## Contents

**PORT-SHAPER AND LLQ IN THE PRESENCE OF EFPs** 17

- Finding Feature Information  17
- Restrictions for Port-Shaper and LLQ in the Presence of EFPs  17
- Information About Port-Shaper and LLQ in the Presence of EFPs  18
  - Ethernet Flow Points and LLQ  18
- How to Configure Port-Shaper and LLQ in the Presence of EFPs  18
  - Configuring Hierarchical Policy Maps  18
  - Configuring an LLQ Policy Map  20
  - Configuring Port Level Shaping on the Main Interface with Ethernet Flow Points  22
- Configuration Examples for Port-Shaper and LLQ in the Presence of EFPs  24
  - Example: Configuring Hierarchical QoS Port Level Shaping on the Main Interface with EFPs  24
  - Example: Configuring Port Level Shaping on the Main Interface with EFPs  25

**ADDITIONAL REFERENCES** 26

**FEATURE INFORMATION FOR PORT-SHAPER AND LLQ IN THE PRESENCE OF EFPs** 27

---

**CONTROL PLANE POLICING** 29

- Finding Feature Information  29
- Restrictions for Control Plane Policing  29
- Information About Control Plane Policing  30
  - Benefits of Control Plane Policing  30
  - Control Plane Terms to Understand  30
  - Control Plane Policing Overview  30
- Supported Protocols  31
  - Input Rate-Limiting and Silent Mode Operation  36
- How to Use Control Plane Policing  36
  - Defining Control Plane Services  36
  - Verifying Control Plane Services  37
  - Configuring Control Plane Policing to Mitigate Denial-of-Service Attacks  38
- Configuration Examples for Control Plane Policing  41
  - Example: Configuring Control Plane Policing on Input Telnet Traffic  41
Class-Based Policing

- Finding Feature Information, on page 1
- Feature Overview, on page 1
- Prerequisites, on page 3
- Configuration Tasks, on page 3
- Monitoring and Maintaining Traffic Policing, on page 4
- Configuration Examples, on page 5
- Additional References, on page 6
- Feature Information for Class-Based Policing, on page 7

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Feature Overview

Class-Based Policing allows you to control the maximum rate of traffic transmitted or received on an interface. The Class-Based Policing feature is applied when you attach a traffic policy contain the Class-Based Policing configuration to an interface.

The Class-Based Policing feature performs the following functions:

- Limits the input or output transmission rate of a class of traffic based on user-defined criteria

- Marks packets by setting the ATM Cell Loss Priority (CLP) bit, Frame Relay Discard Eligibility (DE) bit, IP precedence value, IP differentiated services code point (DSCP) value, MPLS experimental value, and Quality of Service (QoS) group.
**Benefits**

**Bandwidth Management Through Rate Limiting**
Class-Based Policing allows you to control the maximum rate of traffic transmitted or received on an interface. Class-Based Policing is often configured on interfaces at the edge of a network to limit traffic into or out of the network. In most Class-Based Policing configurations, traffic that falls within the rate parameters is transmitted, whereas traffic that exceeds the parameters is dropped or transmitted with a different priority.

**Packet Marking**
Packet marking allows you to partition your network into multiple priority levels or classes of service (CoS). A packet is marked and these markings can be used to identify and classify traffic for downstream devices. In some cases, such as ATM Cell Loss Priority (CLP) marking or Frame Relay Discard Eligibility (DE) marking, the marking is used to classify traffic.

- Use Class-Based Policing to set the IP precedence or DSCP values for packets entering the network. Networking devices within your network can then use the adjusted IP precedence values to determine how the traffic should be treated. For example, the Weighted Random Early Detection (WRED) feature uses the IP precedence values to determine the probability that a packet will be dropped.

- Use Class-Based Policing to assign packets to a QoS group. The router uses the QoS group to determine how to prioritize packets within the router.

Traffic can be marked without using the Class-Based Policing feature. If you want to mark traffic but do not want to use Class-Based Policing, see the "Marking Network Traffic" module.

**Packet Prioritization for Frame Relay Frames**
The Class-Based Policing feature allows users to mark the Frame Relay DE bit of the Frame Relay frame. The Frame Relay DE bit is one bit and, therefore, can be set to either 0 or 1. In congested environments, frames with the DE bit set to 1 are discarded before frames with the DE bit set to 0.

**Packet Prioritization for ATM Cells**
The Class-Based Policing feature allows users to mark the ATM CLP bit in ATM cells. The ATM CLP bit is used to prioritize packets in ATM networks. The ATM CLP bit is one bit and, therefore, can be set to either 0 or 1. In congested environments, cells with the ATM CLP bit set to 1 are discarded before cells with the ATM CLP bit set to 0.

**Restrictions**

- To use the `set-clp-transmit` action available with this feature, the Enhanced ATM Port Adapter (PA-A3) is required. Therefore, the `set-clp-transmit` action is not supported on any platform that does not support the PA-A3 adapter. For more information, see the documentation for your specific device.

- On a Cisco ASR 920 Series router in egress, 1R2C means confirm-action transmit and exceed-action drop. By configuring exceed-action transmit on egress will drop those packets.

- On a Cisco ASR 920 Series router, Class-Based Policing can monitor Cisco Express Forwarding (CEF) switching paths only. In order to use the Class-Based Policing feature, Cisco Express Forwarding must be configured on both the interface receiving the packet and the interface sending the packet.
• On a Cisco ASR 920 Series router, Class-Based Policing cannot be applied to packets that originated from or are destined to a device.

• Class-Based Policing can be configured on an interface or a subinterface.

• As Policier actions and Table-Map configurations are not mutually exclusive, dynamic modifications of these parameters is not supported.

• Class-Based Policing is not supported on the following interfaces:
  • Fast EtherChannel
  • PRI
  • Any interface on a Cisco ASR 920 Series router that does not support Cisco Express Forwarding
  • Tunnel

---

**Note**

Class-Based Policing is supported on tunnels that are using the Cisco generic routing encapsulation (GRE) tunneling protocol.

---

**Prerequisites**

On a Cisco ASR 920 Series router, Cisco Express Forwarding (CEF) must be configured on the interface before Class-Based Policing can be used.

**Configuration Tasks**

**Configuring Traffic Policing**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Device(config-pmap-c)# `police bps burst-normal burst-max conform-action action exceed-action action violate-action action` | Specifies a maximum bandwidth usage by a traffic class. 

**Note**

The Class-Based Policing feature works with a token bucket mechanism. There are currently two types of token bucket algorithms: a single token bucket algorithm and a two token bucket algorithm. A single token bucket system is used when the `violate-action` option is not specified, and a two token bucket system is used when the `violate-action` option is specified. |
Verifying Traffic Policing

Use the `show policy-map interface` EXEC command to verify that the Class-Based Policing feature is configured on your interface. If the feature is configured on your interface, the `show policy-map interface` command output displays policing statistics:

```
Device# show policy-map interface
Ethernet1/7
  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
```

Troubleshooting Tips

- Check the interface type. Verify that your interface is not mentioned in the nonsupported interface description in the Restrictions, on page 2 section of this module.

- For input Class-Based Policing on a Cisco ASR 920 Series router, verify that CEF is configured on the interface where Class-Based Policing is configured.

- For output Class-Based Policing on a Cisco ASR 920 Series router, ensure that the incoming traffic is CEF-switched. Class-Based Policing cannot be used on the switching path unless CEF switching is enabled.

Monitoring and Maintaining Traffic Policing

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device# <code>show policy-map</code></td>
<td>Displays all configured policy maps.</td>
</tr>
<tr>
<td>Device# <code>show policy-map policy-map-name</code></td>
<td>Displays the user-specified policy map.</td>
</tr>
<tr>
<td>Device# <code>show policy-map interface</code></td>
<td>Displays statistics and configurations of all input and output policies that are attached to an interface.</td>
</tr>
<tr>
<td>Device# <code>show policy-map interface service instance</code></td>
<td>Displays the policy map information for a given service instance under a port channel.</td>
</tr>
</tbody>
</table>
Configuration Examples

Example Configuring a Service Policy that Includes Traffic Policing

In the following example, Class-Based Policing is configured with the average rate at 8000 bits per second, the normal burst size at 1000 bytes, and the excess burst size at 1000 bytes for all packets leaving Fast Ethernet interface 0/0.

class-map access-match
match access-group 1
exit
policy-map police-setting
class access-match
police 8000 1000 1000 conform-action transmit exceed-action set-qos-transmit 1 violate-action drop
exit
exit
service-policy output police-setting

The treatment of a series of packets leaving Fast Ethernet interface 0/0 depends on the size of the packet and the number of bytes remaining in the conform and exceed token buckets. The series of packets are policed based on the following rules:

• If the previous arrival of the packet was at T1 and the current arrival of the packet is at T, the bucket is updated with T - T1 worth of bits based on the token arrival rate. The refill tokens are placed in the conform bucket. If the tokens overflow the conform bucket, the overflow tokens are placed in the exceed bucket. The token arrival rate is calculated as follows:

(time between packets <which is equal to T - T1> * policer rate)/8 bytes

• If the number of bytes in the conform bucket B is greater than or equal to 0, the packet conforms and the conform action is taken on the packet. If the packet conforms, B bytes are removed from the conform bucket and the conform action is taken. The exceed bucket is unaffected in this scenario.

• If the number of bytes in the conform bucket B is less than 0, the excess token bucket is checked for bytes by the packet. If the number of bytes in the exceed bucket B is greater than or equal to 0, the exceed action is taken and B bytes are removed from the exceed token bucket. No bytes are removed from the conform bucket in this scenario.

• If the number bytes in the exceed bucket B is fewer than 0, the packet violates the rate and the violate action is taken. The action is complete for the packet.

In this example, the initial token buckets start full at 1000 bytes. If a 450-byte packet arrives, the packet conforms because enough bytes are available in the conform token bucket. The conform action (send) is taken by the packet and 450 bytes are removed from the conform token bucket (leaving 550 bytes).

If the next packet arrives 0.25 seconds later, 250 bytes are added to the conform token bucket

((0.25 * 8000)/8), leaving 800 bytes in the conform token bucket. If the next packet is 900 bytes, the packet does not conform because only 800 bytes are available in the conform token bucket.

The exceed token bucket, which starts full at 1000 bytes (as specified by the excess burst size) is then checked for available bytes. Because enough bytes are available in the exceed token bucket, the exceed action (set the
QoS transmit value of 1) is taken and 900 bytes are taken from the exceed bucket (leaving 100 bytes in the exceed token bucket.

If the next packet arrives 0.40 seconds later, 400 bytes are added to the token buckets ((.40 * 8000)/8). Therefore, the conform token bucket now has 1000 bytes (the maximum number of tokens available in the conform bucket) and 200 bytes overflow the conform token bucket (because it only 200 bytes were needed to fill the conform token bucket to capacity). These overflow bytes are placed in the exceed token bucket, giving the exceed token bucket 300 bytes.

If the arriving packet is 1000 bytes, the packet conforms because enough bytes are available in the conform token bucket. The conform action (transmit) is taken by the packet, and 1000 bytes are removed from the conform token bucket (leaving 0 bytes).

If the next packet arrives 0.20 seconds later, 200 bytes are added to the token bucket ((.20 * 8000)/8). Therefore, the conform bucket now has 200 bytes. If the arriving packet is 400 bytes, the packet does not conform because only 200 bytes are available in the conform bucket. Similarly, the packet does not exceed because only 300 bytes are available in the exceed bucket. Therefore, the packet violates and the violate action (drop) is taken.

Additional References

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>QoS commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples</td>
<td>Cisco IOS Quality of Service Solutions Command Reference</td>
</tr>
<tr>
<td>Modular Quality of Service (QoS) Command-Line Interface (CLI) (MQC), hierarchical policies, policy maps</td>
<td>&quot;Applying QoS Features Using the MQC&quot; module</td>
</tr>
<tr>
<td>Policing and shaping traffic</td>
<td>&quot;Policing and Shaping Overview&quot; module</td>
</tr>
</tbody>
</table>

Standards

<table>
<thead>
<tr>
<th>Standard</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.</td>
<td>--</td>
</tr>
</tbody>
</table>

MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS XE software releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>
RFCs

<table>
<thead>
<tr>
<th>RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.</td>
<td>--</td>
</tr>
</tbody>
</table>

Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.</td>
<td><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></td>
</tr>
</tbody>
</table>

Feature Information for Class-Based Policing

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to [www.cisco.com/go/cfn](http://www.cisco.com/go/cfn). An account on Cisco.com is not required.

**Table 1: Feature Information for Class-Based Policing**

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class-Based Policing</td>
<td>Cisco IOS XE Release 3.13.0S</td>
<td>This feature was introduced on the Cisco ASR 920 Series Aggregation Services Router (ASR-920-12CZ-A, ASR-920-12CZ-D, ASR-920-4SZ-A, ASR-920-4SZ-D).</td>
</tr>
</tbody>
</table>
Punt Policing and Monitoring

Punt policing protects the Route Processor (RP) from having to process noncritical traffic, which increases the CPU bandwidth available to critical traffic. Traffic is placed into different CPU queues based on various criteria. The Punt Policing and Monitoring feature allows you to police the punt rate on a per-queue basis.

• Finding Feature Information, on page 9
• Information About Punt Policing and Monitoring, on page 9
• How to Configure Punt Policing and Monitoring, on page 10
• Configuration Examples for Punt Policing and Monitoring, on page 14
• Additional References, on page 15
• Feature Information for Punt Policing and Monitoring, on page 16

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About Punt Policing and Monitoring

Overview of Punt Policing and Monitoring

Packets received on an interface are punted to the Router Processor (RP) for various reasons. Some examples of these various reasons include, unicast and multicast control plane traffic that are destined for a routing protocol process running on the RP, and IP packets that generate Internet Control Message Protocol (ICMP) exceptions such as a Time to live (TTL) expiration. The RP has a limited capacity to process the punted packets, and while some of them are critical for the router operation and should not be dropped, some can be dropped without impacting the router operation.

Punt policing frees the RP from having to process noncritical traffic. Traffic is placed in queues based on various criteria, and you can configure the maximum punt rate for each queue which allows you to configure the system so that packets are less likely to be dropped from queues that contain critical traffic.
Traffic on certain CPU queues could still be dropped, regardless of the configured punt rate, based on other criteria such as the queue priority, queue size, and traffic punt rate.

### How to Configure Punt Policing and Monitoring

#### Configuring Punt Policing

Traffic on a specific CPU queue may be dropped irrespective of the configured maximum punt rate, based on the queue priority, queue size, and the configured traffic punt rate.

**Perform this task to specify the maximum punt rate on the specified queue.**

**SUMMARY STEPS**

1. enable
2. configure terminal
3. platform qos-policer queue queue-id cir
4. end

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</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>Device# configure terminal</td>
</tr>
<tr>
<td><strong>Step 3</strong> platform qos-policer queue queue-id cir</td>
<td>Enables punt policing on a queue, and specifies the maximum punt rate on a per-queue basis.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# platform punt-policer queue 20 9000 10000</td>
</tr>
<tr>
<td><strong>Step 4</strong> end</td>
<td>(Optional) Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# end</td>
</tr>
</tbody>
</table>
Verifying Punt Policing

Verifying Queue-Based Punt Policing

Use the show platform software infrastructure punt statistics command to display punt police statistics:

```
Router# show platform software infrastructure punt statistics
UEA Punt Statistics

Global drops : 0

<table>
<thead>
<tr>
<th>Queue Name</th>
<th>Rx count</th>
<th>Drop count</th>
</tr>
</thead>
<tbody>
<tr>
<td>SW FORWARDING Q</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>ROUTING PROTOCOL Q</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>ICMP Q</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>HOST Q</td>
<td>57115</td>
<td>0</td>
</tr>
<tr>
<td>ACL LOGGING Q</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>STP Q</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>L2 PROTOCOL Q</td>
<td>6571</td>
<td>0</td>
</tr>
<tr>
<td>MCAST CONTROL Q</td>
<td>208839</td>
<td>0</td>
</tr>
<tr>
<td>BROADCAST Q</td>
<td>4</td>
<td>0</td>
</tr>
<tr>
<td>REP Q</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>CFM Q</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>CONTROL Q</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>IP MPLS TTL Q</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>DEFAULT MCAST Q</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>MCAST ROUTE DATA Q</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>MCAST MISMATCH Q</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>RPF FAIL Q</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>ROUTING THROTTLE Q</td>
<td>87</td>
<td>0</td>
</tr>
<tr>
<td>MCAST Q</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>MPLS OAM Q</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>IP MPLS MTU Q</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>PTP Q</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>LINUX ND Q</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>KEEPALIVE Q</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>ESMC Q</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>FPGA BFD Q</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>FPGA CCM Q</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>FPGA CFE Q</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>L2PT DUP Q</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
```

Verifying Punt Policing Statistics

Use the show platform hardware pp active infrastructure pi npd rx policer command to display the punt policing statistics for all queues:

```
<table>
<thead>
<tr>
<th>Ring</th>
<th>Queue Name</th>
<th>Punt rate</th>
<th>Burst rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>SW FORWARDING Q</td>
<td>500</td>
<td>1000</td>
</tr>
<tr>
<td>1</td>
<td>ROUTING PROTOCOL Q</td>
<td>500</td>
<td>1000</td>
</tr>
<tr>
<td>2</td>
<td>ICMP Q</td>
<td>500</td>
<td>1000</td>
</tr>
<tr>
<td>3</td>
<td>HOST Q</td>
<td>1000</td>
<td>2000</td>
</tr>
<tr>
<td>4</td>
<td>ACL LOGGING Q</td>
<td>500</td>
<td>1000</td>
</tr>
<tr>
<td>5</td>
<td>STP Q</td>
<td>3000</td>
<td>6000</td>
</tr>
<tr>
<td>6</td>
<td>L2 PROTOCOL Q</td>
<td>1000</td>
<td>2000</td>
</tr>
<tr>
<td>7</td>
<td>MCAST CONTROL Q</td>
<td>1000</td>
<td>2000</td>
</tr>
<tr>
<td>8</td>
<td>BROADCAST Q</td>
<td>1000</td>
<td>2000</td>
</tr>
<tr>
<td>9</td>
<td>REP Q</td>
<td>3000</td>
<td>6000</td>
</tr>
<tr>
<td>10</td>
<td>BGP LDP Q</td>
<td>3000</td>
<td>6000</td>
</tr>
</tbody>
</table>
```
### Punt Policing and Monitoring

Verifying Punt Policing Statistics

```
Router# show platform hardware pp active infrastructure pi npd rx policer
PUNT POLICER

Ring | Queue Name           | Punt rate | Burst rate |
-----+----------------------+-----------+------------
 0   | SW FORWARDING Q       | 500       | 1000       |
 1   | ROUTING PROTOCOL Q    | 500       | 1000       |
 2   | ICMP Q                | 500       | 1000       |
 3   | HOST Q                | 1000      | 2000       |
 4   | ACL LOGGING Q         | 500       | 1000       |
 5   | STP Q                 | 3000      | 6000       |
 6   | L2 PROTOCOL Q         | 1000      | 2000       |
 7   | MCAST CONTROL Q       | 1000      | 2000       |
 8   | BROADCAST Q           | 500       | 1000       |
 9   | REP Q                 | 3000      | 6000       |
10   | CFM Q                 | 3000      | 6000       |
11   | CONTROL Q             | 1000      | 2000       |
12   | IP MPLS TTL Q         | 1000      | 2000       |
13   | DEFAULT MCAST Q       | 500       | 1000       |
14   | MCAST ROUTE DATA Q    | 500       | 1000       |
15   | MCAST HIGH PRI Q      | 1000      | 2000       |
16   | RPF FAIL Q            | 500       | 1000       |
17   | ROUTING THROTTLE Q    | 500       | 1000       |
18   | MCAST Q               | 500       | 1000       |
19   | MPLS OAM Q            | 1000      | 2000       |
20   | IP MPLS MTU Q         | 500       | 1000       |
21   | PTP Q                 | 3000      | 6000       |
22   | LINUX ND Q            | 500       | 1000       |
23   | KEEPALIVE Q           | 1000      | 2000       |
24   | ESMC Q                | 3000      | 6000       |
25   | FPGA BFD Q            | 4000      | 8000       |
26   | FPGA CCM Q            | 4000      | 8000       |
27   | FPGA CFE Q            | 1000      | 2000       |
28   | L2PT DUP Q            | 4000      | 8000       |
29   | TDM CTRL Q            | 3000      | 6000       |
30   | ICMP UNREACHABLE Q    | 500       | 1000       |
31   | SSFPD Q               | 6000      | 12000      |

Router# show platform hardware pp active infrastructure pi npd rx policer
PUNT POLICER

Ring | Queue Name           | Punt rate | Burst rate |
-----+----------------------+-----------+------------
 0   | SW FORWARDING Q       | 500       | 1000       |
 1   | ROUTING PROTOCOL Q    | 500       | 1000       |
```

QoS: Policing and Shaping Configuration Guide (Cisco ASR 920 Series)
<table>
<thead>
<tr>
<th>#</th>
<th>Queue Name</th>
<th>Min Rate</th>
<th>Max Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>ICMP Q</td>
<td>500</td>
<td>1000</td>
</tr>
<tr>
<td>3</td>
<td>HOST Q</td>
<td>1000</td>
<td>2000</td>
</tr>
<tr>
<td>4</td>
<td>ACL LOGGING Q</td>
<td>500</td>
<td>1000</td>
</tr>
<tr>
<td>5</td>
<td>STP Q</td>
<td>3000</td>
<td>6000</td>
</tr>
<tr>
<td>6</td>
<td>L2 PROTOCOL Q</td>
<td>1000</td>
<td>2000</td>
</tr>
<tr>
<td>7</td>
<td>MCAST CONTROL Q</td>
<td>1000</td>
<td>2000</td>
</tr>
<tr>
<td>8</td>
<td>BROADCAST Q</td>
<td>500</td>
<td>1000</td>
</tr>
<tr>
<td>9</td>
<td>REP Q</td>
<td>3000</td>
<td>6000</td>
</tr>
<tr>
<td>10</td>
<td>CFM Q</td>
<td>3000</td>
<td>6000</td>
</tr>
<tr>
<td>11</td>
<td>CONTROL Q</td>
<td>1000</td>
<td>2000</td>
</tr>
<tr>
<td>12</td>
<td>IP MPLS TTL Q</td>
<td>1000</td>
<td>2000</td>
</tr>
<tr>
<td>13</td>
<td>DEFAULT MCAST Q</td>
<td>500</td>
<td>1000</td>
</tr>
<tr>
<td>14</td>
<td>MCAST ROUTE DATA Q</td>
<td>500</td>
<td>1000</td>
</tr>
<tr>
<td>15</td>
<td>MCAST MISMATCH Q</td>
<td>500</td>
<td>1000</td>
</tr>
<tr>
<td>16</td>
<td>RPF FAIL Q</td>
<td>500</td>
<td>1000</td>
</tr>
<tr>
<td>17</td>
<td>ROUTING THROTTLE Q</td>
<td>500</td>
<td>1000</td>
</tr>
<tr>
<td>18</td>
<td>MCAST Q</td>
<td>500</td>
<td>1000</td>
</tr>
<tr>
<td>19</td>
<td>MPLS OAM Q</td>
<td>1000</td>
<td>2000</td>
</tr>
<tr>
<td>20</td>
<td>IP MPLS MTU Q</td>
<td>9000</td>
<td>10000</td>
</tr>
<tr>
<td>21</td>
<td>PTP Q</td>
<td>3000</td>
<td>6000</td>
</tr>
<tr>
<td>22</td>
<td>LINUX ND Q</td>
<td>500</td>
<td>1000</td>
</tr>
<tr>
<td>23</td>
<td>KEEPALIVE Q</td>
<td>1000</td>
<td>2000</td>
</tr>
<tr>
<td>24</td>
<td>ESMC Q</td>
<td>3000</td>
<td>6000</td>
</tr>
<tr>
<td>25</td>
<td>FPGA BFD Q</td>
<td>4000</td>
<td>8000</td>
</tr>
<tr>
<td>26</td>
<td>FPGA CCM Q</td>
<td>2000</td>
<td>4000</td>
</tr>
<tr>
<td>27</td>
<td>FPGA CFE Q</td>
<td>3000</td>
<td>6000</td>
</tr>
<tr>
<td>28</td>
<td>L2PT DUP Q</td>
<td>4000</td>
<td>8000</td>
</tr>
</tbody>
</table>

Use the `show platform hardware pp active feature qos policer cpu all 1` command to clear the statistics of all the CPU queues.

Use the `show platform hardware pp active feature qos policer cpu all 0` command to clear the statistics of a particular CPU queue.

```
########## Stats for CPU queue 0 ##########
Internal Qnum: 1     Queue Name: SW FORWARDING Q
Policer conform: 0 (packets) 0 (bytes)
Policer exceed: 0 (packets) 0 (bytes)
RM Drops: 0 (packets) 0 (bytes)
Policer commit rate is: 1000000, Policer burst commit is 100000

########## Stats for CPU queue 1 ##########
Internal Qnum: 2     Queue Name: ROUTING PROTOCOL Q
Policer conform: 0 (packets) 0 (bytes)
Policer exceed: 0 (packets) 0 (bytes)
RM Drops: 0 (packets) 0 (bytes)
Policer commit rate is: 1000000, Policer burst commit is 100000

########## Stats for CPU queue 30 ##########
Internal Qnum: 31    Queue Name: ICMP UNREACHABLE Q
Policer conform: 0 (packets) 0 (bytes)
Policer exceed: 0 (packets) 0 (bytes)
RM Drops: 0 (packets) 0 (bytes)
Policer commit rate is: 1000000, Policer burst commit is 100000

########## Stats for CPU queue 31 ##########
Internal Qnum: 32    Queue Name: SSFPD Q
Policer conform: 0 (packets) 0 (bytes)
Policer exceed: 0 (packets) 0 (bytes)
RM Drops: 0 (packets) 0 (bytes)
Policer commit rate is: 1000000, Policer burst commit is 100000
```
Use show platform hardware pp active feature qos policer cpu 3 0 to display the queue specific statistics.

```
############## Stats for CPU queue 3 ##############
Internal Qnum: 4 Queue Name: HOST Q
Policer conform: 0 (packets) 0 (bytes)
Policer exceed: 0 (packets) 0 (bytes)
RM Drops: 0 (packets) 0 (bytes)
Policer commit rate is: 12000000, Policer burst commit is 3000000
```

Use the show platform hardware pp active feature qos policer cpu all 0 to display the output after adding the drop cause. Following commands are applicable only for RSP3 module:

```
############## Stats for CPU queue 0 ##############
Internal Qnum: 8000CPU
Port num: 0
Policer conform: 0 (packets) 0 (bytes)
Policer exceed: 0 (packets) 0 (bytes)
Policer commit rate is: 500000 bps, Policer burst commit is 16000 bytes

############## Stats for CPU queue 1 ##############
Internal Qnum: 8008CPU
Port num: 0
Policer conform: 0 (packets) 0 (bytes)
Policer exceed: 0 (packets) 0 (bytes)
Policer commit rate is: 1000000 bps, Policer burst commit is 100000 bytes

############## Stats for CPU queue 2 ##############
Internal Qnum: 8016CPU
Port num: 0
Policer conform: 0 (packets) 0 (bytes)
Policer exceed: 0 (packets) 0 (bytes)
Policer commit rate is: 1000000 bps, Policer burst commit is 100000 bytes
```

When a packet is dropped by per interface punt policer, a log including the source interface is displayed as follows (the log shows one log in 30 seconds):

```
*Jun 6 08:25:35.893: %IOSXE-5-PLATFORM: F0: cpp_cp: QFP:0.0
Thread:046 TS:0000000040085958264 %PUNT_INJECT-5-DROP_PUNT_INTF:
punt interface policer drop packet from GigabitEthernet2/3/1.726
```

**Configuration Examples for Punt Policing and Monitoring**

**Example: Configuring Punt Policing**

The following example shows how to enable punt-policing:

```
Router# enable
Router# configure terminal
Router(config)# platform qos-policer queue 3 64000
```
# Additional References

## Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>QoS commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples</td>
<td><em>Cisco IOS Quality of Service Solutions Command Reference</em></td>
</tr>
<tr>
<td>Traffic marking</td>
<td>“Marking Network Traffic” module</td>
</tr>
<tr>
<td>Traffic policing</td>
<td>“Traffic Policing” module</td>
</tr>
<tr>
<td>Traffic policing and shaping concepts and overview information</td>
<td>“Policing and Shaping Overview” module</td>
</tr>
<tr>
<td>Modular quality of service command-line interface (MQC)</td>
<td>“Applying QoS Features Using the MQC” module</td>
</tr>
</tbody>
</table>

## Standards

<table>
<thead>
<tr>
<th>Standard</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>—</td>
</tr>
</tbody>
</table>

## MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS XE Software releases, and feature sets, use Cisco MIB Locator found at the following URL:</td>
</tr>
<tr>
<td></td>
<td><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

## RFCs

<table>
<thead>
<tr>
<th>RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>—</td>
</tr>
</tbody>
</table>
Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.</td>
<td><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></td>
</tr>
</tbody>
</table>

Feature Information for Punt Policing and Monitoring

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to [www.cisco.com/go/cfn](http://www.cisco.com/go/cfn). An account on Cisco.com is not required.

**Table 2: Feature Information for Punt Policing and Monitoring**

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Feature Information for Punt Policing and Monitoring</td>
<td>Cisco IOS XE Release 3.13.0S</td>
<td>This feature was introduced on the Cisco ASR 920 Series Aggregation Services Router (ASR-920-12CZ-A, ASR-920-12CZ-D, ASR-920-4SZ-A, ASR-920-4SZ-D).</td>
</tr>
</tbody>
</table>
Port-Shaper and LLQ in the Presence of EFPs

The Port-Shaper and LLQ in the Presence of EFPs feature allows network designers to configure port and class policies on ports that contain Ethernet Flow Points (EFPs). These policies support Low Latency Queueing (LLQ) and traffic prioritization across the EFPs.

- Finding Feature Information, on page 17
- Restrictions for Port-Shaper and LLQ in the Presence of EFPs, on page 17
- Information About Port-Shaper and LLQ in the Presence of EFPs, on page 18
- How to Configure Port-Shaper and LLQ in the Presence of EFPs, on page 18
- Configuration Examples for Port-Shaper and LLQ in the Presence of EFPs, on page 24
- Additional References, on page 26
- Feature Information for Port-Shaper and LLQ in the Presence of EFPs, on page 27

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for Port-Shaper and LLQ in the Presence of EFPs

- If you configure port level shaper with the policy applied at EFP level then port shaper does not work. However, 3 level HQoS policy with port and logical shaper can be applied at the EFP level. Logical shaper configured at logical level does work but port shaper does not work.

- If you configure a class-based policy on the port, then you cannot configure service-policies on Ethernet Flow Points (EFPs).

- Attaching a service policy to the BDI is not supported.

- ACL based shaping policy-map cannot be applied to the EFP and/or egress interface.

- Usage of bandwidth remaining percentage (BRP) in the absence of priority class, allocates the available bandwidth in an iterative way. For example, the bandwidth is allocated for the first BRP class as per the
Percentage of share configured in the respective class-map and the remaining bandwidth is iteratively allocated to all other BRP classes until the bandwidth is exhausted.

Information About Port-Shaper and LLQ in the Presence of EFPs

Ethernet Flow Points and LLQ

An Ethernet Flow Point (EFP) is a forwarding decision point in the provider edge (PE) router, which gives network designers flexibility to make many Layer 2 flow decisions within the interface. Many EFPs can be configured on a single physical port. (The number varies from one device to another.) EFPs are the logical demarcation points of an Ethernet virtual connection (EVC) on an interface. An EVC that uses two or more User-Network Interfaces (UNIs) requires an EFP on the associated ingress and egress interfaces of every device that the EVC passes through.

The Egress HQoS with Port Level Shaping feature allows network designers to configure port and class policies on ports that contain EFPs. These policies support Low Latency Queueing (LLQ) and traffic prioritization across the EFPs.

For information on how to configure LLQ, see the QoS Congestion Management Configuration Guide.

How to Configure Port-Shaper and LLQ in the Presence of EFPs

To configure the Port-Shaper and LLQ in the Presence of EFPs feature, you first create either a hierarchical or flat policy map that supports Low Latency Queueing (LLQ), which you then attach to an EFP interface.

Configuring Hierarchical Policy Maps

To configure hierarchical policy maps, you create child policies which you then attach to a parent policy. The parent policy is then attached to an interface.

SUMMARY STEPS

1. enable
2. configure terminal
3. policy-map policy-map-name
4. class class-map-name
5. set cos value
6. bandwidth percent percent
7. exit
8. class class-map-name
9. bandwidth percent percent
10. exit
11. policy-map policy-map-name
12. class class-default
13. service-policy policy-map-name
### 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>Purpose</strong></td>
</tr>
<tr>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>- Enter your password if prompted.</td>
</tr>
<tr>
<td><code>Device&gt; enable</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td><code>configure</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><code>terminal</code></td>
<td></td>
</tr>
<tr>
<td><code>Device# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td><code>policy-map policy-map-name</code></td>
<td>Creates or modifies the child policy and enters QoS policy-map configuration mode.</td>
</tr>
<tr>
<td><code>Device(config)# policy-map child-llq</code></td>
<td>- child-llq is the name of the child policy map.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td><code>class class-map-name</code></td>
<td>Assigns the traffic class you specify to the policy map and enters QoS policy-map class configuration mode.</td>
</tr>
<tr>
<td><code>Device(config-pmap)# class precedenc-1</code></td>
<td>- precedenc-1 is the name of a previously configured class map and is the traffic class for which you want to define QoS actions.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td><code>set cos value</code></td>
<td>(Optional) Sets the Layer 2 class of service (CoS) value of an outgoing packet.</td>
</tr>
<tr>
<td><code>Device(config-pmap-c)# set cos 5</code></td>
<td>- The value is a specific IEEE 802.1Q CoS value from 0 to 7.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td><code>bandwidth percent percent</code></td>
<td>(Optional) Specifies a bandwidth percent for class-level queues to be used during congestion to determine the amount of excess bandwidth (unused by priority traffic) to allocate to nonpriority queues.</td>
</tr>
<tr>
<td><code>Device(config-pmap-c)# bandwidth percent 20</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td><code>exit</code></td>
<td>Exits QoS policy-map class configuration mode.</td>
</tr>
<tr>
<td><code>Device(config-pmap-c)# exit</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td><code>class class-map-name</code></td>
<td>Assigns the traffic class you specify to the policy map and enters QoS policy-map class configuration mode.</td>
</tr>
<tr>
<td><code>Device(config-pmap)# class precedenc-2</code></td>
<td>- precedenc-2 is the name of a previously configured class map and is the traffic class for which you want to define QoS actions.</td>
</tr>
</tbody>
</table>

**Note**: match on qos-group is supported on the Cisco RSP3 Module.
### Configuring an LLQ Policy Map

**SUMMARY STEPS**

1. **enable**
2. **configure terminal**
3. **policy-map policy-map-name**
4. **class class-map-name**
5. **priority**
6. **exit**
7. **class class-map-name**
8. **shape average value**
9. **exit**
10. **class class-map-name**
11. **bandwidth percent**
12. **exit**

---

#### Command or Action | Purpose
--- | ---
**Step 9** | bandwidth percent *percent*
**Example:**
Device(config-pmap-c)# bandwidth percent 80

(Optional) Specifies a bandwidth percent for class-level queues to be used during congestion to determine the amount of excess bandwidth (unused by priority traffic) to allocate to nonpriority queues.

**Step 10** | exit
**Example:**
Device(config-pmap-c)# exit

Exits QoS policy-map class configuration mode.

**Step 11** | policy-map *policy-map-name*
**Example:**
Device(config-pmap-c)# policy-map parent-llq

Creates or modifies the parent policy.
- parent-llq is the name of the parent policy map.

**Step 12** | class class-default
**Example:**
Device(config-pmap-c)# class class-default

Configures or modifies the parent class-default class and enters QoS policy-map class configuration mode.
- You can configure only the class-default class in a parent policy. Do not configure any other traffic class.

**Step 13** | service-policy *policy-map-name*
**Example:**
Device(config-pmap-c)# service-policy child-llq

Applies the child policy to the parent class-default class.
- child-llq is the name of the child policy map configured in step 1.
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enables privileged EXEC mode.</td>
<td><em>Enter your password if prompted.</em></td>
</tr>
<tr>
<td>enable</td>
<td></td>
<td><em>Device</em> <code>&gt; enable</code></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enters global configuration mode.</td>
<td><em>Device</em> <code># configure terminal</code></td>
</tr>
<tr>
<td>configure terminal</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Creates a policy and enters QoS policy-map configuration mode.</td>
<td><em>Device</em> <code>(config)# policy-map llq-flat</code></td>
</tr>
<tr>
<td>policy-map policy-map-name</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Assigns the traffic class you specify to the policy map and enters policy-map class configuration mode.</td>
<td><em>Device</em> <code>(config-pmap)# class dscp-af1</code></td>
</tr>
<tr>
<td>class class-map-name</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Configures LLQ, providing strict priority queueing (PQ) for class-based weighted fair queueing (CBWFQ).</td>
<td><em>Device</em> <code>config-pmap-c)# priority</code></td>
</tr>
<tr>
<td>priority</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Exits QoS policy-map class configuration mode.</td>
<td><em>Device</em> <code>config-pmap-c)# exit</code></td>
</tr>
<tr>
<td>exit</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>Assigns the traffic class you specify to the policy map and enters QoS policy-map class configuration mode.</td>
<td><em>Device</em> <code>config-pmap)# class dscp-af2</code></td>
</tr>
<tr>
<td>class class-map-name</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>Configures a shape entity with a Committed Information Rate of 200 Mb/s.</td>
<td><em>Device</em> <code>config-pmap-c)# shape average 200000000</code></td>
</tr>
<tr>
<td>shape average value</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td>Exits QoS policy-map class configuration mode.</td>
<td><em>Device</em> <code>config-pmap-c)# exit</code></td>
</tr>
<tr>
<td>exit</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Configuring Port Level Shaping on the Main Interface with Ethernet Flow Points

To configure port level shaping on the main interface with EFPS, first you enable the autonegotiation protocol on the interface, then you attach a policy map to the interface and finally you configure the Ethernet service instance.

#### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `interface type number`
4. `no ip address`
5. `negotiation auto`
6. `service-policy output policy-map-name`
7. `service instance id ethernet`
8. `encapsulation dot1q vlan-id`
9. `bridge-domain bridge-domain-id`
10. `exit`
11. `service instance id ethernet`
12. `encapsulation dot1q vlan-id`
13. `bridge-domain bridge-domain-id`
14. `exit`
15. `end`

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
</tbody>
</table>

---

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Command or Action</th>
</tr>
</thead>
</table>
| **Assigns the traffic class you specify to the policy map and enters QoS policy-map class configuration mode.** | `Step 10` class class-map-name  
Example:  
Device(config-pmap)# class dscp-af3 |
| *(Optional) Specifies a bandwidth percent for class-level queues to be used during congestion to determine the amount of excess bandwidth (unused by priority traffic) to allocate to non-priority queues.* | `Step 11` bandwidth percent  
Example:  
Device(config-pmap-c)# bandwidth 4000000 |
| **Exits QoS policy-map class configuration mode.** | `Step 12` exit  
Example:  
Device(config-pmap-c)# exit |
### Purpose

**Command or Action**

**Example:**

Device> enable

- Enter your password if prompted.

**Step 2**

configure terminal

**Example:**

Device# configure terminal

- Enters global configuration mode.

**Step 3**

interface **type number**

**Example:**

Device(config)# interface GigabitEthernet 0/0/1

- Configures an interface type and enters interface configuration mode.

- Enter the interface type number.

**Step 4**

no ip address

**Example:**

Device(config-if)# no ip address

- Disables IP routing on the interface.

**Step 5**

negotiation auto

**Example:**

Device(config-if)# negotiation auto

- Enables the autonegotiation protocol to configure the speed, duplex, and automatic flow control of the Gigabit Ethernet interface.

**Step 6**

service-policy output **policy-map-name**

**Example:**

Device(config-if)# service-policy output parent-llq

- Specifies the name of the policy map to be attached to the input or output direction of the interface.

  - You can enter the name of a hierarchical or a flat policy map.

**Step 7**

service instance **id ethernet**

**Example:**

Device(config-if)# service instance 1 ethernet

- Configures an Ethernet service instance on an interface and enters service instance configuration mode.

**Step 8**

encapsulation dot1q **vlan-id**

**Example:**

Device(config-if-srv)# encapsulation dot1q 100

- Defines the matching criteria to map 802.1Q frames' ingress on an interface to the service instance.

**Step 9**

bridge-domain **bridge-domain-id**

**Example:**

Device(config-if-srv)# bridge-domain 100

- Binds the bridge domain to the service instance.

**Step 10**

exit

**Example:**

- Exits service instance configuration mode.
**Purpose**

Device(config-if-serv)# exit

**Command or Action**

Device(config-if-serv)# exit

**Step 11**

**service instance id ethernet**

*Example:*

Device(config-if)# service instance 2 ethernet

**Purpose**

Configures an Ethernet service instance on an interface and enters service instance configuration mode.

**Step 12**

**encapsulation dot1q vlan-id**

*Example:*

Device(config-if-srv)# encapsulation dot1q 101

**Purpose**

Defines the matching criteria to map 802.1Q frames' ingress on an interface to the service instance.

**Step 13**

**bridge-domain bridge-domain-id**

*Example:*

Device(config-if-srv)# bridge-domain 101

**Purpose**

Binds the bridge domain to the service instance.

**Step 14**

**exit**

*Example:*

Device(config-if-srv)# exit

**Purpose**

Exits QoS policy-map class configuration mode.

**Step 15**

**end**

*Example:*

Device(config-if)# end

**Purpose**

(Optional) Exits interface configuration mode.

---

**Configuration Examples for Port-Shaper and LLQ in the Presence of EFPs**

**Example: Configuring Hierarchical QoS Port Level Shaping on the Main Interface with EFPs**

The following example shows how to configure hierarchical QoS port level shaping on a main physical interface to support traffic prioritization and Low Level Queueing across all EFPs configured on the interface:

```
policy-map parent-llq
  class class-default
    service-policy child-llq

policy-map child-llq
  class precedent-1
    set cos 5
```
Example: Configuring Port Level Shaping on the Main Interface with EFPs

The following example shows how to configure port level shaping on a main physical interface to support traffic prioritization and Low Level Queueing across all Ethernet Flow Points (EFPs) configured on the interface:

```
policy-map llq_flat
class dscp-af1
  priority
class dscp-af2
  shape average 200000000
class dscp-af3
  bandwidth 400000

interface GigabitEthernet 0/0/1
  no ip address
  negotiation auto
  service-policy output llq_flat
  service instance 1 ethernet
    encapsulation dot1q 100
    bridge-domain 100
  !
  service instance 2 ethernet
    encapsulation dot1q 101
    bridge-domain 101
```
## Additional References

### Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS commands</td>
<td><em>Cisco IOS Master Commands List, All Releases</em></td>
<td></td>
</tr>
<tr>
<td>QoS commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples</td>
<td><em>Cisco IOS QoS Command Reference</em></td>
<td></td>
</tr>
<tr>
<td>Policing and shaping</td>
<td>&quot;Policing and Shaping Overview&quot; module</td>
<td></td>
</tr>
<tr>
<td>Class maps</td>
<td>&quot;Applying QoS Features Using the MQC&quot; module</td>
<td></td>
</tr>
<tr>
<td>Policy maps</td>
<td>&quot;Applying QoS Features Using the MQC&quot; module</td>
<td></td>
</tr>
<tr>
<td>Low Latency Queueing</td>
<td><em>QoS Congestion Management Configuration Guide</em></td>
<td></td>
</tr>
</tbody>
</table>

### Standards and RFCs

<table>
<thead>
<tr>
<th>Standard</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified standards are supported, and support for existing standards has not been modified.</td>
<td>--</td>
</tr>
</tbody>
</table>

### MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified MIBs are supported, and support for existing MIBs has not been modified.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS XE software releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

### Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.</td>
<td><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></td>
</tr>
</tbody>
</table>
Feature Information for Port-Shaper and LLQ in the Presence of EFPs

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 3: Feature Information for Port-Shaper and LLQ in the Presence of EFPs

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port-Shaper and LLQ in the Presence of EFPs</td>
<td>Cisco IOS XE Release 3.13.0S</td>
<td>This feature was introduced on the Cisco ASR 920 Series Aggregation Services Router (ASR-920-12CZ-A, ASR-920-12CZ-D, ASR-920-4SZ-A, ASR-920-4SZ-D).</td>
</tr>
</tbody>
</table>
Feature Information for Port-Shaper and LLQ in the Presence of EFPs
CHAPTER 4

Control Plane Policing

The Control Plane Policing feature allows you to configure a quality of service (QoS) filter that manages the traffic flow of control plane packets to protect the control plane of routers and switches against reconnaissance and denial-of-service (DoS) attacks. In this way, the control plane (CP) can help maintain packet forwarding and protocol states despite an attack or heavy traffic load on the router or switch.

- Finding Feature Information, on page 29
- Restrictions for Control Plane Policing, on page 29
- Information About Control Plane Policing, on page 30
- How to Use Control Plane Policing, on page 36
- Configuration Examples for Control Plane Policing, on page 41
- Additional References, on page 41
- Feature Information for Control Plane Policing, on page 42

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for Control Plane Policing

Input Rate-Limiting Support

Input rate-limiting is performed in silent (packet discard) mode. Silent mode enables a router to silently discard packets using policy maps applied to input control plane traffic with the service-policy input command. For more information, see the “Input Rate-Limiting and Silent Mode Operation” section.
MQC Restrictions
The Control Plane Policing feature requires the Modular QoS CLI (MQC) to configure packet classification and traffic policing. All restrictions that apply when you use the MQC to configure traffic policing also apply when you configure control plane policing.

Match Criteria Support
Only the extended IP access control lists (ACLs) classification (match) criteria is supported.

Information About Control Plane Policing

Benefits of Control Plane Policing
Configuring the Control Plane Policing feature on your Cisco router or switch provides the following benefits:

- Protection against DoS attacks at infrastructure routers and switches
- QoS control for packets that are destined to the control plane of Cisco routers or switches
- Ease of configuration for control plane policies
- Better platform reliability and availability

Control Plane Terms to Understand
On the router, the following terms are used for the Control Plane Policing feature:

- Control plane—A collection of processes that run at the process level on the Route Processor (RP). These processes collectively provide high-level control for most Cisco IOS XE functions. The traffic sent to or sent by the control plane is called control traffic.
- Forwarding plane—A device that is responsible for high-speed forwarding of IP packets. Its logic is kept simple so that it can be implemented by hardware to do fast packet-forwarding. It punts packets that require complex processing (for example, packets with IP options) to the RP for the control plane to process them.

Control Plane Policing Overview
To protect the control plane on a router from DoS attacks and to provide fine-control over the traffic to the control plane, the Control Plane Policing feature treats the control plane as a separate entity with its own interface for ingress (input) and egress (output) traffic. This interface is called the punt/inject interface, and it is similar to a physical interface on the router. Along this interface, packets are punted from the forwarding plane to the RP (in the input direction) and injected from the RP to the forwarding plane (in the output direction). A set of quality of service (QoS) rules can be applied on this interface (in the input direction) in order to achieve CoPP.

These QoS rules are applied only after the packet has been determined to have the control plane as its destination. You can configure a service policy (QoS policy map) to prevent unwanted packets from progressing
after a specified rate limit has been reached; for example, a system administrator can limit all TCP/TELNET packets that are destined for the control plane.

Figure 1: Abstract Illustration of a Router with a Single RP and Forwarding Plane

The figure above provides an abstract illustration of the router with a single RP and forwarding plane. Packets destined to the control plane come in through the carrier card and then go through the forwarding plane before being punted to the RP. When an input QoS policy map is configured on the control plane, the forwarding plane performs the QoS action (for example, a transmit or drop action) before puntng packets to the RP in order to achieve the best protection of the control plane in the RP.

### Note

As shown in “Control Plane Policing Overview” section, the control plane interface is directly connected to the RP, so all traffic through the control plane interface to or from the control-plane is not subject to the CoPP function performed by the forwarding plane.

### Supported Protocols

The following table lists the protocols supported on Control Plane Policing feature.

<table>
<thead>
<tr>
<th>Supported Protocols</th>
<th>Criteria</th>
<th>Match</th>
<th>Queue#</th>
</tr>
</thead>
<tbody>
<tr>
<td>TFTP - Trivial FTP</td>
<td>IP/Port Match</td>
<td>permit udp 64.202.160.0 0.0.1.255 eq 69 any</td>
<td>NQ_CPU_HOST_Q</td>
</tr>
<tr>
<td></td>
<td></td>
<td>permit udp 64.202.160.0 0.0.1.255 any eq 69</td>
<td></td>
</tr>
<tr>
<td>TELNET</td>
<td>IP/Port Match</td>
<td>permit tcp 169.223.252.0 0.0.3.255 host 169.223.253.1 eq telnet</td>
<td>NQ_CPU_CONTROL_Q</td>
</tr>
<tr>
<td></td>
<td></td>
<td>permit tcp 169.223.252.0 0.0.3.255 eq telnet host 169.223.253.1</td>
<td></td>
</tr>
<tr>
<td>Supported Protocols</td>
<td>Criteria</td>
<td>Match</td>
<td>Queue#</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>------------</td>
<td>-----------------------------------------------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>NTP - Network Time Protocol</td>
<td>IP/Port Match</td>
<td>permit udp 169.223.252.0 0.0.3.255 host 169.223.253.1 eq ntp permit udp 169.223.252.0 0.0.3.255 eq ntp host 169.223.253.1</td>
<td>NQ_CPU_HOST_Q</td>
</tr>
<tr>
<td>FTP - File Transfer Protocol</td>
<td>IP/Port Match</td>
<td>permit tcp host &lt;FTP server&gt; eq ftp &lt;loopback block&gt; permit tcp host &lt;FTP server&gt; &lt;loopback block&gt; eq ftp</td>
<td>NQ_CPU_HOST_Q</td>
</tr>
<tr>
<td>SNMP - Simple Network Management Protocol</td>
<td>IP/Port Match</td>
<td>permit udp 169.223.252.0 0.0.3.255 host 169.223.253.1 eq snmp permit udp 169.223.252.0 0.0.3.255 eq snmp host 169.223.253.1</td>
<td>NQ_CPU_HOST_Q</td>
</tr>
<tr>
<td>TACACS - Terminal Access Controller</td>
<td>IP/Port Match</td>
<td>permit tcp 169.223.252.0 0.0.3.255 host 169.223.253.1 eq tacacs permit tcp 169.223.252.0 0.0.3.255 eq tacacs host 169.223.253.1 permit udp 169.223.252.0 0.0.3.255 host 169.223.253.1 eq tacacs permit udp 169.223.252.0 0.0.3.255 eq tacacs host 169.223.253.1</td>
<td>NQ_CPU_HOST_Q</td>
</tr>
<tr>
<td>FTP-DATA</td>
<td>IP/Port Match</td>
<td>permit tcp any any eq 20 permit tcp any eq 20 any permit udp any any eq 20 any permit udp any eq 20 any</td>
<td>NQ_CPU_HOST_Q</td>
</tr>
<tr>
<td>HTTP - Hypertext Transfer Protocol</td>
<td>IP/Port Match</td>
<td>permit tcp any any eq www permit tcp any eq www any</td>
<td>NQ_CPU_HOST_Q</td>
</tr>
<tr>
<td>Supported Protocols</td>
<td>Criteria</td>
<td>Match</td>
<td>Queue#</td>
</tr>
<tr>
<td>----------------------------------------------------------</td>
<td>-------------------------</td>
<td>----------------------------------------------------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>WCCP - Web Cache Communication Protocol</td>
<td>IP/Port Match</td>
<td>IP access list</td>
<td>NQ_CPU_HOST_Q</td>
</tr>
<tr>
<td></td>
<td></td>
<td>copp-system-acl-wccp</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>10 permit udp any eq 2048 any eq 2048</td>
<td></td>
</tr>
<tr>
<td>BGP - Border Gateway Protocol</td>
<td>IP/Port Match</td>
<td>permit tcp 169.223.252.0 0.0.3.255 host 169.223.253.1 eq bgp</td>
<td>NQ_CPU_CFQ_Q</td>
</tr>
<tr>
<td></td>
<td></td>
<td>permit tcp 169.223.252.0 0.0.3.255 eq bgp host 169.223.253.1</td>
<td></td>
</tr>
<tr>
<td>SSH - Secure Shell</td>
<td>IP/Port Match</td>
<td>permit udp [remote vty mgmt subnet] 0.0.0.255 any eq 22</td>
<td>NQ_CPU_HOST_Q</td>
</tr>
<tr>
<td></td>
<td></td>
<td>permit udp [remote vty mgmt subnet] 0.0.0.255 eq 22 any</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>permit tcp [remote vty mgmt subnet] 0.0.0.255 any eq 22</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>permit tcp [remote vty mgmt subnet] 0.0.0.255 eq 22 any</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Protocol Match</td>
<td>access-list 110 permit icmp any 169.223.253.1</td>
<td>NQ_CPU_HOST_Q</td>
</tr>
<tr>
<td>ICMP - Internet Control Message Protocol</td>
<td>IP/Port Match</td>
<td>permit udp any host x.x.x.x eq isakmp</td>
<td>NQ_CPU_HOST_Q</td>
</tr>
<tr>
<td></td>
<td></td>
<td>permit udp any eq isakmp host x.x.x.x</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>permit udp any host x.x.x.x eq non500-isakmp</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>permit udp any eq non500-isakmp host x.x.x.x</td>
<td></td>
</tr>
<tr>
<td>SAA - Service Assurance Agent</td>
<td>IP/Port Match</td>
<td>permit icmp host 10.2.2.4 host 10.1.1.1</td>
<td>NQ_CPU_HOST_Q</td>
</tr>
<tr>
<td>Supported Protocols</td>
<td>Criteria</td>
<td>Match</td>
<td>Queue#</td>
</tr>
<tr>
<td>---------------------------------------------------------</td>
<td>----------------</td>
<td>----------------------------------------------------------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>DHCP - Dynamic Host Configuration Protocol</td>
<td>IP/Port Match</td>
<td>permit udp host 0.0.0.0 host 255.255.255.255 eq bootps</td>
<td>NQ_CPU_HOST_Q</td>
</tr>
<tr>
<td></td>
<td></td>
<td>permit udp any eq bootps any eq bootps</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>permit udp host 0.0.0.0 host 255.255.255.255 eq bootpc</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>permit udp any eq bootpc any eq bootpc</td>
<td></td>
</tr>
<tr>
<td>DNS - Domain Name System</td>
<td>IP/Port Match</td>
<td>permit udp host <code>&lt;DNS server&gt;</code> eq domain any</td>
<td>NQ_CPU_HOST_Q</td>
</tr>
<tr>
<td></td>
<td></td>
<td>permit udp host <code>&lt;DNS server&gt;</code> any eq domain</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>permit tcp host <code>&lt;DNS server&gt;</code> eq domain any</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>permit tcp host <code>&lt;DNS server&gt;</code> any eq domain</td>
<td></td>
</tr>
<tr>
<td>DLSw - Data-Link Switching</td>
<td>IP/Port Match</td>
<td>permit any any eq 2065</td>
<td>NQ_CPU_HOST_Q</td>
</tr>
<tr>
<td></td>
<td></td>
<td>permit any eq 2065</td>
<td></td>
</tr>
<tr>
<td>LDP - Label Distribution Protocol</td>
<td>IP/Port Match</td>
<td>permit tcp any any eq 646</td>
<td>NQ_CPU_CFM_Q</td>
</tr>
<tr>
<td></td>
<td></td>
<td>permit tcp any eq 646</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>permit udp any any eq 646</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>permit udp any eq 646</td>
<td></td>
</tr>
<tr>
<td>Supported Protocols</td>
<td>Criteria</td>
<td>Match</td>
<td>Queue#</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>---------------</td>
<td>--------------------------------------------</td>
<td>----------------------------</td>
</tr>
<tr>
<td>RADIUS - Remote Authentication Dial In User Service</td>
<td>IP/Port Match</td>
<td>permit udp 64.202.160.0 0.0.1.255 eq 1645 any&lt;br&gt;permit udp 64.202.160.0 0.0.1.255 any eq 1645&lt;br&gt;permit udp 64.202.160.0 0.0.1.255 eq 1646 any&lt;br&gt;permit udp 64.202.160.0 0.0.1.255 any eq 1646&lt;br&gt;permit udp 64.202.160.0 0.0.1.255 eq 1812 any&lt;br&gt;permit udp 64.202.160.0 0.0.1.255 any eq 1812&lt;br&gt;permit udp 64.202.160.0 0.0.1.255 eq 1813 any&lt;br&gt;permit udp 64.202.160.0 0.0.1.255 any eq 1813&lt;br&gt;permit tcp 64.202.160.0 0.0.1.255 eq 1645 any&lt;br&gt;permit tcp 64.202.160.0 0.0.1.255 any eq 1645&lt;br&gt;permit tcp 64.202.160.0 0.0.1.255 eq 1646 any&lt;br&gt;permit tcp 64.202.160.0 0.0.1.255 any eq 1646&lt;br&gt;permit tcp 64.202.160.0 0.0.1.255 eq 1812 any&lt;br&gt;permit tcp 64.202.160.0 0.0.1.255 any eq 1812&lt;br&gt;permit tcp 64.202.160.0 0.0.1.255 eq 1813 any&lt;br&gt;permit tcp 64.202.160.0 0.0.1.255 any eq 1813</td>
<td>NQ_CPU_HOST_Q</td>
</tr>
<tr>
<td>HSRP - Hot Standby Router Protocol</td>
<td>IP/Port Match</td>
<td>permit udp any 224.0.0.0/24 eq 1985&lt;br&gt;permit udp any eq 1985 224.0.0.0/24</td>
<td>NQ_CPU_HOST_Q</td>
</tr>
</tbody>
</table>
### Input Rate-Limiting and Silent Mode Operation

A router is automatically enabled to silently discard packets when you configure input policing on control plane traffic using the `service-policy input policy-map-name` command.

Rate-limiting (policing) of input traffic from the control plane is performed in silent mode. In silent mode, a router that is running Cisco IOS XE software operates without receiving any system messages. If a packet that is entering the control plane is discarded for input policing, you do not receive an error message.

### How to Use Control Plane Policing

#### Defining Control Plane Services

Perform this task to define control plane services, such as packet rate control and silent packet discard for the RP.

**Before you begin**

Before you enter control-plane configuration mode to attach an existing QoS policy to the control plane, you must first create the policy using MQC to define a class map and policy map for control plane traffic.

- Platform-specific restrictions, if any, are checked when the service policy is applied to the control plane interface.
- Input policing does not provide any performance benefits. It simply controls the information that is entering the device.

---

**Step 1** `enable`

**Example:**

```bash
Device> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

**Step 2** `configure terminal`

**Example:**

```bash
Device# configure terminal
```

Enters global configuration mode.

**Step 3** `control-plane`

**Example:**

```bash
Device(config)# control-plane
```

Enters control-plane configuration mode (which is a prerequisite for defining control plane services).

**Step 4** `service-policy input policy-map-name`

---
Example:
Device(config-cp)# service-policy input control-plane-policy
Attaches a QoS service policy to the control plane.

- **input**—Applies the specified service policy to packets received on the control plane.
- **policy-map-name**—Name of a service policy map (created using the `policy-map` command) to be attached.

**Step 5**
Example:
Device(config-cp)# end
(Optional) Returns to privileged EXEC mode.

---

**Verifying Control Plane Services**

**SUMMARY STEPS**

1. `enable`
2. `show policy-map control-plane [all] [input [class class-name]]`
3. `exit`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>enable</td>
</tr>
<tr>
<td>Example:</td>
<td>Device&gt; enable</td>
</tr>
<tr>
<td></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>- Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>show policy-map control-plane [all] [input [class class-name]]</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# show policy-map control-plane all</td>
</tr>
<tr>
<td></td>
<td>Displays information about the control plane.</td>
</tr>
<tr>
<td></td>
<td>- all—(Optional) Displays service policy information about all QoS policies used on the CP.</td>
</tr>
<tr>
<td></td>
<td>- input—(Optional) Displays statistics for the attached input policy.</td>
</tr>
<tr>
<td></td>
<td>- class class-name—(Optional) Specifies the name of the traffic class whose configuration and statistics are displayed.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>exit</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# exit</td>
</tr>
<tr>
<td></td>
<td>(Optional) Exits privileged EXEC mode.</td>
</tr>
</tbody>
</table>
Examples
The following example shows that the policy map TEST is associated with the control plane.

Device# show policy-map control-plane

Control Plane
Service-policy input:TEST
Class-map:TEST (match-all)
  20 packets, 11280 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
Match:access-group 101
police:
  8000 bps, 1500 limit, 1500 extended limit
  conformed 15 packets, 6210 bytes; action:transmit
  exceeded 5 packets, 5070 bytes; action:drop
  violated 0 packets, 0 bytes; action:drop
Class-map:class-default (match-any)
  0 packets, 0 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
Match:any

Configuring Control Plane Policing to Mitigate Denial-of-Service Attacks

Apply control plane policing (CoPP) to ICMP packets to mitigate denial of service (DoS) attacks.

SUMMARY STEPS

1. enable
2. configure terminal
3. access-list access-list-number permit protocol {any | host {address | name}} {any | host {address | name}}
4. access-list access-list-number permit protocol {tcp | udp} {any | host {source-addr | name}} eq port number {any | host {source-addr | name}} eq port number
5. class-map class-map-name
6. match access-group access-list-index
7. exit
8. policy-map policy-map-name
9. class class-map-name
10. police {rate-bps | cir {cir-bps | percent percent}} [bc burst-bytes] [conform-action action] [pir pir-bps]
11. conform-action action
12. exit
13. exit
14. control-plane
15. service-policy input policy-map-name
16. exit
17. exit
### Detailed Steps

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device&gt; <code>enable</code></td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device# <code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>`access-list access-list-number permit protocol {any</td>
<td>host {address</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# <code>access-list 110 permit icmp any 169.223.253.1</code></td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>`access-list access-list-number permit protocol {tcp</td>
<td>udp} {any</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# <code>access-list 111 permit icmp any eq 1699 any eq 1698</code></td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td><code>class-map class-map-name</code></td>
<td>Creates a class-map and enters QoS class-map configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# <code>class-map match-any MyClassMap</code></td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td><code>match access-group access-list-index</code></td>
<td>Specifies access groups to apply to an identity policy. The range of valid values is 1-2799.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-cmap)# <code>match access-group 140</code></td>
<td></td>
</tr>
<tr>
<td>Step 7</td>
<td><code>exit</code></td>
<td>Exits QoS class-map configuration mode and returns to global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-cmap)# <code>exit</code></td>
<td></td>
</tr>
<tr>
<td>Step 8</td>
<td><code>policy-map policy-map-name</code></td>
<td>Specifies a service policy and enters QoS policy-map configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# <code>policy-map Policy1</code></td>
<td></td>
</tr>
<tr>
<td>Step 9</td>
<td><code>class class-map-name</code></td>
<td>Enters QoS policy-map class configuration mode</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-pmap-)# <code>class MyClassMap</code></td>
<td></td>
</tr>
</tbody>
</table>
### Purpose

Configure a traffic policer based on the traffic rate or committed information rate (CIR). By default, no policer is defined.

- **rate-bps** — Specifies average traffic rate in bits per second (b/s). The range is 64000 to 1000000000. Supply an optional postfix (K, M, G). Decimal point is allowed.
- **cir** — Specifies a committed information rate (CIR).
- **cir-bps** — Specifies a CIR in bits per second (b/s). The range is 64000 to 1000000000. Supply an optional postfix (K, M, G). Decimal point is allowed.
- **bc burst-bytes** — (Optional) Specifies the conformed burst (bc) or the number of acceptable burst bytes. The range is 8000 to 16000000.
- **conform-action action** — (Optional) Specifies action to take on packets that conform to the specified rate limit.
- **pir pir-bps** — (Optional) Specifies the peak information rate (PIR).

### Note

**cir percent** option is not supported on the router.

### Command or Action

#### Step 10

**police** `{rate-bps | cir {cir-bps | percent percent}} {bc burst-bytes} [conform-action action] [pir pir-bps]`

**Example:**

```
Device(config-pmap-c)# police cir 10m
```

#### Step 11

**conform-action action**

**Example:**

```
Device(config-pmap-c-police)# conform-action transmit
```

#### Step 12

**exit**

**Example:**

```
Device(config-pmap-c-police)# exit
```

#### Step 13

**exit**

**Example:**

```
Device(config-pmap-)# exit
```

#### Step 14

**control-plane**

**Example:**

```
Device(config)# control-plane
```

#### Step 15

**service-policy input policy-map-name**

**Example:**

```
Device(config-cp)# service-policy input Policy1
```
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 16</td>
<td>Exits control plane configuration mode and returns to global configuration mode.</td>
</tr>
<tr>
<td>exit</td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Device(config-cp)# exit</td>
</tr>
<tr>
<td>Step 17</td>
<td>Exits global configuration mode returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>exit</td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Device(config)# exit</td>
</tr>
</tbody>
</table>

Configuration Examples for Control Plane Policing

Example: Configuring Control Plane Policing on Input Telnet Traffic

```plaintext
! Rate-limit all other Telnet traffic.
Device(config)# access-list 140 permit tcp any any eq telnet

! Define class-map "telnet-class."
Device(config)# class-map telnet-class
Device(config-cmap)# match access-group 140
Device(config-cmap)# exit
Device(config)# policy-map control-plane-in
Device(config-pmap)# class telnet-class
Device(config-pmap-c)# police 80000 conform transmit exceed drop
Device(config-pmap-c)# exit
Device(config-pmap)# exit

! Define aggregate control plane service for the active route processor.
Device(config)# control-plane
Device(config-cp)# service-policy input control-plane-in
Device(config-cp)# end
```

Additional References

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
</table>

Standards and RFCs

<table>
<thead>
<tr>
<th>Standard/RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>No specific Standards and RFCs are supported by the features in this document.</td>
<td>—</td>
</tr>
</tbody>
</table>
### MIBs

<table>
<thead>
<tr>
<th>MB</th>
<th>MIBs Link</th>
</tr>
</thead>
</table>
|    | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:  

### Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
</table>
| The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.  
To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.  

### Feature Information for Control Plane Policing

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to [www.cisco.com/go/cfn](http://www.cisco.com/go/cfn). An account on Cisco.com is not required.

#### Table 4: Feature Information for Control Plane Policing

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
</table>
CHAPTER 5

Priority Shaper

Earlier, when the priority of a queue at Per-Hop Behavior (PHB) was propagated all the way up the hierarchy towards the channel level, the PHB classes that had priority at PHB level would only be prioritized over other classes of subchannels. To avoid this, Priority Shaper feature is implemented.

Priority Shaper feature helps to balance the packet drops between the streams when multiple streams egress out of a priority queue. Egress QoS policy is supported on Priority Shaper.

- Restrictions for Priority Shaper, on page 43
- Configuring Priority Shaper, on page 43

Restrictions for Priority Shaper

- Priority Shaper is supported only for PHB level classes.
- Egress QoS Policy map with Priority Shaper can be applied only on the member interface of port channel and not at the logical level.
- Policer configuration is not supported with the Priority Shaper configuration under same class map.
- Priority Traffic Latency is increased during congestion with Priority Shaper configuration at Q level. Configure the queue limit with a lesser value for the priority queue to reduce the latency of priority traffic.
- If the packet is from a 10G interface to a 1G interface, the business is introduced. Due to this, dequeuing rate of this strict priority queue may be sometimes more than enqueuing. As a result, very few packet counters are seen in other queues.

Configuring Priority Shaper

Perform the following steps to configure Priority Shaper.

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `class-map class-map-name`
4. `match cos number`
5. `policy-map policy-map-name`
6. `class class-map-name`
7. `priority level <level 1/2> percent <percentage 1-100>` or `priority level <level 1/2> kbps <burst size>`
8. `interface interface-type interface-number`
9. `service-policy output policy-map-name`
10. `end`

**DETAILED STEPS**

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

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

| **Step 3**        | Configures class map and specifies the name of the class map to be created. |
| class-map class-map-name | Configures class map and specifies the name of the class map to be created. |
| Example:          | Configures class map and specifies the name of the class map to be created. |
| Device(config)#class-map class_priority | Configures class map and specifies the name of the class map to be created. |

| **Step 4**        | Matched different PHBs for different class maps. |
| match cos number  | Matched different PHBs for different class maps. |
| Example:          | Matched different PHBs for different class maps. |
| Device(config-cmap)# match cos 1 | Matched different PHBs for different class maps. |

| **Step 5**        | Configures the policy map. |
| policy-map policy-map-name | Configures the policy map. |
| Example:          | Configures the policy map. |
| Device(config)#policy-map shape_priority | Configures the policy map. |

| **Step 6**        | Specifies the name of the class whose policy you want to create and enters policy-map class configuration mode. |
| class class-map-name | Specifies the name of the class whose policy you want to create and enters policy-map class configuration mode. |
| Example:          | Specifies the name of the class whose policy you want to create and enters policy-map class configuration mode. |
| Device(config-pmap)#class class_priority | Specifies the name of the class whose policy you want to create and enters policy-map class configuration mode. |

| **Step 7**        | Assigns priority to a traffic class at the priority level specified. |
| priority level <level 1/2> percent <percentage 1-100> | Assigns priority to a traffic class at the priority level specified. |
| or priority level <level 1/2> kbps <burst size> | Assigns priority to a traffic class at the priority level specified. |
| Example:          | Assigns priority to a traffic class at the priority level specified. |
| Device(config-pmap-c)# priority <1-10000000> Kilo Bits per second | Assigns priority to a traffic class at the priority level specified. |
| Device(config-pmap-c)# priority Percent <1-100> | Assigns priority to a traffic class at the priority level specified. |
| Device(config-pmap-c)# priority level <1-2> <1-10000000> | Assigns priority to a traffic class at the priority level specified. |
| Device(config-pmap-c)# priority level <1-2> percent <1-100> | Assigns priority to a traffic class at the priority level specified. |

**Note:** *level* is the level of priority assigned to the priority class. Valid values are 1 (high priority) and 2 (low priority). The default value is 1. Do not specify the same priority level for two different classes in the same policy map.
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 8</strong> interface interface-type interface-number</td>
<td>Specifies the port to attach to the policy map and allows to enter the interface configuration mode. Valid interfaces are physical ports.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config)# interface gigabitethernet 0/0/1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong> service-policy output policy-map-name</td>
<td>Applies output policy to the interface.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config-if)# service instance 1 ethernet Device(config-if-srv)# service-policy output shape_priority</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong> You can also attach the service policy over the service instance.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 10</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config)#end</td>
<td></td>
</tr>
</tbody>
</table>

### Configuration Examples for Priority Shaper

This section shows sample configurations for Priority Shaper.

### Example: Configuring Priority Shaper

The following is a sample configuration for ECMP load balancing.

```
Device(config)# class-map match-any class_level1
Device(config-cmap)# match cos 1
Device(config-cmap)# match cos 2
Device(config-cmap)# class-map match-any class_level2
Device(config-cmap)# match cos 3
Device(config-cmap)# match cos 4
Device(config-cmap)# class-map match-any class_bw
Device(config-cmap)# match cos 5
Device(config-cmap)# end

Device(config)# policy-map shape_priority
Device(config-pmap)# class class_level1
Device(config-pmap-c)# priority level 1 per 10
Device(config-pmap-c)# class class_level2
Device(config-pmap-c)# priority level 2 per 20
Device(config-pmap-c)# class class_bw
Device(config-pmap-c)# bandwidth remaining percent 70
Device(config-pmap-c)# end

Device(config)# interface GigabitEthernet0/0/3
Device(config-if)# load-interval 30
Device(config-if)# service-policy output shape_priority
Device(config-if)# end
```

*Note:* The match cos is *not* supported at egress on the Cisco RSP3 Module.
Verifying Priority Shaper

Use the following command to verify that the Priority Shaper feature is configured on your interface.

Device# show policy-map interface TenGigabitEthernet0/0/2
show policy-map interface TenGigabitEthernet0/0/2
TenGigabitEthernet0/0/2
Service-policy output: shape_priority

queue stats for all priority classes:
  Queueing
  priority level 1
  queue limit 3932 us/ 49152 bytes
  (queue depth/total drops/no-buffer drops) 49476/44577300/0
  (pkts output/bytes output) 2348138/1202246656

queue stats for all priority classes:
  Queueing
  priority level 2
  queue limit 1966 us/ 49152 bytes
  (queue depth/total drops/no-buffer drops) 51072/42228358/0
  (pkts output/bytes output) 4697080/2404904960

Class-map: class_priority (match-any)
  46925438 packets, 24025824256 bytes
  30 second offered rate 1871849000 bps, drop rate 1778171000 bps
  Match: cos 1
  Match: cos 2
  Priority: 10% (100000 kbps), burst bytes 2500000, b/w exceed drops: 44577300
  Priority Level: 1

Class-map: class_priority_level2 (match-any)
  46925438 packets, 24025824256 bytes
  30 second offered rate 1871849000 bps, drop rate 1684485000 bps
  Match: cos 3
  Match: cos 4
  Priority: 20% (200000 kbps), burst bytes 5000000, b/w exceed drops: 42228358
  Priority Level: 2

Class-map: class_bw (match-any)
  23462719 packets, 12012912128 bytes
  30 second offered rate 935925000 bps, drop rate 281045000 bps
  Match: cos 5
  Queueing
  queue limit 393 us/ 49152 bytes
  (queue depth/total drops/no-buffer drops) 49476/7045085/0
  (pkts output/bytes output) 16417634/8405828608
  bandwidth remaining 70%

Class-map: class-default (match-any)
  0 packets, 0 bytes
  30 second offered rate 0000 bps, drop rate 0000 bps
  Match: any

  queue limit 393 us/ 49152 bytes
  (queue depth/total drops/no-buffer drops) 0/0/0
  (pkts output/bytes output) 0/0
Hierarchical Color-Aware Policing

The Hierarchical Color-Aware Policing feature provides two levels of policing where the policer ordering is evaluated from child to parent, and there is preferential treatment of certain traffic at the parent level.

- Finding Feature Information, on page 47
- Prerequisites for Hierarchical Color-Aware Policing, on page 47
- Restrictions for Hierarchical Color-Aware Policing, on page 47
- Information About Hierarchical Color-Aware Policing, on page 48
- How to Configure Hierarchical Color-Aware Policing, on page 51
- Configuration Examples for Hierarchical Color-Aware Policing, on page 54
- Additional References, on page 56
- Feature Information for Hierarchical Color-Aware Policing, on page 57

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Hierarchical Color-Aware Policing

You must have Cisco IOS XE Release 3.15S or a later version installed and running on your router.

You must already be familiar with relevant features and technologies including modular QoS CLI (MQC) and the master control processor (MCP) software and hardware architecture. The Additional References, on page 41 section provides pointers to relevant feature and technology documents.

Restrictions for Hierarchical Color-Aware Policing

The following restrictions apply to the Hierarchical Color-Aware Policing feature:
• Color-aware class maps support only QoS group matching.
• Color-aware statistics are not supported, only existing policer statistics.
• Color-aware class map removal (using the no class-map class-map-name command) is not allowed while the class map is being referenced in a color-aware policer. It must be removed from all color-aware policers (using either the no conform-color class-map-name or no exceed-color class-map-name command first).
• By default, the child policer is color-blind. If any control traffic is classified as default class then it may be dropped.
• For dual policers in HQoS policy, if parent policer is color-aware, child level policer cannot be configured as color-aware and is rejected.
• When parent policer is color-aware, child cannot be configured with PIR, it can only be a 1R2C policer.
• Conform or exceed color classification should be part of child policer conform marking action.
• When parent is color aware, status of child policer which comes under red classification based on parent’s conform and exceed class may not work properly.
• QoS-group can be set in child policer through tablemap, but complete child class classification should map either to conform class qos-group or exceed class qos-group.
• Exceeded traffic can either drop or transmit packets. When exceeded traffic is configured to transmit packets in the parent, the statistics for exceeded traffic is not made color-aware.

Information About Hierarchical Color-Aware Policing

Hierarchical Order Policing

Policers are evaluated from child to parent in QoS policies. This ordering is not configurable for both ingress and egress directions.

The following sample configuration for a simple two-level policer would result in the changed behavior shown in the figure below:

```
policy-map child
class user1
  police 100k
class user2
  police 100k
policy-map parent
class class-default
  police 150k
service-policy child
```
Limited Color-Aware Policing

The following sample configuration for a simple two-level color-aware policer would result in the changed behavior shown in the figure below:

```
ip access-list extended user1-acl
 permit ip host 192.168.1.1 any
 permit ip host 192.168.1.2 any
ip access-list extended user2-acl
 permit ip host 192.168.2.1 any
 permit ip host 192.168.2.2 any
class-map match-all user1-acl-child
 match access-group name user1-acl
class-map match-all user2-acl-child
 match access-group name user2-acl
class-map match-all hipri-conform
 match qos-group 5
policy-map child-policy
 class user1-acl-child
  police 10000 bc 1500
  conform-action set-qos-transmit 5
class user2-acl-child
 police 20000 bc 1500
  conform-action set-qos-transmit 5
class class-default
 police 50000 bc 1500
policy-map parent-policy
 class class-default
 police 50000 bc 3000
 confirm-action transmit
 exceed-action transmit
 violate-action drop
 conform-color hipri-conform
service-policy child-policy
```
Figure 2: Simple Two-Level Color-Aware Policer

Child policing and marking

Parent color classification and color-aware policing

---

Note

To avoid drops at the parent level for "conformed" child traffic, the parent policer must have a rate and burst that are equal to or greater than the sum of the child conform rates and burst sizes. There is no check for inappropriate (parent-to-child) rates and burst sizes in code. You must be aware of this limitation and configure appropriately. In the following example, explicit marking actions are supported in conjunction with color-aware policing and operate similarly color-aware policer marking actions. If these marking actions ("set qos-group," for example) are present in the child policies, the resulting bit values are evaluated by the parent color-aware policer (same as for child policer marking actions): 50k >= 10k (user1-acl-child) + 20k (user2-acl-child)

---

Policing Traffic in Child Classes and Parent Classes

Prior to the release of the Hierarchical Color-Aware Policing feature, policing and marking were typically used as input QoS options. For example, a voice customer was limited to 112 kb/s for voice control and 200 kb/s for voice traffic. The class-default class has no policer. The only limit is the physical bandwidth of the xDSL connection. As shown in the figure below, a customer could send up to 1000 kb/s. However, this involved sending more voice and voice-control packets, which required policing the traffic for both classes.

Figure 3: Policing Traffic in Child Classes

As shown in the figure below, it is important to control the overall input bandwidth. The important requirement is that the premium traffic in the overall limit is not affected. In the figure below, voice and voice-control packets are not dropped in the overall limit. Only packets from the child class-default class are dropped to fulfill the limit.
Figure 4: Policing Traffic in Parent Classes

The first classes function the same way. Voice and voice-control are policed to the allowed level and the class-default class is not affected. In the next level, the overall bandwidth is forced to 500 kb/s and must only drop packets from the class-default class. Voice and voice-control must remain unaffected.

The order of policer execution is as follows:

1. Police the traffic in the child classes, as shown in the figure above, police VoIP-Control class to 112 kb/s, police VoIP class to 200 kb/s, and police class-default to 500 kb/s.

2. Police the traffic in the class default of the parent policy map, but only drop the traffic from the child class default, and do not drop the remaining child classes. As shown in the figure above, 112 kb/s VoIP-Control and 200 kb/s VoIP traffic are unaffected at the parent policer, but 500 kb/s class default from the child is policed to 188 kb/s to meet the overall police policy of 500 kb/s at the parent level.

How to Configure Hierarchical Color-Aware Policing

Configuring the Hierarchical Color-Aware Policing Feature

**SUMMARY STEPS**

1. enable
2. configure terminal
3. policy-map policy-map-name
4. class {class-name | class-default}
5. conform-color class-map-name [exceed-color class-map-name]
6. police [cir cir] [bc conform-burst] [pir pir] [be peak-burst] [conform-action action] [exceed-action action] [violate-action action] [conform-color hipri-conform] [exceed-color lipri-exceed]
7. service-policy policy-map-name
8. end

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
</tbody>
</table>
### Configuring the Hierarchical Color-Aware Policing Feature

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 2**
  **Example:**
  ```
  Router> enable
  ```
  | • Enter your password if prompted. |
| **Step 2**
  **Example:**
  ```
  Configure terminal
  ```
  | Enters global configuration mode. |
| **Step 3**
  **Example:**
  ```
  Policy-map policy-map-name
  ```
  | Enters policy-map configuration mode and creates a policy map. |
| **Step 4**
  **Example:**
  ```
  Class {class-name | class-default}
  ```
  | Enters policy-map class configuration mode. |
| **Step 4**
  **Example:**
  ```
  Router(config)# class user1-acl-child
  ```
  | Specifies the name of the class whose policy you want to create or change or specifies the default class (commonly known as the class-default class) before you configure its policy. Repeat this command as many times as necessary to specify the child or parent classes that you are creating or modifying:
  - **class name**—Name of the class to be configured or whose policy is to be modified. The class name is used for both the class map and to configure a policy for the class in the policy map.
  - **class-default**—Specifies the default class so that you can configure or modify its policy. |
| **Step 5**
  **Example:**
  ```
  Conform-color class-map-name [exceed-color class-map-name]
  ```
  | Enables color-aware traffic policing and creates the conform-color and exceed-color class-maps used for color-aware traffic policing. |
| **Step 5**
  **Example:**
  ```
  Router(config-pmap-c-police)# conform-color c1 exceed-color c2
  ```
  | The **conform-color class-map-name** command creates the conform-color class. The **exceed-color class-map-name** option creates the exceed-color class. |
| **Step 6**
  **Example:**
  ```
  Police [cir cir] [bc conform-burst] [pir pir] [be peak-burst] [conform-action action [exceed-action action [violate-action action]]] [conform-color hipri-conform] [exceed-color lipri-exceed]
  ```
  | Configures traffic policing and specifies multiple actions applied to packets marked as conforming to, exceeding, or violating a specific rate. |
| **Step 6**
  **Example:**
  ```
  Router(config-pmap-c)# police 10000 bc 1500
  ```
  | Enters policy-map class police configuration mode. Use one line per action that you want to specify:
  - **cir**—Committed information rate. Indicates that the CIR will be used for policing traffic.
  - **conform-action**—(Optional) Action to take on packets when the rate is less than the conform burst. |
### Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• <strong>exceed-action</strong>—(Optional) Action to take on packets whose rate is within the conform and conform plus exceed burst.</td>
</tr>
<tr>
<td></td>
<td>• <strong>violate-action</strong>—(Optional) Action to take on packets whose rate exceeds the conform plus exceed burst. You must specify the exceed action before you specify the violate action.</td>
</tr>
<tr>
<td></td>
<td>• <strong>conform-color</strong>—(Optional) Enables color-aware policing (on the policer being configured) and assigns the class map to be used for conform color determination. The <code>hipri-conform</code> keyword is the class map (previously configured via the <code>class-map</code> command) to be used.</td>
</tr>
<tr>
<td></td>
<td>• <strong>exceed-color</strong>—(Optional) Enables color-aware policing (on the policer being configured) and assigns the class map to be used for exceed color determination. The <code>lipri-exceed</code> keyword is the class map (previously configured via the <code>class-map</code> command) to be used.</td>
</tr>
</tbody>
</table>

**Example**

The following is a sample configuration for the Hierarchical Color-Aware Policing feature:

```plaintext
class-map qos_group1
match qos_group 1

class-map qos_group2
match qos_group 2

Class-map cos1
match cos 1

class-map cos 2
match cos 2

policy-map tc001_ch
```

---

**Step 7**

```
service-policy policy-map-name
```

**Example:**

```
Router(config-pmap-c-police)# service-policy child-policy
```

Specifies a service policy as a QoS policy within a policy map (called a hierarchical service policy).

- **policy-map-name**—Name of the predefined policy map to be used as a QoS policy. The name can be a maximum of 40 alphanumeric characters.

**Step 8**

```
end
```

**Example:**

```
Router(config-pmap-c-police)# end
```

Exits the current configuration mode.
Configuration Examples for Hierarchical Color-Aware Policing

Example Enabling the Hierarchical Color-Aware Policing Feature

The following example shows a sample configuration that enables the Hierarchical Color-Aware Policing feature:

class-map qos_group1
match qos_group 1

class-map qos_group2
match qos_group 2

class-map cos1
match cos 1

class-map cos 2
match cos 2

policy-map tc001_ch
class cos1
police cir 20000000 bc 625000
conform-action set-qos-transmit 1
exceed-action drop
class cos2
police cir 50000000 bc 1562500
conform-action set-qos-transmit 2
exceed-action drop

policy-map tc001_parent
class class-default
police cir 70000000 bc 2187500 pir 100000000 be 3125000
conform-color qos_group1 exceed-color qos_group2
conform-action transmit exceed-action transmit
violate-action drop
service-policy tc001_child
Example Disallowing Multiple Entries in Class Map

The following example shows a rejected attempt to configure multiple entries in a class map:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# class-map hipri-conform
Router(config-cmap)# match qos-group 5
Router(config-cmap)# match qos-group 6
Only one match statement is supported for color-aware policing
Router(config-cmap)# no match qos-group 6
```

Example Disallowing the Removal of an Active Color-Aware Class Map

The following example shows that an active color-aware class map cannot be disallowed:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# no class-map hipri-conform
Class-map hipri-conform is being used
```

Example Dismantling a Configuration of the Hierarchical Color-Aware Policing Feature

The following example shows how to dismantle the configuration of the Hierarchical Color-Aware Policing feature:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# no policy-map parent-policy
Router(config)# no policy-map child-policy
Router(config)# no class-map hipri-conform
Router(config)# no class-map user1-acl-child
Router(config)# no class-map user2-acl-child
```

Example Applying show Command with Hierarchical Color-Aware Policing

The following is sample output from the `show policy-map interface` command when a policy with hierarchical color-aware policing is applied:

```
Router# show policy-map interface
GigabitEthernet0/0/0
Service-policy input: parent-policy
Class-map: class-default (match-any)
  0 packets, 0 bytes
  5 minute offered rate 0000 bps, drop rate 0000 bps
Match: any
police:
cir 50000 bps, bc 3000 bytes, be 3000 bytes
conformed 0 packets, 0 bytes; actions: transmit
exceeded 0 packets, 0 bytes; actions: transmit
```
violated 0 packets, 0 bytes; actions: drop
No color-aware policing statistics available
conformed 0 packets, 0 bytes; actions: drop
No color-aware policing statistics available
conformed 0 packets, 0 bytes; actions: drop

Service-policy: child-policy
Class-map: user1-acl-child (match-all)
0 packets, 0 bytes
5 minute offered rate 0000 bps, drop rate 0000 bps
Match: access-group name user1-acl
police:
cir 10000 bps, bc 1500 bytes
conformed 0 packets, 0 bytes; actions: set-qos-transmit 5
exceeded 0 packets, 0 bytes; actions: drop
conformed 0000 bps, exceed 0000 bps
Class-map: user2-acl-child (match-all)
0 packets, 0 bytes
5 minute offered rate 0000 bps, drop rate 0000 bps
Match: access-group name user2-acl
police:
cir 20000 bps, bc 1500 bytes
conformed 0 packets, 0 bytes; actions: set-qos-transmit 5
exceeded 0 packets, 0 bytes; actions: drop
conformed 0000 bps, exceed 0000 bps
Class-map: class-default (match-any)
0 packets, 0 bytes
5 minute offered rate 0000 bps, drop rate 0000 bps
Match: any
cir 50000 bps, bc 1500 bytes
conformed 0 packets, 0 bytes; actions: transmit
exceeded 0 packets, 0 bytes; actions: drop
conformed 0000 bps, exceed 0000 bps

Additional References

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
</table>

Standards and RFCs

<table>
<thead>
<tr>
<th>Standard/RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>No specific Standards and RFCs are supported by the features in this document.</td>
<td>—</td>
</tr>
</tbody>
</table>
### MIBs

<table>
<thead>
<tr>
<th>MB</th>
<th>MIBs Link</th>
</tr>
</thead>
</table>
|    | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:  
http://www.cisco.com/go/mibs |

### Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
</table>
| The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.  
To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.  

### Feature Information for Hierarchical Color-Aware Policing

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to [www.cisco.com/go/cfn](http://www.cisco.com/go/cfn). An account on Cisco.com is not required.

**Table 5: Feature Information for Hierarchical Color-Aware Policing**

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
</table>
Feature Information for Hierarchical Color-Aware Policing