on either a Layer 3 interface or an SVI. With releases earlier than Release 15.1(1)SY1, policies attached with the `output` keyword do not support microflow policing.

- You cannot attach a policy map that configures a trust state with the `service-policy output` command.

- Filtering based on IP precedence or DSCP in policies attached with the `output` keyword uses the received IP precedence or DSCP values. Filtering based on IP precedence or DSCP in policies attached with the `output` keyword is not based on any IP precedence or DSCP changes made by ingress QoS.

- A shared aggregate policer cannot be applied in both ingress and egress directions.

- When distributed aggregate policing is enabled, aggregate policers synchronize policing on interfaces supported by different DFC-equipped switching modules or the PFC. Distributed aggregate policing applies to the first 4,096 aggregate policer instances of these types:
  - Aggregate policers applied to VLAN, tunnel, or port channel interfaces.
  - Shared aggregate policers.
  - Aggregate policers in egress policies.

With distributed aggregate policing enabled, aggregate policers in excess of the hardware-supported capacity function as nondistributed aggregate policers.

- Nondistributed aggregate policing works independently on each DFC-equipped switching module and independently on the PFC, which supports any non-DFC-equipped switching modules. Aggregate policing does not combine flow statistics from different DFC-equipped switching modules. You can display aggregate policing statistics for each DFC-equipped switching module and for the PFC and any non-DFC-equipped switching modules supported by the PFC.

Each PFC or DFC polices independently, which might affect QoS features being applied to traffic that is distributed across the PFC and any DFCs. Examples of these QoS feature are:
  - Policers applied to a port channel interface.
  - Policers applied to a switched virtual interface.
  - Egress policers applied to either a Layer 3 interface or an SVI.

Policers affected by this restriction deliver an aggregate rate that is the sum of all the independent policing rates.

- For nonaggregate policers, each PFC or DFC polices independently, which might affect QoS features being applied to traffic that is distributed across the PFC and any DFCs. Examples of these QoS feature are:
  - Policers applied to a port channel interface.
  - Policers applied to a switched virtual interface.
  - Egress policers applied to either a Layer 3 interface or an SVI.

Policers affected by this restriction deliver an aggregate rate that is the sum of all the independent policing rates.

- When you apply both ingress policing and egress policing to the same traffic, both the input policy and the output policy must either mark down traffic or drop traffic. PFC QoS does not support ingress markdown with egress drop or ingress drop with egress markdown.
This example shows how to attach the policy map named `pmap1` to gigabit Ethernet port 5/36:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface gigabitethernet 5/36
Router(config-if)# service-policy input pmap1
Router(config-if)# end
```

This example shows how to verify the configuration:

```
Router# show policy-map interface gigabitethernet 5/36
gigabitethernet5/36
  service-policy input: pmap1
    class-map: cmap1 (match-all)
      0 packets, 0 bytes
      5 minute rate 0 bps
      match: ip precedence 5
    class cmap1
      police 8000 8000 conform-action transmit exceed-action drop
    class-map: cmap2 (match-any)
      0 packets, 0 bytes
      5 minute rate 0 bps
      match: ip precedence 2
      0 packets, 0 bytes
      5 minute rate 0 bps
    class cmap2
      police 8000 10000 conform-action transmit exceed-action drop
```

---

**Configuring Dynamic Per-Session Attachment of a Policy Map**

- Policy Map Dynamic Per-Session Attachment Prerequisites, page 34-19
- Defining and Associating Policy Maps, page 34-19

**Policy Map Dynamic Per-Session Attachment Prerequisites**

- Define the ingress and egress QoS policy maps to be assigned when users are authenticated.
- Configure identity policies to specify the policy maps to be assigned.
- In the user profiles on the RADIUS server, configure the Cisco vendor-specific attributes (VSAs) to specify which ingress and egress QoS policy maps will be assigned to each user.

**Defining and Associating Policy Maps**

To define the policy maps and associate them with an identity policy, follow these steps:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>Router(config)# policy-map in_policy_name</code> Configures an ingress QoS policy map.</td>
</tr>
<tr>
<td>Step 2</td>
<td><code>Router(config-pmap)# class class_map_name</code> Configures policy map class.</td>
</tr>
<tr>
<td>Step 3</td>
<td><code>Router(config-pmap-c)# exit</code> Exits policy map class configuration submode.</td>
</tr>
<tr>
<td>Step 4</td>
<td><code>Router(config)# policy-map out_policy_name</code> Configures an egress QoS policy map.</td>
</tr>
</tbody>
</table>
To remove the identity policy, use the `no identity policy policy_name` command.

After the policy maps have been defined, configure the Cisco AV pair attributes in each user profile on the RADIUS server using the policy map names:

- `cisco-avpair = “ip:sub-policy-In=in_policy_name”`
- `cisco-avpair = “ip:sub-policy-Out=out_policy_name”`

To set the Cisco AV pair attributes on the RADIUS server, perform the following task:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 5</td>
<td><code>Router(config-pmap)# class class_map_name</code> Configures policy map class.</td>
</tr>
<tr>
<td>Step 6</td>
<td><code>Router(config-pmap-c)# exit</code> Exits policy map class configuration submode.</td>
</tr>
<tr>
<td>Step 7</td>
<td><code>Router(config)# identity policy policy1</code> Creates an identity policy, and enters identity policy configuration submode.</td>
</tr>
<tr>
<td>Step 8</td>
<td><code>Router(config-identity-policy)# service-policy type qos input in_policy_name</code> Associates the ingress QoS policy map with this identity.</td>
</tr>
<tr>
<td>Step 9</td>
<td><code>Router(config-identity-policy)# service-policy type qos output out_policy_name</code> Associates the egress QoS policy map with this identity.</td>
</tr>
<tr>
<td>Step 10</td>
<td><code>Router(config-identity-policy)# end</code> Exits identity policy configuration submode and returns to privileged EXEC mode.</td>
</tr>
</tbody>
</table>

This example shows the configuration in the user file on the RADIUS server:

```plaintext
userid Password ="cisco"
Service-Type = Framed,
Framed-Protocol = PPP,
cisco-avpair = "sub-policy-In=example_in_qos",
cisco-avpair = "sub-policy-Out=example_out_qos"
```

This example shows the output of the `show epm session summary` command when a session is active:

```
Router# show epm session summary
EPM Session Information
-----------------------
Total sessions seen so far : 5
Total active sessions : 1
Session IP Address : 192.0.2.1
-----------------------
```
This example shows the output of the `show epm session ip ip_addr` command when a session is active on the interface with IP address 192.0.2.1:

```
Router# show epm session ip 192.0.2.1

Admission feature       : AUTHPROXY
AAA Policies            :
Input Service Policy    : in_policy_name
Output Service Policy   : out_policy_name
```

Tip

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


Participate in the Technical Documentation Ideas forum