QoS: Policing and Shaping Configuration Guide, Cisco IOS XE 17 (Cisco ASR 920 Series)

First Published: 2019-11-14

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2020 Cisco Systems, Inc. All rights reserved.

CONTENTS

CHAPTER 1 Feature History 1

CHAPTER 2 Class-Based Policing 3

- Feature Overview 3
  - Benefits 3
  - Restrictions 4
- Prerequisites 5
- Configuration Tasks 5
  - Configuring Traffic Policing 5
  - Verifying Traffic Policing 5
  - Troubleshooting Tips 6
- Monitoring and Maintaining Traffic Policing 6
- Configuration Examples 6
  - Example Configuring a Service Policy that Includes Traffic Policing 6
- Additional References 8

CHAPTER 3 Punt Policing and Monitoring 11

- Information About Punt Policing and Monitoring 11
  - Overview of Punt Policing and Monitoring 11
- How to Configure Punt Policing and Monitoring 12
  - Configuring Punt Policing 12
  - Verifying Punt Policing 13
    - Verifying Queue-Based Punt Policing 13
    - Verifying Punt Policing Statistics 13
- Configuration Examples for Punt Policing and Monitoring 17
  - Example: Configuring Punt Policing 17

Additional References 17

CHAPTER 4 Port-Shaper and LLQ in the Presence of EFPs 19

Restrictions for Port-Shaper and LLQ in the Presence of EFPs 19

Information About Port-Shaper and LLQ in the Presence of EFPs 19

Ethernet Flow Points and LLQ 19

How to Configure Port-Shaper and LLQ in the Presence of EFPs 20

Configuring Hierarchical Policy Maps 20

Configuring an LLQ Policy Map 22

Configuring Port Level Shaping on the Main Interface with Ethernet Flow Points 24

Configuration Examples for Port-Shaper and LLQ in the Presence of EFPs 27

Example: Configuring Hierarchical QoS Port Level Shaping on the Main Interface with EFPs 27

Example: Configuring Port Level Shaping on the Main Interface with EFPs 27

Additional References 28

CHAPTER 5 Control Plane Policing 31

Information About Control Plane Policing 31

Control Plane Policing Overview 31

Benefits of Control Plane Policing 32

Control Plane Terms to Understand 32

Supported Protocols 33

Input Rate-Limiting and Silent Mode Operation 38

Restrictions for Control Plane Policing 38

IP Access List Overview 39

Benefits 39

IP Address Range-Based Filtering Support for CoPP ACL 40

How to Use Control Plane Policing 41

Defining Control Plane Services 41

Verifying Control Plane Services 42

Configuring Control Plane Policing to Mitigate Denial-of-Service Attacks 43

Configuring CoPP ACL 45

Verifying CoPP ACL 45

Configuration Examples for Control Plane Policing 46

Example: Configuring Control Plane Policing on Input Telnet Traffic 46

Additional References 47

CHAPTER 6 Priority Shaper 49

Restrictions for Priority Shaper 49

Configuring Priority Shaper 49

Configuration Examples for Priority Shaper 51

Example: Configuring Priority Shaper 51

Verifying Priority Shaper 52

CHAPTER 7 Hierarchical Color-Aware Policing 53

Prerequisites for Hierarchical Color-Aware Policing 53

Restrictions for Hierarchical Color-Aware Policing 53

Information About Hierarchical Color-Aware Policing 55

Hierarchical Order Policing 55

Limited Color-Aware Policing 56

Policing Traffic in Child Classes and Parent Classes 57

How to Configure Hierarchical Color-Aware Policing 58

Configuring the Hierarchical Color-Aware Policing Feature 58

Configuration Examples for Hierarchical Color-Aware Policing 61

Example Enabling the Hierarchical Color-Aware Policing Feature 61

Example Disallowing the Removal of an Active Color-Aware Class Map 61

Example Dismantling a Configuration of the Hierarchical Color-Aware Policing Feature 61

Example Applying show Command with Hierarchical Color-Aware Policing 61

Additional References 62

CHAPTER 8 QoS Overhead Accounting 65

Restrictions for QoS Overhead Accounting 65

OH Accounting Support for L3VPN 66

How to Configure QoS Overhead Accounting 67

Applying Overhead Accounting on a Particular Interface 67

Configuring Number of Bytes to be Accounted 67

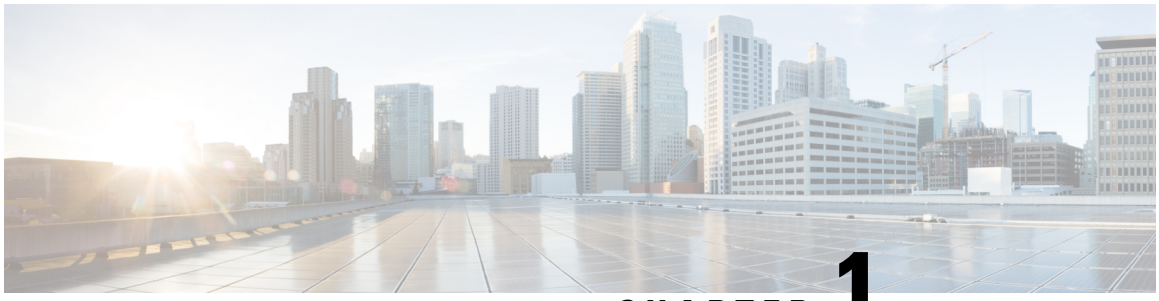
Configuring Overhead Accounting for MPLS Imposition 67

Verifying Overhead Accounting compensation 67

Apply OH Accounting on a Particular L3VPN Interface 68

Configure Number of Bytes to be Accounted 68
Verify OH Accounting Compensation 68

CHAPTER 9 Policer Adjustment in QoS Policy Map 69
Restrictions for Policer Adjustment 69
How to configure Policer Adjustment 70
Enabling Policer Adjustment 70
Disabling Policer Adjustment 70
Verifying Policer Adjustment 70

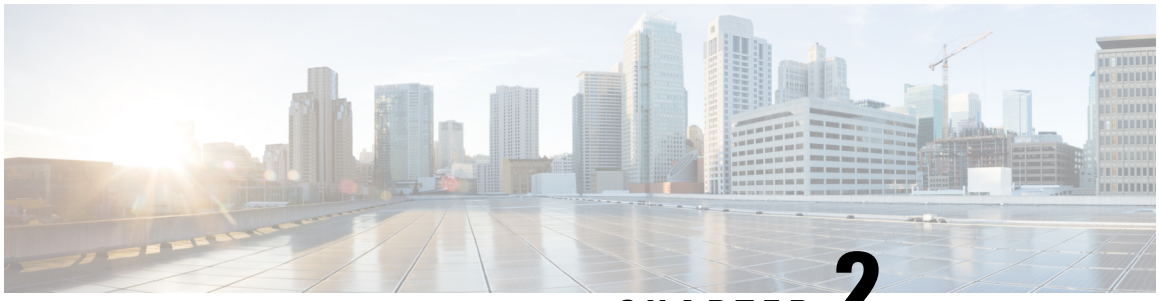


CHAPTER 1

Feature History

The following table lists the new and modified features that are supported in the QoS: Policing and Shaping Configuration Guide in Cisco IOS XE 17 releases.

Feature	Description
Cisco IOS XE Bengaluru 17.5.1	
IP Address Range-Based Filtering Support for CoPP ACL	The CoPP ACL Template feature supports Ingress on In-band Management Loopback interface and Ingress on Data plane interface to block traffic using MPLS. CoPP ACL supports Source IP based filtering on the Cisco router.



CHAPTER 2

Class-Based Policing

- Feature Overview, on page 3
- Prerequisites, on page 5
- Configuration Tasks, on page 5
- Monitoring and Maintaining Traffic Policing, on page 6
- Configuration Examples, on page 6
- Additional References, on page 8

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 Policer 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

Command	Purpose
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 4 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

Command	Purpose
Device# show policy-map	Displays all configured policy maps.
Device# show policy-map policy-map-name	Displays the user-specified policy map.
Device# show policy-map interface	Displays statistics and configurations of all input and output policies that are attached to an interface.
Device# show policy-map interface service instance	Displays the policy map information for a given service instance under a port channel.

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 starts 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

Related Topic	Document Title
QoS commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	Cisco IOS Quality of Service Solutions Command Reference
Modular Quality of Service (QoS) Command-Line Interface (CLI) (MQC), hierarchical policies, policy maps	"Applying QoS Features Using the MQC" module
Policing and shaping traffic	"Policing and Shaping Overview" module

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

MIBs

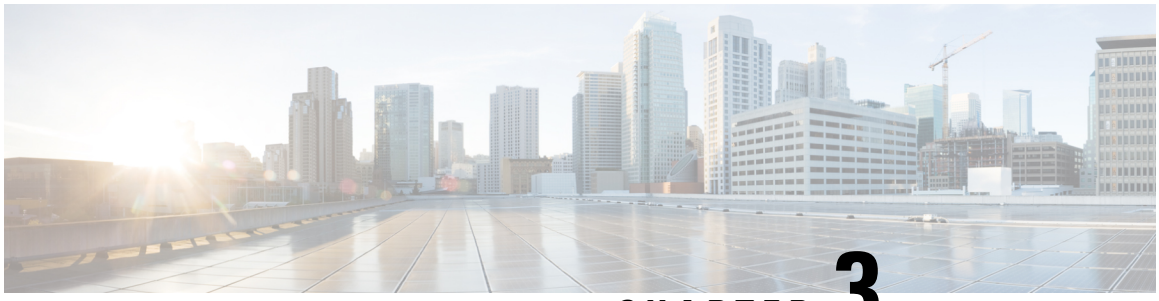
MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS XE software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	--

Technical Assistance

Description	Link
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.	http://www.cisco.com/cisco/web/support/index.html



CHAPTER 3

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.

- Information About Punt Policing and Monitoring, on page 11
- How to Configure Punt Policing and Monitoring, on page 12
- Configuration Examples for Punt Policing and Monitoring, on page 17
- Additional References, on page 17

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.

Note 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.

Per-Interface Per-Cause Punt Policer

Per-interface per-cause (PIPC) punt policing is an enhancement to the Punt Policing and Monitoring feature that allows you to control and limit traffic per interface. From Cisco IOS XE Release 17.5.1, you can set the PIPC rate for all the control plane-punted traffic. When you set the PIPC rate, any traffic beyond the set limit is dropped, thereby enabling you to control the traffic during conditions such as L2 storming.

The PIPC punt policer configuration is supported for the following interfaces:

- Main interface
- Subinterface
- Port channel
- Port channel subinterface
- Tunnels
- PPPoE interface

How to Configure Punt Policing and Monitoring

Configuring Punt Policing

Note 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.

Procedure

	Command or Action	Purpose
Step 1	enable	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	configure terminal **Example:** Device# configure terminal	Enters the global configuration mode.
Step 3	platform qos-policer queue queue-id cir bc **Example:** Device(config)# platform qos-policer queue 20 384000 8000	Enables punt policing on a queue, and specifies the maximum punt rate on a per-queue basis. cir— Indicates Committed Information Rate (CIR). The range is 384000-20000000 bps. bc— Indicates Committed Burts (BC). The range is 8000-16000000 bps.
Step 4	end **Example:** Device(config)# end	(Optional) Returns to privileged EXEC mode.

Verifying Punt Policing

Verifying Queue-Based Punt Policing

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

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

Global drops : 0

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

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.

```
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 |                1000 |               2000
 9   |               REP Q |                3000 |               6000
10   |           BGP LDP 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
 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 MISMATCH Q |                 500 |                1000
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 |                3000 |                6000
26   |          FPGA CCM Q |                3000 |                6000
27   |          FPGA CFE Q |                3000 |                6000
28   |          L2PT DUP Q |                4000 |                8000
```

```
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 MISMATCH Q |                500 |               1000
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 |               9000 |              10000
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 |               2000 |               4000
27   |          FPGA CFE Q |               3000 |               6000
28   |          L2PT DUP Q |               4000 |               8000
```

Use the show platform software infrastructure punt statistics command to view the statistics on the RSP3 module.

```
Router#

Global drops : 0

 Queue Name              | Rx count                    |  Drop count
-------------------------+-----------------------------+-----------------------
 SW FORWARDING Q         | 0                           | 0
 ROUTING PROTOCOL Q      | 0                           | 0
 ICMP Q                  | 0                           | 0
 HOST Q                  | 0                           | 0
 ACL LOGGING Q           | 0                           | 0
 STP Q                   | 0                           | 0
 L2 PROTOCOL Q           | 0                           | 0
 MCAST CONTROL Q         | 0                           | 0
 BROADCAST Q             | 0                           | 0
 REP Q                   | 0                           | 0
 BGP LDP Q               | 0                         | 0
 CONTROL Q               | 0                           | 0
 IP MPLS TTL Q           | 0                           | 0
 DEFAULT MCAST Q         | 0                           | 0
 MCAST ROUTE DATA Q      | 0                           | 0
 MCAST MISMATCH Q        | 0                         | 0
 RPF FAIL Q              | 0                           | 0
 ROUTING THROTTLE Q      | 0                           | 0

MCAST Q                | 0                           | 0
 MPLS OAM Q              | 0                           | 0
 IP MPLS MTU Q           | 0                           | 0
 PTP Q                   | 0                           | 0
 LINUX ND Q              | 0                           | 0
 KEEPALIVE Q             | 0                         | 0
 ESMC Q                  | 0                           | 0
 FPGA BFD Q              | 0                           | 0
```

```
 FPGA CCM Q             | 0                          | 0
 FPGA CFE Q             | 0                          | 0
 L2PT DUP Q             | 0                          | 0
 TDM CTRL Q             | 0                          | 0
 ICMP UNREACHABLE Q     | 0                    | 0
 SSFP Q                 | 0                          | 0
 MIRROT Q               | 0                          | 0
```

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

3 —— queueId of CPU   and 0 — show stats
```

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
```

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 384000 8000
```

Additional References

Related Documents

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

Standards

Standard	Title
None	—

MIBs

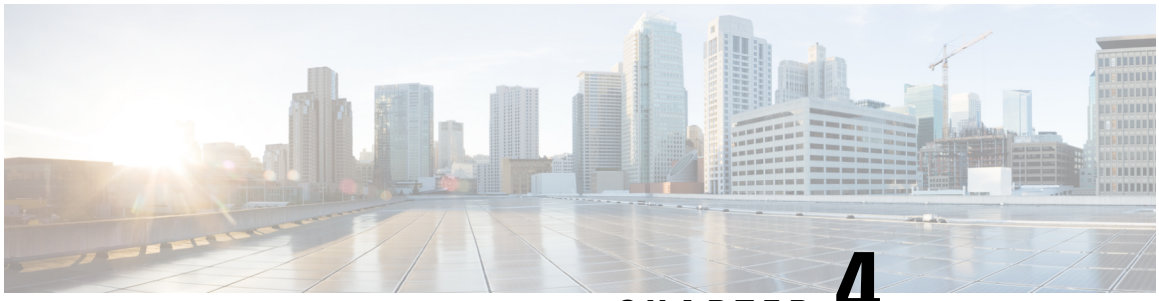
MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS XE Software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
None	

Technical Assistance

Description	Link
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.	http://www.cisco.com/cisco/web/support/index.html



CHAPTER 4

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.

- Restrictions for Port-Shaper and LLQ in the Presence of EFPs, on page 19
- Information About Port-Shaper and LLQ in the Presence of EFPs, on page 19
- How to Configure Port-Shaper and LLQ in the Presence of EFPs, on page 20
- Configuration Examples for Port-Shaper and LLQ in the Presence of EFPs, on page 27
- Additional References, on page 28

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 that is 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 that is 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.

Procedure

Step 1 enable

Example:

```
Device> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 configure terminal

Example:

```
Device# configure terminal
```

Enters global configuration mode.

Step 3 policy-map policy-map-name

Example:

```
Device(config)# policy-map child-llq
```

Creates or modifies the child policy and enters QoS policy-map configuration mode.

- child-llq is the name of the child policy map.

Step 4 class class-map-name

Example:

```
Device(config-pmap)# class precedenc-1
```

Assigns the traffic class you specify to the policy map and enters QoS policy-map class configuration mode.

- precedenc-1 is the name of a previously configured class map and is the traffic class for which you want to define QoS actions.

Step 5 set cos value

Example:

```
Device(config-pmap-c)# set cos 5
```

(Optional) Sets the Layer 2 class of service (CoS) value of an outgoing packet.

- The value is a specific IEEE 802.1Q CoS value from 0 to 7.

Step 6 bandwidth percent percent

Example:

```
Device(config-pmap-c)# bandwidth percent 20
```

(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 7 exit

Example:

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

Exits QoS policy-map class configuration mode.

Step 8 class class-map-name

Example:

```
Device(config-pmap)# class precedenc-2
```

Assigns the traffic class you specify to the policy map and enters QoS policy-map class configuration mode.

- precedenc-2 is the name of a previously configured class map and is the traffic class for which you want to define QoS actions.

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)# 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)# 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.

Configuring an LLQ Policy Map

Procedure

Step 1 enable

Example:

```
Device> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 configure terminal

Example:

```
Device# configure terminal
```

Enters global configuration mode.

Step 3 policy-map policy-map-name

Example:

```
Device(config)# policy-map llq-flat
```

Creates a policy and enters QoS policy-map configuration mode.

Step 4 class class-map-name

Example:

```
Device(config-pmap)# class dscp-af1
```

Assigns the traffic class you specify to the policy map and enters policy-map class configuration mode.

Step 5 priority

Example:

```
Device(config-pmap-c)# priority
```

Configures LLQ, providing strict priority queueing (PQ) for class-based weighted fair queueing (CBWFQ).

Step 6 exit

Example:

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

Exits QoS policy-map class configuration mode.

Step 7 class class-map-name

Example:

```
Device(config-pmap)# class dscp-af2
```

Assigns the traffic class you specify to the policy map and enters QoS policy-map class configuration mode.

Step 8 shape average value

Example:

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

Configures a shape entity with a Comitted Information Rate of 200 Mb/s.

Step 9 exit

Example:

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

Exits QoS policy-map class configuration mode.

Step 10 class class-map-name

Example:

```
Device(config-pmap)# class dscp-af3
```

Assigns the traffic class you specify to the policy map and enters QoS policy-map class configuration mode.

Step 11 bandwidth percent

Example:

```
Device(config-pmap-c)# bandwidth 4000000
```

(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 12 exit

Example:

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

Exits QoS policy-map class configuration mode.

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.

Procedure

Step 1 enable

Example:

```
Device> enable
```

Enables privileged EXEC mode.

- 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:

```
Device(config-if-serv)# exit
```

Exits service instance configuration mode.

Step 11 service instance id ethernet

Example:

```
Device(config-if)# service instance 2 ethernet
```

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
```

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
```

Binds the bridge domain to the service instance.

Step 14 exit

Example:

```
Device(config-if-srv)# exit
```

Exits QoS policy-map class configuration mode.

Step 15 end

Example:

```
Device(config-if)# end
```

(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 precedenc-1
  set cos 5
  bandwidth percent 20
 class precedenc-2
  bandwidth percent 80

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

Note Only match EFP and match qos-group is supported on RSP3 in egress policy map.

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

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
QoS commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	Cisco IOS QoS Command Reference
Policing and shaping	"Policing and Shaping Overview" module
Class maps	"Applying QoS Features Using the MQC" module
Policy maps	"Applying QoS Features Using the MQC" module
Low Latency Queueing	QoS Congestion Management Configuration Guide

Standards and RFCs

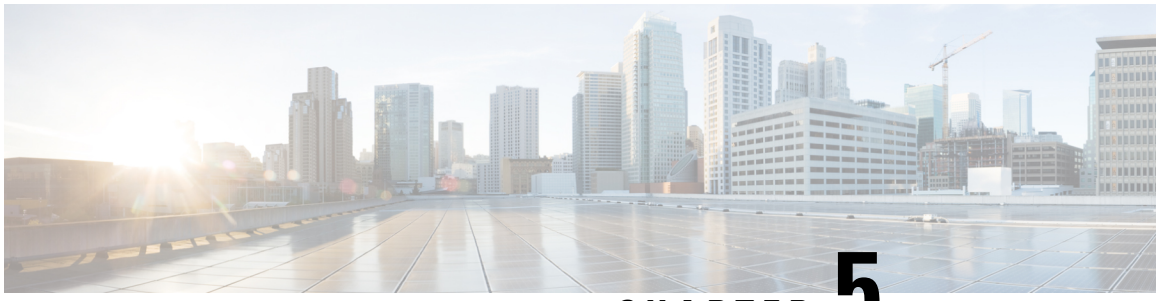
Standard	Title
No new or modified standards are supported, and support for existing standards has not been modified.	--

MIBs

MIB	MIBs Link
No new or modified MIBs are supported, and support for existing MIBs has not been modified.	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: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
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.	http://www.cisco.com/cisco/web/support/index.html



CHAPTER 5

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.

- Information About Control Plane Policing, on page 31
- How to Use Control Plane Policing, on page 41
- Configuration Examples for Control Plane Policing, on page 46
- Additional References, on page 47

Information About Control Plane Policing

Control Plane Policing Overview

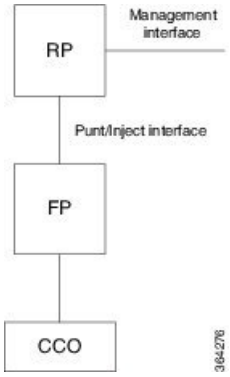
To protect the control plane on a router from DoS attacks and to provide fine-control over the traffic to the control plane, the Control Plane Policing feature treats the control plane as a separate entity with its own interface for ingress (input) and egress (output) traffic. This interface is called the punt or 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.

You can use the platform qos-feature copp-mpls enable command to enable the Control Plane Policing feature on the device for MPLS explicit null scenario, control packets destined to the device is punted to proper control CPU Q. If CoPP-MPLS remains disabled, then self destined control packets like BGP, LDP, telnet and so on, that are MPLS explicit null tagged are not classified by CoPP and is punted to HOST_Q instead of CFM_Q/CONTROL_Q.

Note The command platform qos-feature copp-mpls enable is supported only on Cisco ASR 920 platform.

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



The figure provides an abstract illustration of the router with a single RP and forwarding plane. Packets that are 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 punting packets to the RP in order to achieve the best protection of the control plane in the RP.

Note As mentioned in this 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.

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.

Supported Protocols

The following table lists the protocols supported on Control Plane Policing feature. It is mandatory that the IP address should match the source or destination IP address.

Supported Protocols	Criteria	Match	Queue#
TFTP - Trivial FTP	IP/Port Match	permit udp 64.202.160.0 0.0.1.255 eq 69 any permit udp 64.202.160.0 0.0.1.255 any eq 69	NQ_CPU_HOST_Q
TELNET	IP/Port Match	permit tcp 169.223.252.0 0.0.3.255 host 169.223.253.1 eq telnet permit tcp 169.223.252.0 0.0.3.255 eq telnet host 169.223.253.1	NQ_CPU_CONTROL_Q
NTP - Network Time Protocol	IP/Port Match	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	NQ_CPU_HOST_Q
FTP - File Transfer Protocol	IP/Port Match	permit tcp host <FTP server> eq ftp <loopback block> permit tcp host <FTP server> <loopback block> eq ftp	NQ_CPU_HOST_Q
SNMP - Simple Network Management Protocol	IP/Port Match	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	NQ_CPU_HOST_Q

Supported Protocols	Criteria	Match	Queue#
TACACS - Terminal Access Controller Access-Control System	IP/Port Match	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	NQ_CPU_HOST_Q
FTP-DATA	IP/Port Match	permit tcp any any eq 20 permit tcp any eq 20 any permit udp any any eq 20 permit udp any eq 20 any	NQ_CPU_HOST_Q
HTTP - Hypertext Transfer Protocol	IP/Port Match	permit tcp any any eq www permit tcp any eq www any	NQ_CPU_HOST_Q
WCCP - Web Cache Communication Protocol	IP/Port Match	IP access list copp-system-acl-wccp 10 permit udp any eq 2048 any eq 2048	NQ_CPU_HOST_Q
BGP - Border Gateway Protocol	IP/Port Match	permit tcp 169.223.252.0 0.0.3.255 host 169.223.253.1 eq bgp permit tcp 169.223.252.0 0.0.3.255 eq bgp host 169.223.253.1	NQ_CPU_CFM_Q

Supported Protocols	Criteria	Match	Queue#
SSH - Secure Shell	IP/Port Match	permit udp [remote vty mgmt subnet] 0.0.0.255 any eq 22 permit udp [remote vty mgmt subnet] 0.0.0.255 eq 22 any permit tcp [remote vty mgmt subnet] 0.0.0.255 any eq 22 permit tcp [remote vty mgmt subnet] 0.0.0.255 eq 22 any	NQ_CPU_HOST_Q
ICMP - Internet Control Message Protocol	Protocol Match	access-list 110 permit icmp any 169.223.253.1	NQ_CPU_HOST_Q
ISAKMP - Internet Security Association and Key Management Protocol	IP/Port Match	permit udp any host x.x.x.x eq isakmp permit udp any eq isakmp host x.x.x.x permit udp any host x.x.x.x eq non500-isakmp permit udp any eq non500-isakmp host x.x.x.x	NQ_CPU_HOST_Q
SAA - Service Assurance Agent	IP/Port Match	permit icmp host 10.2.2.4 host 10.1.1.1	NQ_CPU_HOST_Q
DHCP - Dynamic Host Configuration Protocol	IP/Port Match	permit udp host 0.0.0.0 host 255.255.255.255 eq bootps permit udp any eq bootps any eq bootps permit udp host 0.0.0.0 host 255.255.255.255 eq bootpc permit udp any eq bootpc any eq bootpc	NQ_CPU_HOST_Q

Supported Protocols	Criteria	Match	Queue#
DNS - Domain Name System	IP/Port Match	permit udp host <DNS server> eq domain any permit udp host <DNS server> any eq domain permit tcp host <DNS server> eq domain any permit tcp host <DNS server> any eq domain	NQ_CPU_HOST_Q
DLSw - Data-Link Switching	IP/Port Match	permit any any eq 2065 permit any eq 2065 any	NQ_CPU_HOST_Q
LDP - Label Distribution Protocol	IP/Port Match	permit tcp any any eq 646 permit tcp any eq 646 any permit udp any any eq 646 permit udp any eq 646 any	NQ_CPU_CFM_Q

Supported Protocols	Criteria	Match	Queue#
RADIUS - Remote Authentication Dial In User Service	IP/Port Match	permit udp 64.202.160.0 0.0.1.255 eq 1645 any permit udp 64.202.160.0 0.0.1.255 any eq 1645 permit udp 64.202.160.0 0.0.1.255 eq 1646 any permit udp 64.202.160.0 0.0.1.255 any eq 1646 permit udp 64.202.160.0 0.0.1.255 eq 1812 any permit udp 64.202.160.0 0.0.1.255 any eq 1812 permit udp 64.202.160.0 0.0.1.255 eq 1813 any permit udp 64.202.160.0 0.0.1.255 any eq 1813 permit tcp 64.202.160.0 0.0.1.255 eq 1645 any permit tcp 64.202.160.0 0.0.1.255 any eq 1645 permit tcp 64.202.160.0 0.0.1.255 eq 1646 any permit tcp 64.202.160.0 0.0.1.255 any eq 1646 permit tcp 64.202.160.0 0.0.1.255 eq 1812 any permit tcp 64.202.160.0 0.0.1.255 any eq 1812 permit tcp 64.202.160.0 0.0.1.255 eq 1813 any permit tcp 64.202.160.0 0.0.1.255 any eq 1813	NQ_CPU_HOST_Q
HSRP - Hot Standby Router Protocol	IP/Port Match	permit udp any 224.0.0.0/24 eq 1985 permit udp any eq 1985 224.0.0.0/24	NQ_CPU_HOST_Q

Supported Protocols	Criteria	Match	Queue#
Network Configuration Protocol (NETCONF)	IP/Port Match	IP access list ext copp-system-acl-telnet permit tcp any any eq 830 - NETCONF	NQ_CPU_HOST_Q
PostgreSQL Support	IP/Port Match	IP access list ext copp-system-acl-telnet PostgreSQL IP/Port Match permit tcp 169.223.252.0.0 0.0.3.255 host 169.223.253.1 eq 5432	NQ_CPU_HOST_Q
Source IP or Destination IP	IP Match only	Permit IP host 10.1.1.1 or 10.1.1.2 **Note** The **permit ip any any** command is not supported.	NQ_CPU_HOST_Q

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.

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.

Restrictions for CoPP

- IPv6 is not supported.
- Port range ACL is not supported.
- To filter MPLS labeled packets, use the platform qos-feature copp-mpls enable command.
- Due to hardware limitation, to match the control plane packets against CoPP, ACL rules that match with IP addresses should be added, since adding generic ACL rules with any any matches both the data plane and control plane traffic.

IP Access List Overview

Access control lists (ACLs) perform packet filtering to control which packets move through the network and where. Such control provides security by helping to limit network traffic, restrict the access of users and devices to the network, and prevent traffic from leaving a network. IP access lists can reduce the chance of spoofing and denial-of-service attacks and allow dynamic, temporary user access through a firewall.

IP access lists can also be used for purposes other than security, such as bandwidth control, restricting the content of routing updates, redistributing routes, triggering dial-on-demand (DDR) calls, limiting debug output, and identifying or classifying traffic for quality of service (QoS) features. This module provides an overview of IP access lists.

Benefits

Improved Traffic Flow

This feature improves the Turbo ACL processing process in PXF by more expediently removing older entries. As a result, more Turbo ACL processing can be done in the PXF processing path, thereby allowing more router traffic to be accelerated using the PXF processing path.

Configuration of Route Processor Memory Limits for ACL Processing

This feature allows users to set the amount of memory reserved for ACL processes (such as compilation, storage, and classification) in the RP path. Users who need more memory for ACL processes now have the ability to set aside additional memory resources in the RP path for ACL processes. Users who need more more memory for other processes in the RP path now can set aside less memory for ACL processes.

Benefits of IP Access Lists

Access control lists (ACLs) perform packet filtering to control the flow of packets through a network. Packet filtering can restrict the access of users and devices to a network, providing a measure of security. Access lists can save network resources by reducing traffic. The benefits of using access lists are as follows:

- Authenticate incoming rsh and rcp requests—Access lists can simplify the identification of local users, remote hosts, and remote users in an authentication database that is configured to control access to a device. The authentication database enables Cisco software to receive incoming remote shell (rsh) and remote copy (rcp) protocol requests.
- Block unwanted traffic or users—Access lists can filter incoming or outgoing packets on an interface, thereby controlling access to a network based on source addresses, destination addresses, or user authentication. You can also use access lists to determine the types of traffic that are forwarded or blocked

at device interfaces. For example, you can use access lists to permit e-mail traffic to be routed through a network and to block all Telnet traffic from entering the network.

- Control access to vty—Access lists on an inbound vty (Telnet) can control who can access the lines to a device. Access lists on an outbound vty can control the destinations that the lines from a device can reach.
- Identify or classify traffic for QoS features—Access lists provide congestion avoidance by setting the IP precedence for Weighted Random Early Detection (WRED) and committed access rate (CAR). Access lists also provide congestion management for class-based weighted fair queueing (CBWFQ), priority queueing, and custom queueing.
- Limit debug command output—Access lists can limit debug output based on an IP address or a protocol.
- Provide bandwidth control—Access lists on a slow link can prevent excess traffic on a network.
- Provide NAT control—Access lists can control which addresses are translated by Network Address Translation (NAT).
- Reduce the chance of DoS attacks—Access lists reduce the chance of denial-of-service (DoS) attacks. Specify IP source addresses to control traffic from hosts, networks, or users from accessing your network. Configure the TCP Intercept feature to can prevent servers from being flooded with requests for connection.
- Restrict the content of routing updates—Access lists can control routing updates that are sent, received, or redistributed in networks.
- Trigger dial-on-demand calls—Access lists can enforce dial and disconnect criteria.

IP Address Range-Based Filtering Support for CoPP ACL

IP Access Control Lists are a set of rules that perform packet filtering to control the flow of packets through a network. Packet filtering provides security by the following features:

- Limiting the access of traffic into a network.
- Restricting user and device access to a network.
- Preventing traffic from leaving a network.
- Reduce the chance of spoofing and denial-of-service attacks.

Table 1: Feature History Table

Feature Name	Release Information	Description
IP Address Range-Based Filtering Support for CoPP ACL	Cisco IOS XE Bengaluru 17.5.1	The CoPP ACL Template feature supports Ingress on In-band Management Loopback interface and Ingress on Data plane interface to block traffic using MPLS. CoPP ACL supports Source IP based filtering on the Cisco router.

Prior to the Cisco IOS XE Bengaluru 17.5.1 release, IP address Range-Based Filtering for CoPP ACL was not supported. Effective Cisco IOS XE Bengaluru 17.5.1 this feature enables you to securely manage MPLS traffic by supporting the following requirements:

- Ingress on In-Band Management Loopback interface.
- Ingress on Data plane interface to block MGMT Traffic on MPLS.

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.

Procedure

Step 1 enable

Example:

```
Device> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 configure terminal

Example:

```
Device# configure terminal
```

Enters global configuration mode.

Step 3 control-plane

Example:

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

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

Step 4 service-policy [input |output] 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 end

Example:

```
Device(config-cp)# end
```

(Optional) Returns to privileged EXEC mode.

Verifying Control Plane Services

Procedure

Step 1 enable

Example:

```
Device> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 show policy-map control-plane [all] [input |output [class class-name]]

Example:

```
Device# show policy-map control-plane all
```

Displays information about the control plane.

- all—(Optional) Displays service policy information about all QoS policies used on the CP.
- input—(Optional) Displays statistics for the attached input policy.
- class class-name—(Optional) Specifies the name of the traffic class whose configuration and statistics are displayed.

Step 3 exit

Example:

```
Device# exit
```

(Optional) Exits privileged EXEC mode.

Examples

The following example shows that the policy map TEST is associated with the control plane.

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.

Procedure

Step 1 enable

Example:

```
Device> enable
```

Enables privileged EXEC mode.

Step 2 configure terminal

Example:

```
Device# configure terminal
```

Enters global configuration mode.

Step 3 access-list access-list-number permit protocol {tcd | udp} {any | host {source-addr | name}} eq port number {any | host {source-addr | name}} eq port number

Example:

Configures an access list for filtering frames by UDP protocol and matches only packets with a given port number.

Step 4 class-map [match-any | match-all | type] class-map-name

Example:

```
Device(config)# class-map match-any MyClassMap
```

Creates a class-map and enters QoS class-map configuration mode.

Step 5 match access-group [access-list-index | access-group-name]

Example:

```
Device(config-cmap)# match access-group 111
```

Specifies access groups to apply to an identity policy. The range of valid values is 1-2799.

Step 6 exit

Example:

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

Exits QoS class-map configuration mode and returns to global configuration mode.

Step 7 policy-map policy-map-name

Example:

```
Device(config)# policy-map Policy1
```

Specifies a service policy and enters QoS policy-map configuration mode.

Step 8 class [class-map-name | class-default]

Example:

```
Device(config-pmap)# class MyClassMap
```

Enters QoS policy-map class configuration more

Step 9 police {rate-bps | cir {cir-bps | percent percent}} [bc burst-bytes] [conform-action | exceed-action | violate-action]action] [ ]

Example:

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 10000000000. 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 10000000000. Supply an optional postfix (K, M, G). Decimal point is allowed.
- be burst-bytes—(Optional) Specifies the conformed burst (be) 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 percent option is not supported on the router.

Step 10 exit

Example:

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

Exits policy-map class police configuration mode

Step 11 exit

Example:

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

Exits policy-map class configuration mode

Step 12 exit

Example:

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

Exits policy-map configuration mode

Step 13 control-plane

Example:

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

Enters control plane configuration mode.

Step 14 service-policyinput policy-map-name

Example:

```
Device(config-cp)# service-policy input Policy1
```

Attaches a policy map to a control plane.

Step 15 exit

Example:

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

Exits control plane configuration mode and returns to global configuration mode.

Step 16 exit

Example:

```
Device(config)# exit
```

Exits global configuration mode returns to privileged EXEC mode.

Configuring CoPP ACL

Before you begin

- To filter MPLS labelled packets, use the **platform qos-feature copp-mpls enable** command.

Procedure

	Command or Action	Purpose
Step 1	enable **Example:** `Device> enable`	Enter privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal **Example:** `Router# configure terminal`	Enter global configuration mode.
Step 3	platform qos-feature copp-mpls enable **Example:** `Router(config)#platform qos-feature copp-mpls enable`	Configure the CoPP MPLS command on the Cisco Router.
Step 4	exit **Example:** `Router(config)#exit`	Exit global configuration mode.

Verifying CoPP ACL

The following example shows how to verify the CoPP ACL on the Cisco Router.

```
Router(config)#sdm prefer enable_acl_copp
COPP ACL template change.
Current template = disable_acl_copp
Updated template = enable_acl_copp
Standby is reloaded, it will come up with in it required for new template
once standby comes up Please trigger SSO
```

Configuration Examples for Control Plane Policing

Example: Configuring Control Plane Policing on Input Telnet Traffic

The following example shows how to apply a QoS policy for aggregate control plane services to Telnet traffic that is received on the control plane. Trusted hosts with source addresses 10.1.1.1 and 10.1.1.2 forward Telnet packets to the control plane but are still policed for a maximum rate.

All remaining Telnet packets are dropped by the control-plane.

```
! Define trusted host traffic.
DEVICE(config)#ip access-list extended telnet-trust
DEVICE(config-ext-nacl)#10 permit tcp host 10.1.1.1 any eq telnet
DEVICE(config-ext-nacl)#20 permit tcp host 10.1.1.2 any eq telnet
DEVICE(config-ext-nacl)#exit

! Define all other Telnet traffic.
DEVICE(config)#ip access-list extended telnet-drop
DEVICE(config-ext-nacl)#10 permit tcp any any eq telnet
DEVICE(config-ext-nacl)#exit

! Define class map for trusted hosts
DEVICE(config)#class-map match-all copp-trust
DEVICE(config-cmap)#match access-group name telnet-trust
DEVICE(config-cmap)#exit

! Define class map for un-trusted hosts
DEVICE(config)#class-map match-all copp-drop
DEVICE(config-cmap)#match access-group name telnet-drop
DEVICE(config-cmap)#exit

! Define the policy-map for both type of hosts
DEVICE(config)#policy-map control-plane-in
DEVICE(config-pmap)#class copp-trust
DEVICE(config-pmap-c)#police 1000000 conform-action transmit  exceed-action drop
DEVICE(config-pmap-c-police)#class copp-drop
DEVICE(config-pmap-c-police)#exit
DEVICE(config-pmap-c)#police 1000000 conform-action drop  exceed-action drop
DEVICE(config-pmap-c-police)#exit
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

Related Documents

Related Topic	Document Title
Cisco IOS commands	https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mcl/allreleasemcl/all-book.html

Standards and RFCs

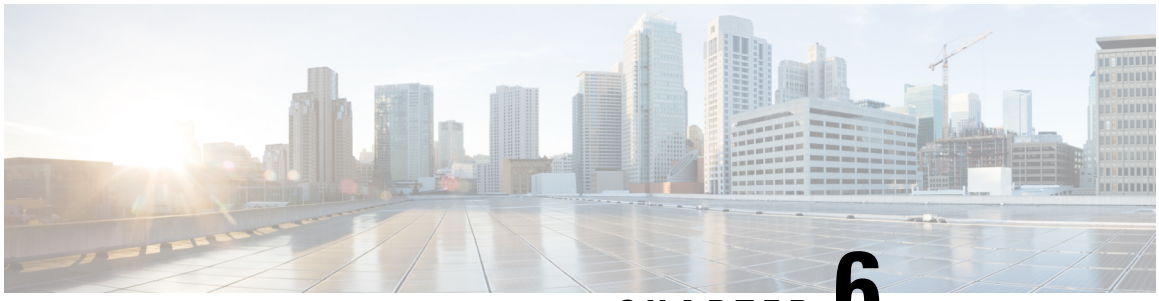
Standard/RFC	Title
No specific Standards and RFCs are supported by the features in this document.	—

MIBs

MIB	MIBs Link
—	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

Description	Link
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. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html



CHAPTER 6

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.

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

- Restrictions for Priority Shaper, on page 49
- Configuring Priority Shaper, on page 49

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 burstiness 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.

Procedure

Step 1 enable

Example:

```
Device> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 configure terminal

Example:

```
Device# configure terminal
```

Enters global configuration mode.

Step 3 class-map class-map-name

Example:

```
Device(config)#class-map class_priority
```

Configures class map and specifies the name of the class map to be created.

Step 4 match cos number

Example:

```
Device(config-cmap)# match cos 1
```

Matched different PHBs for different class maps.

Step 5 policy-map policy-map-name

Example:

```
Device(config)#policy-map shape_priority
```

Configures the policy map.

Step 6 class class-map-name

Example:

```
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. This class is associated with the class map that is created earlier.

Step 7 priority level <level 1/2 > percent <percentage 1-100 > or priority level <level 1/2> <kbps> <burst size>

Example:

```
Device(config-pmap-c)# priority <1-10000000> Kilo Bits per second
Device(config-pmap-c)# priority Percent <1-100>
Device(config-pmap-c)# priority level <1-2> <1-10000000> Kilo Bits per second
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.

Step 8 interface interface-type interface-number

Example:

```
Device(config)# interface gigabitethernet 0/0/1
```

Specifies the port to attach to the policy map and allows to enter the interface configuration mode. Valid interfaces are physical ports.

Step 9 service-policy output policy-map-name

Example:

```
Device(config-if)# service instance 1 ethernet
Device(config-if-srv)# service-policy output shape_priority
```

Applies output policy to the interface.

Note You can also attach the service policy over the service instance.

Step 10 end

Example:

```
Device(config)#end
```

Returns to privileged EXEC mode.

Configuration Examples for Priority Shaper

This section shows sample configurations for Priority Shaper.

Example: Configuring Priority Shaper

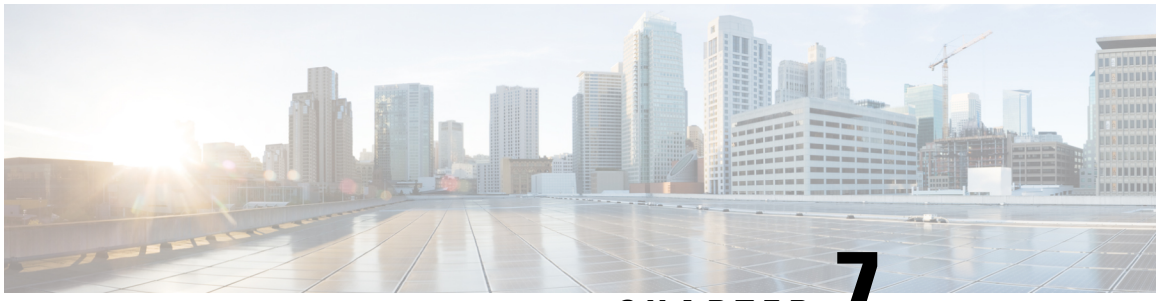
The following is a sample configuration for priority shaper.

```
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
```

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
```



CHAPTER 7

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.

- Prerequisites for Hierarchical Color-Aware Policing, on page 53
- Restrictions for Hierarchical Color-Aware Policing, on page 53
- Information About Hierarchical Color-Aware Policing, on page 55
- How to Configure Hierarchical Color-Aware Policing, on page 58
- Configuration Examples for Hierarchical Color-Aware Policing, on page 61
- Additional References, on page 62

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 47 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-mapclass-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-colorclass-map-name or no exceed-colorclass-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.

- 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.
- When a parent has a color-aware policy, packets to the parent take the color marking of the child policer.

  The colors for a parent policy using a single rate, three color-policer (1r3c) or dual rate three color-policer (2r3c) scheme are:

  · green for conform-action

  · yellow for exceed-action

  · red for violate-action.

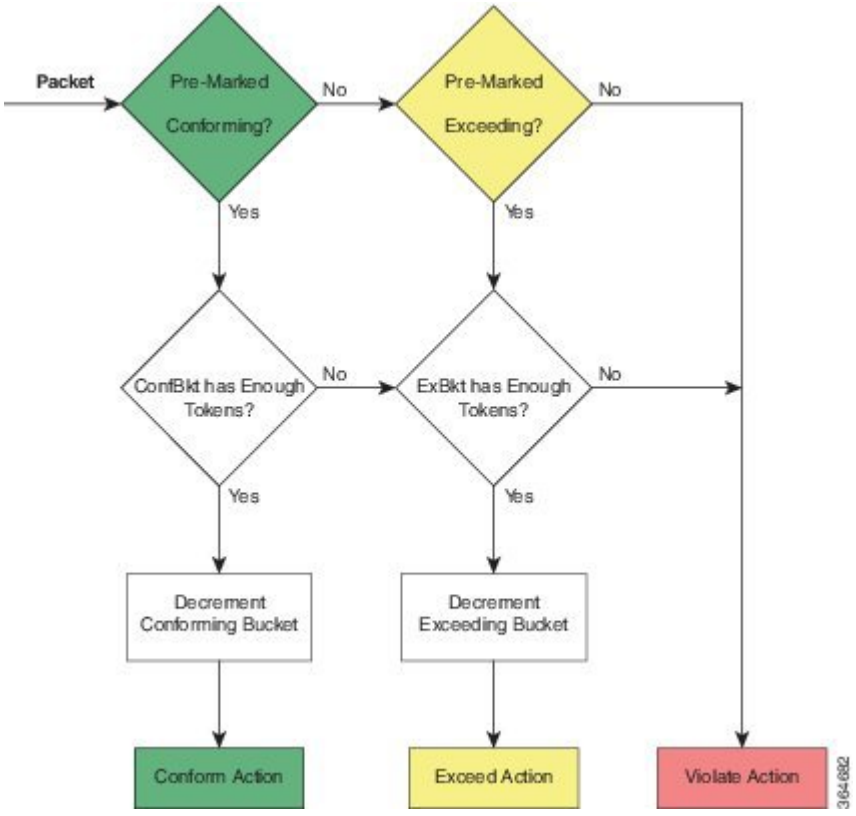
  However, the policer at the child level only supports single rate, two color-policer (1r2c) scheme, and the colors are green for conform-action, and red for exceed-action.

  So, even if the exceed action of a child policer is 'transmit', all exceed (red) packets from the child policer will always fall into the red bucket of the parent.

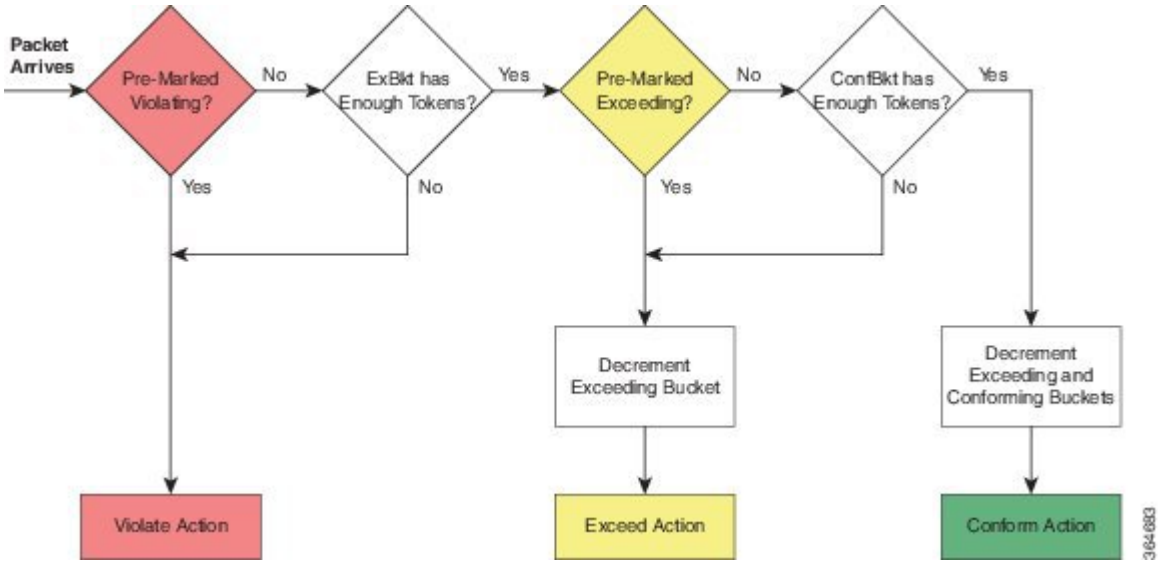
  You must, therefore, ensure that the conform-color and exceed-color classes together form a superset of the respective class matches so as to avoid packets being treated as red and therefore, being dropped.

  See the following images for more information.

  Single-Rate, Color-Aware, Three-Color Policer



  Dual-Rate, Color-Aware, Three-Color Policer



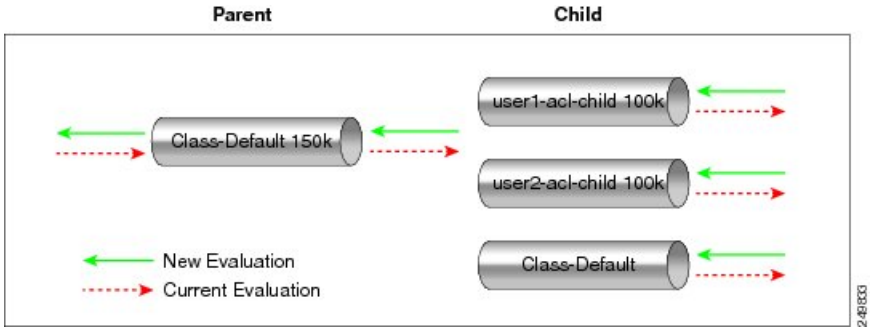
Information About Hierarchical Color-Aware Policing

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
```

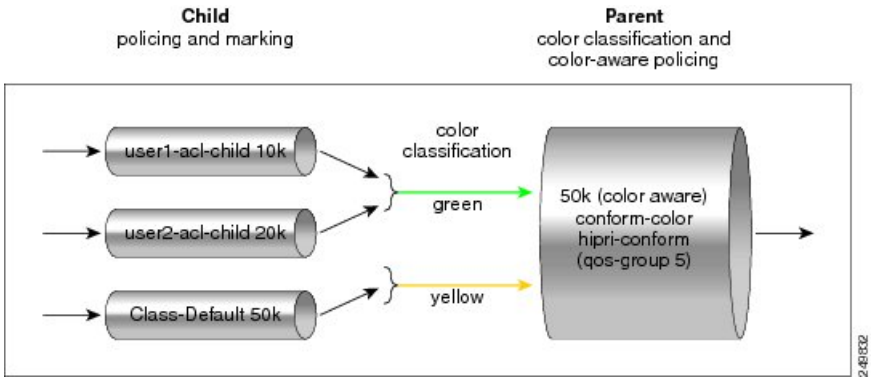


Limited Color-Aware Policing

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

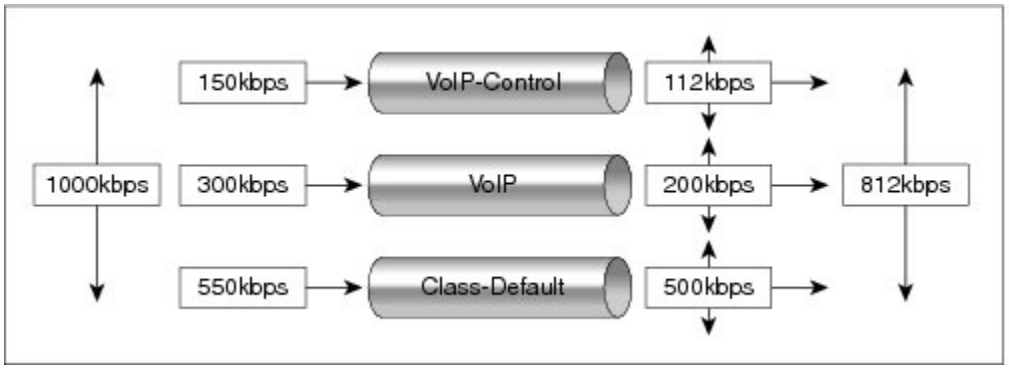


Note To avoid drops at the parent level for "conformed" child traffic, the parent policer must have a rate and burst that are equal to or greater than the sum of the child conform rates and burst sizes. There is no check for inappropriate (parent-to-child) rates and burst sizes in code. You must be aware 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

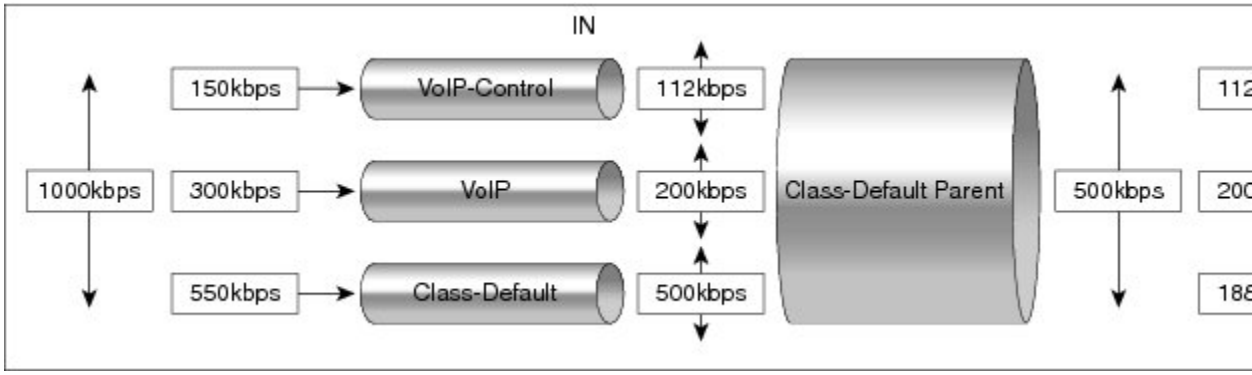
Prior to the release of the Hierarchical Color-Aware Policing feature, policing and marking were typically used as input QoS options. For example, a voice customer was limited to 112 kb/s for voice control and 200 kb/s for voice traffic. The class-default class has no policer. The only limit is the physical 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 188kb/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

Procedure

	Command or Action	Purpose
Step 1	enable **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	policy-map policy-map-name **Example:** `Router(config)# policy-map child-policy`	Enters policy-map configuration mode and creates a policy map.
Step 4	class {class-name | class-default} **Example:** `Router(config-pmap)# class user1-acl-child`	Enters policy-map class configuration mode. 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

	Command or Action	Purpose
		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	conform-color class-map-name [exceed-color class-map-name] **Example:** `Router(config-pmap-c-police)# conform-color c1 exceed-color c2`	Enables color-aware traffic policing and creates the conform-color and exceed-color class-maps used for color-aware traffic policing. 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	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]
	Example:
	`Router(config-pmap-c)# police 10000 bc 1500`
	Example:
	`Router(config-pmap-c-police)# conform-action set-qos-transmit 5`
		Configures traffic policing and specifies multiple actions applied to packets marked as conforming to, exceeding, or violating a specific rate.
		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.
		• exceed-action—(Optional) Action to take on packets whose rate is within the conform and conform plus exceed burst.
		• violate-action—(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.
		• conform-color—(Optional) Enables color-aware policing (on the policer being configured) and assigns the class map to be used for conform color determination. The hipri-conform keyword is the class map (previously configured via the class-map command) to be used.
		• exceed-color—(Optional) Enables color-aware policing (on the policer being

	Command or Action	Purpose
		configured) and assigns the class map to be used for exceed color determination. The lipri-exceed keyword is the class map (previously configured via the class-map command) to be used.
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.

Example

The following is a sample configuration for 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
```

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:

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 0000 bps, exceed 0000 bps, violate 0000 bps
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
police:
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

Related Topic	Document Title
Cisco IOS commands	https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mcl/allreleasemcl/all-book.html

Standards and RFCs

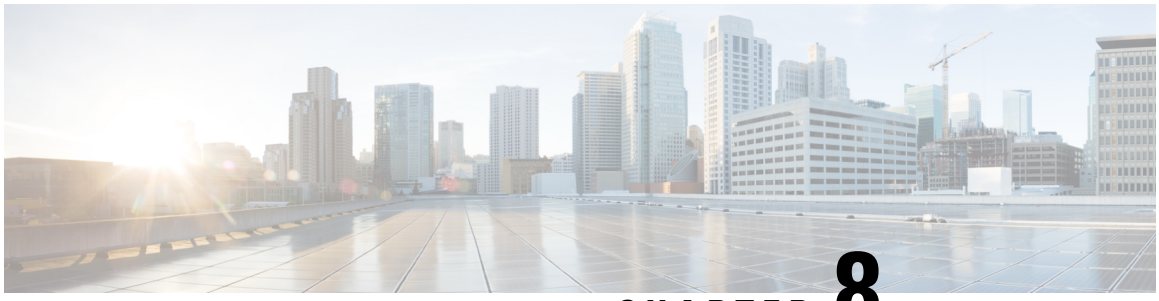
Standard/RFC	Title
No specific Standards and RFCs are supported by the features in this document.	—

MIBs

MIB	MIBs Link
—	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

Description	Link
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. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html



CHAPTER 8

QoS Overhead Accounting

Overhead accounting enables the router to account for packet overhead when shaping traffic to a specific rate. This accounting ensures that the router executes quality of service (QoS) features on the actual bandwidth that is used by subscriber traffic.

The overhead accounting feature enables the router to account for downstream Ethernet frame headers when applying shaping to packets. The traffic scheduler allows a minimum amount of value more than the configured rate at the port, in addition to the excess bytes configured on that port.

- Restrictions for QoS Overhead Accounting, on page 65
- OH Accounting Support for L3VPN, on page 66
- How to Configure QoS Overhead Accounting, on page 67
- Applying Overhead Accounting on a Particular Interface, on page 67
- Configuring Number of Bytes to be Accounted, on page 67
- Configuring Overhead Accounting for MPLS Imposition, on page 67
- Verifying Overhead Accounting compensation, on page 67
- Apply OH Accounting on a Particular L3VPN Interface, on page 68
- Configure Number of Bytes to be Accounted, on page 68
- Verify OH Accounting Compensation, on page 68

Restrictions for QoS Overhead Accounting

- Accounting feature is supported only for the following scenarios:
  - MPLS imposition
  - MPLS disposition
- Accounting feature can be enabled per interface and only one value of compensation bytes can be configured globally.
- The feature is applied in the following scenarios:
  - Per interface QoS overhead accounting can take effect only during a policy-map detach or attach process.
  - Any dynamic modification, for example, enabling or disabling on an interface or change in global compensation bytes can reflect per interface only after a policy-map detach or attach process.

- Already configured policy-map on the accounting enabled interface needs to be detached and reattached.

- While detaching, ensure to perform the following tasks:
  - Detach the policy-map per interface.
  - Disable the accounting feature for that interface.
  - Re-attach the policy-map based on the requirement.

- QoS overhead accounting is not supported for port channel interface and member links.
- QoS overhead accounting is not supported for trunk EFPs on an interface.
- Accounting is not supported if interface has Ethernet loopback that is enabled.

OH Accounting Support for L3VPN

Table 2: Feature History

Feature Name	Release Information	Feature Description
OH Accounting Support for L3VPN	Cisco IOS XE Cupertino 17.7.1	This feature enables OverHead (OH) accounting support for L3VPN traffic. This feature adds a header value and helps to match the Tx and Rx rates during a packet transfer.

Prior to Cisco IOS XE Cupertino release 17.7.1, OverHead (OH) accounting was only supported for native IP traffic and L2VPN.

Starting with Cisco IOS XE Cupertino release 17.7.1, OH accounting is also supported for L3VPN traffic. When a minimal packet size is transferred, the Transmission Traffic (Tx) rate gets reduced and you receive a reduced Receiving Traffic (Rx) rate. You do not experience any packet drop and this phenomenon is referred to as header compression.

This feature adds a header value to match the Tx and Rx rates. The header value or compensation range is from —48 to +48 bytes. Thus, it is useful when the traffic rate is calcuated based on the Tx and Rx rates.

Note The restrictions for layer 2 OH accounting also apply to layer 3 OH accounting.

How to Configure QoS Overhead Accounting

Applying Overhead Accounting on a Particular Interface

To apply overhead accounting on a particular interface, for example layer 2 interface and MPLS disposition, enter the following commands:

```
Router> enable
Router# configure terminal
Router(config)# qos-overhead-accounting enable gi 0/0/0
```

Configuring Number of Bytes to be Accounted

To configure the number of bytes that need to be accounted, enter the following commands:

```
Router> enable
Router# configure terminal
Router(config)# qos-overhead-accounting positive 8
```

Configuring Overhead Accounting for MPLS Imposition

To configure compensation for the MPSL imposition with access interface as gig 0/0/0 and core port as gig 0/0/1, enter the following steps:

```
Router> enable
Router# configure terminal
Router(config)# qos-overhead-accounting enable gi 0/0/1
Router(config)# qos-overhead-accounting positive 8
Router(config)# qos-overhead-accounting enable gi 0/0/0
```

To disable the compensation, enter the following commands:

```
Router> enable
Router# configure terminal
Router(config)#no qos-overhead-accounting enable gi 0/0/1
Router(config)#no qos-overhead-accounting enable gi 0/0/0
```

Verifying Overhead Accounting compensation

Use the following show command to display the set of interfaces on which overhead accounting is enabled:

```
Router#show platform hardware pp active feature qos oh-accounting interface all
Overhead Accounting Target Info
Interface Name                  GID    Status    Bytes (Shadow)   Bytes (Actual)
-------------------------------------------------------------------------------
```

```
GigabitEthernet0/0/0            269    Enabled    8                8
```

Apply OH Accounting on a Particular L3VPN Interface

To apply overhead accounting on a particular L3VPN interface:

```
Router> enable
Router# configure terminal
Router(config)# qos-overhead-accounting enable gi 0/0/0
```

Configure Number of Bytes to be Accounted

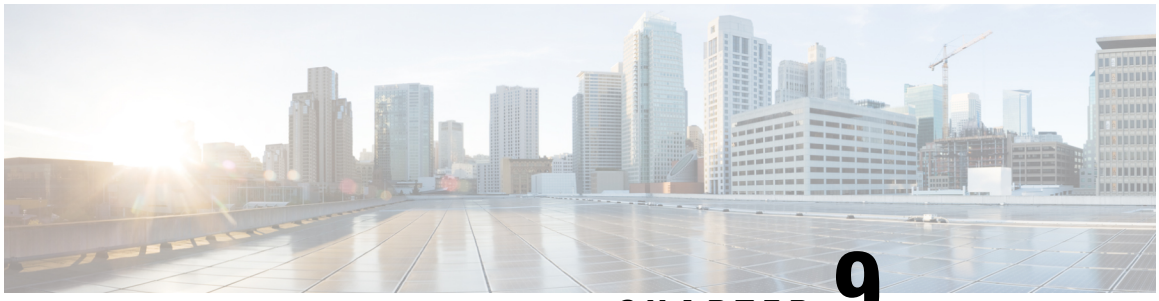
To configure the number of bytes to be accounted for the L3VPN interface:

```
Router> enable
Router# configure terminal
Router(config)# qos-overhead-accounting positive/negative value
```

Verify OH Accounting Compensation

Use the following show command to display the set of L3VPN interfaces on which overhead accounting is enabled:

```
Router#show platform hardware pp active feature qos oh-accounting interface all
Overhead Accounting Target Info
Interface Name                  GID    Status    Bytes (Shadow)   Bytes (Actual)
-------------------------------------------------------------------------------
GigabitEthernet0/0/0            269    Enabled    8                8
```



CHAPTER 9

Policer Adjustment in QoS Policy Map

Policers are configured usually at a value range of 64,000–10 G whereas the hardware policer is programmed only to discrete value. The policer rate received is less than that of the configured CIR and PIR values. The policer adjustment feature is added to adjust the CIR and PIR values of hardware policer either to match the configured value or to the next higher value available in hardware.

The policer adjustment feature is supported on the RSP2 module.

To enable policer adjustment, use the platform qos-adjust-policer enable at the global configuration mode for a table map. You can view the show platform hardware pp active feature QoS interface command to compare the configured values of CIR and PIR values in the qos-policy and the actual programmed values in hardware.

With the policer adjustment feature, the policer rate is compensated with + 0 to + 0.5 to the configured policer rate so that you can achieve the received rate more than or equal to that of the configured rate.

- Restrictions for Policer Adjustment, on page 69
- How to configure Policer Adjustment, on page 70

Restrictions for Policer Adjustment

- Policy adjustment is performed at a global configuration level and it is not supported on each port or EFP.
- Detaching and attaching of policer from ports after applying the policy adjustment feature at a global configuration works for applied ports. For the remaining ports to which detaching and attaching is not performed after enabling the policy adjustment works in a legacy QoS functionality manner.
- Policer enhancement is supported on EFP, TEFP, routed port, and port channel.
- BC or BE values are not adjusted, and only CIR and PIR or EIR are adjusted. Even if BC or BE values are configured, the values that are displayed in the show command do not match exactly with IOS values.
- CIR rates 64,000–3,00,000 can have rates more than 0.5 percent as this rate limits to already available percent and effects higher rates.

How to configure Policer Adjustment

Enabling Policer Adjustment

To enable a policer adjustment at the global configuration mode, enter the following command:

```
Router> enable
Router# configure terminal
Router(config)# platform qos-adjust-policer enable
```

After enabling the policer adjustment, you must detach and attach the policer from port, then only the feature is applied on the port.

Disabling Policer Adjustment

To disable the policer adjustment globally, enter the no form of the following command:

```
{no} platform qos-adjust-policer enable
```

After disabling the policer adjustment, you need to detach and attach the existing policy-map from the port or service and then only the policer adjustment is disabled.

Verifying Policer Adjustment

Use the following **show platform hardware pp active feature QoS interface {intf_name} {service-instance} {EVC_num} input/ouput** command to view the configured and programmed policer values:

```
Router# show platform hardware pp active feature qos interface te 0/0/13 ser 2 in

Policy details:

Interface: TenGigabitEthernet0/0/13
Policy: TMO-EVC
Service instance number: 2
Direction: input
------------------------------------------------------------------
Class: EVC, Level: 2
Policer Mode: IETF_2R3C
Policer Index Id: 33
Policer Profile Id: 12
Policer feature         Software value             Asic value
CIR                        5000000 kbps             5062500 kbps
PIR                        7000000 kbps                  NA
EIR (PIR - CIR)            2000000 kbps             2024884 kbps
BC                         2500000 bytes            2500000 bytes
BE                        16000000 bytes           16000000 bytes
```