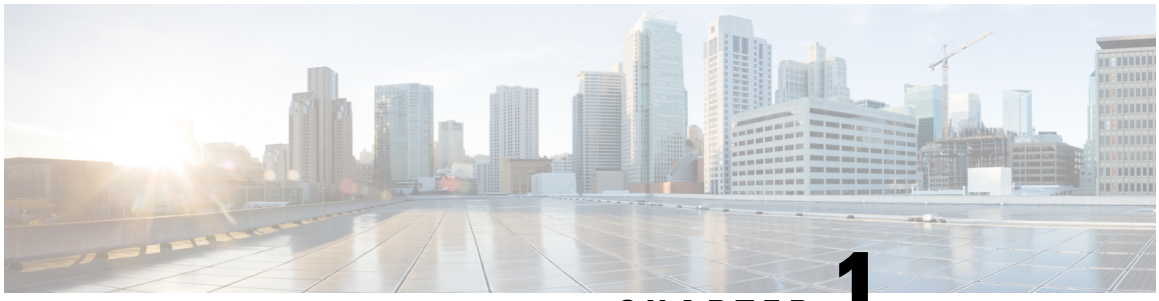
QoS: Policing and Shaping Configuration Guide, Cisco IOS XE Fuji 16.9.x

First Published: 2016-03-16

Last Modified: 2018-07-19

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

CONTENTS



CHAPTER 1

Read Me First

Important Information about Cisco IOS XE 16

Effective Cisco IOS XE Release 3.7.0E (for Catalyst Switching) and Cisco IOS XE Release 3.17S (for Access and Edge Routing) the two releases evolve (merge) into a single version of converged release—the Cisco IOS XE 16—providing one release covering the extensive range of access and edge products in the Switching and Routing portfolio.

Feature Information

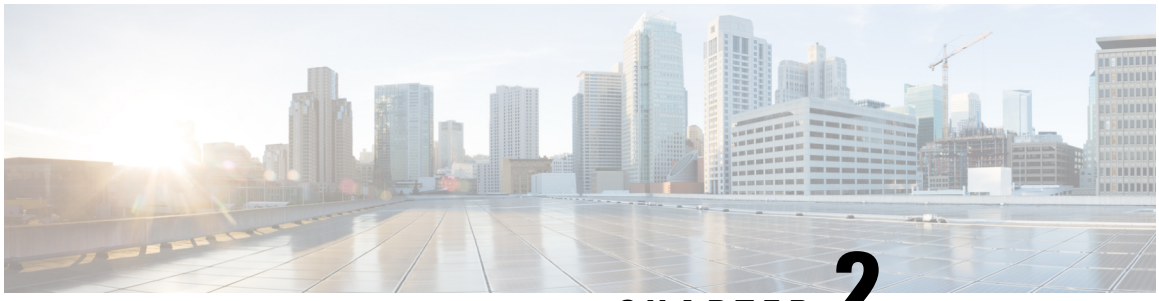
Use Cisco Feature Navigator to find information about feature support, platform support, and Cisco software image support. An account on Cisco.com is not required.

Related References

- Cisco IOS Command References, All Releases

Obtaining Documentation and Submitting a Service Request

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.



CHAPTER 2

Policing and Shaping Overview

Cisco IOS XE QoS offers two kinds of traffic regulation mechanisms--policing and shaping.

You can deploy these traffic regulation mechanisms (referred to as policers and shapers) throughout your network to ensure that a packet, or data source, adheres to a stipulated contract and to determine the QoS to render the packet. Both policing and shaping mechanisms use the traffic descriptor for a packet--indicated by the classification of the packet--to ensure adherence and service.

Policers and shapers usually identify traffic descriptor violations in an identical manner. They usually differ, however, in the way they respond to violations, for example:

- A policer typically drops traffic, but it can also change the setting or "marking" of a packet. (For example, a policer will either drop the packet or rewrite its IP precedence, resetting the type of service bits in the packet header.)
- A shaper typically delays excess traffic using a buffer, or queueing mechanism, to hold packets and shape the flow when the data rate of the source is higher than expected. (For example, Class-Based Shaping uses a weighted fair queue to delay packets in order to shape the flow.)

Traffic shaping and policing can work in tandem. For example, a good traffic shaping scheme should make it easy for nodes inside the network to detect misbehaving flows. This activity is sometimes called policing the traffic of the flow.

This chapter gives a brief description of the Cisco IOS XE QoS traffic policing and shaping mechanisms. Because policing and shaping both use the token bucket mechanism, this chapter first explains how a token bucket works. This chapter includes the following sections:

What Is a Token Bucket

A token bucket is a formal definition of a rate of transfer. It has three components: a burst size, a mean rate, and a time interval (Tc). Although the mean rate is generally represented as bits per second, any two values may be derived from the third by the relation shown as follows:

```
mean rate = burst size / time interval
```

Here are some definitions of these terms:

- Mean rate--Also called the committed information rate (CIR), it specifies how much data can be sent or forwarded per unit time on average.
- Burst size--Also called the Committed Burst (Bc) size, it specifies in bits (or bytes) per burst, how much traffic can be sent within a given unit of time to not create scheduling concerns. (For a shaper, such as GTS, it specifies bits per burst; for a policer, such as CAR, it specifies bytes per burst, per second.)
- Time interval--Also called the measurement interval, it specifies the time quantum in seconds per burst.

By definition, over any integral multiple of the interval, the bit rate of the interface will not exceed the mean rate. The bit rate, however, may be arbitrarily fast within the interval.

A token bucket is used to manage a device that regulates the data in a flow. For example, the regulator might be a traffic policer, such as CAR, or a traffic shaper, such as FRTS or GTS. A token bucket itself has no discard or priority policy. Rather, a token bucket discards tokens and leaves to the flow the problem of managing its transmission queue if the flow overdrives the regulator. (Neither CAR nor FRTS and GTS implement either a true token bucket or true leaky bucket.)

In the token bucket metaphor, tokens are put into the bucket at a certain rate. The bucket itself has a specified capacity. If the bucket fills to capacity, newly arriving tokens are discarded. Each token is permission for the source to send a certain number of bits into the network. To send a packet, the regulator must remove from the bucket a number of tokens equal in representation to the packet size.

If not enough tokens are in the bucket to send a packet, the packet either waits until the bucket has enough tokens (in the case of GTS) or the packet is discarded or marked down (in the case of CAR). If the bucket is already full of tokens, incoming tokens overflow and are not available to future packets. Thus, at any time, the largest burst a source can send into the network is roughly proportional to the size of the bucket.

Note that the token bucket mechanism used for traffic shaping has both a token bucket and a data buffer, or queue; if it did not have a data buffer, it would be a policer. For traffic shaping, packets that arrive that cannot be sent immediately are delayed in the data buffer.

For traffic shaping, a token bucket permits burstiness but bounds it. It guarantees that the burstiness is bounded so that the flow will never send faster than the token bucket's capacity, divided by the time interval, plus the established rate at which tokens are placed in the token bucket. See the following formula:

```
(token bucket capacity in bits / time interval in seconds) + established rate in bps =
maximum flow speed in bps
```

This method of bounding burstiness also guarantees that the long-term transmission rate will not exceed the established rate at which tokens are placed in the bucket.

Traffic Policing

Traffic policing allows you to control the maximum rate of traffic sent or received on an interface and to partition a network into multiple priority levels or class of service (CoS).

Traffic policing manages the maximum rate of traffic through a token bucket algorithm. The token bucket algorithm can use the user-configured values to determine the maximum rate of traffic allowed on an interface at a given moment in time. The token bucket algorithm is affected by all traffic entering or leaving (depending on where the traffic policy with traffic policing is configured) and is useful in managing network bandwidth when several large packets are sent in the same traffic stream.

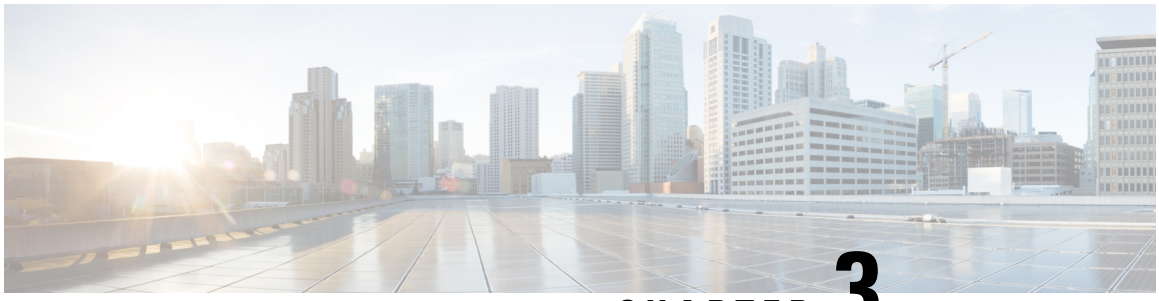
The token bucket algorithm provides users with three actions for each packet: a conform action, an exceed action, and an optional violate action. Traffic that is entering the interface with Traffic Policing configured

is placed in to one of these categories. Within these three categories, users can decide packet treatments. For instance, packets that conform can be configured to be transmitted, packets that exceed can be configured to be sent with a decreased priority, and packets that violate can be configured to be dropped.

Traffic policing is often configured on interfaces at the edge of a network to limit the rate of traffic that is entering or leaving the network. In the most common traffic policing configurations, traffic that conforms is transmitted and traffic that exceeds is sent with a decreased priority or is dropped. Users can change these configuration options to suit their network needs.

Traffic Shaping to Regulate Packet Flow

Regulating the packet flow (that is, the flow of traffic) on the network is also known as traffic shaping. Traffic shaping allows you to control the speed of traffic that is leaving an interface. This way, you can match the flow of the traffic to the speed of the interface receiving the packet.



CHAPTER 3

IPv6 QoS: MQC Traffic Shaping

Traffic shaping allows you to limit the packet dequeue rate by holding additional packets in the queues and forwarding them as specified by parameters configured for traffic shaping features

Finding Feature Information

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

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

Information About IPv6 QoS: MQC Traffic Shaping

Implementation Strategy for QoS for IPv6

IPv6 packets are forwarded by paths that are different from those for IPv4. QoS features supported for IPv6 environments include packet classification, queuing, traffic shaping, weighted random early detection (WRED), class-based packet marking, and policing of IPv6 packets. These features are available at both the process switching and Cisco Express Forwarding switching paths of IPv6.

All of the QoS features available for IPv6 environments are managed from the modular QoS command-line interface (MQC). The MQC allows you to define traffic classes, create and configure traffic policies (policy maps), and then attach those traffic policies to interfaces.

To implement QoS in networks that are running IPv6, follow the same steps that you would follow to implement QoS in networks running only IPv4. At a very high level, the basic steps for implementing QoS are as follows:

- Know which applications in your network need QoS.

- Understand the characteristics of the applications so that you can make decisions about which QoS features would be appropriate.
- Know your network topology so that you know how link layer header sizes are affected by changes and forwarding.
- Create classes based on the criteria that you establish for your network. In particular, if the same network is also carrying IPv4 traffic along with IPv6 traffic, decide if you want to treat both of them the same way or treat them separately and specify match criteria accordingly. If you want to treat them the same, use match statements such as **match precedence**, **match dscp**, **set precedence**, and **set dscp**. If you want to treat them separately, add match criteria such as **match protocol ip** and **match protocol ipv6** in a match-all class map.
- Create a policy to mark each class.
- Work from the edge toward the core in applying QoS features.
- Build the policy to treat the traffic.
- Apply the policy.

Traffic Policing in IPv6 Environments

Congestion management for IPv6 is similar to IPv4, and the commands used to configure queueing and traffic shaping features for IPv6 environments are the same commands as those used for IPv4. Traffic shaping allows you to limit the packet dequeue rate by holding additional packets in the queues and forwarding them as specified by parameters configured for traffic shaping features. Traffic shaping uses flow-based queueing by default. CBWFQ can be used to classify and prioritize the packets. Class-based policer and generic traffic shaping (GTS) or Frame Relay traffic shaping (FRTS) can be used for conditioning and policing traffic.

Additional References

Related Documents

Related Topic	Document Title
IPv6 addressing and connectivity	*IPv6 Configuration Guide*
Cisco IOS commands	*Cisco IOS Master Commands List, All Releases*
IPv6 commands	*Cisco IOS IPv6 Command Reference*
Cisco IOS IPv6 features	*Cisco IOS IPv6 Feature Mapping*

Standards and RFCs

Standard/RFC	Title
RFCs for IPv6	*IPv6 RFCs*

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 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

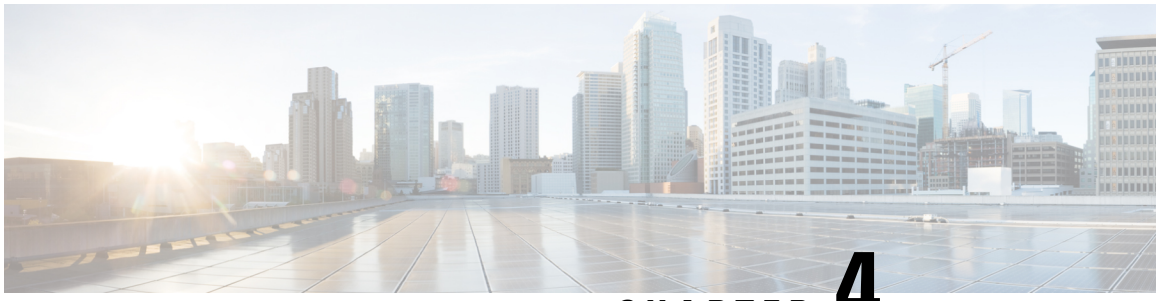
Feature Information for IPv6 QoS: MQC Traffic Shaping

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

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

Table 1: Feature Information for IPv6 QoS: MQC Traffic Shaping

Feature Name	Releases	Feature Information
IPv6 QoS: MQC Traffic Shaping	Cisco IOS XE Release 2.1	Traffic shaping allows you to limit the packet dequeue rate by holding additional packets in the queues and forwarding them as specified by parameters configured for traffic shaping features.



CHAPTER 4

Distribution of Remaining Bandwidth Using Ratio

The Distribution of Remaining Bandwidth Using Ratio feature allows service providers to configure a bandwidth-remaining ratio on subinterfaces and class queues. This ratio specifies the relative weight of a subinterface or queue with respect to other subinterfaces or queues. During congestion, the router uses this bandwidth-remaining ratio to determine the amount of excess bandwidth (unused by priority traffic) to allocate to a class of nonpriority traffic. The router allocates excess bandwidth relative to the other subinterface-level queues and class queues configured on the physical interface. By administration of a bandwidth-remaining ratio, traffic priority is not based solely on speed. Instead, the service provider can base priority on alternative factors such as service product and subscription rate.

Finding Feature Information

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

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

Prerequisites for Distribution of Remaining Bandwidth Using Ratio

Before enabling the Distribution of Remaining Bandwidth Using Ratio feature, create as many traffic classes as you need by using the class-map command.

Restrictions for Distribution of Remaining Bandwidth Using Ratio

- Bandwidth-remaining ratios can be used on outbound interfaces only.
- The bandwidth remaining ratio command cannot coexist with another bandwidth command in different traffic classes of the same policy map. For example, the following configuration is not valid and causes an error message to display:

```
policy-map Prec1
 class precedence_0
  bandwidth remaining ratio 10
 class precedence_2
  bandwidth 1000
```

- The bandwidth remaining ratio command cannot coexist with another bandwidth command in the same class. For example, the following configuration is not valid and causes an error message to display:

```
policy-map Prec1
 class precedence_0
  bandwidth 1000
  bandwidth remaining ratio 10
```

- The bandwidth remaining ratio command cannot coexist with the priority command in the same class. For example, the following configuration is not valid and causes an error message to display:

```
policy-map Prec1
 class precedence_1
  priority percent 10
  bandwidth remaining ratio 10
```

Information About Distribution of Remaining Bandwidth Using Ratio

Benefits of the Distribution of Remaining Bandwidth Using Ratio Feature

The Distribution of Remaining Bandwidth Using Ratio feature allows service providers to prioritize subscriber traffic during periods of congestion. A bandwidth-remaining ratio is used to influence how the router allocates excess bandwidth (unused by priority traffic) to a class of nonpriority traffic. Instead of using only bandwidth rate, the router considers configured minimum bandwidth rates, maximum bandwidth rates, and bandwidth-remaining ratios when determining excess bandwidth allocation. A bandwidth-remaining ratio adds more flexibility in prioritizing traffic and enables you to influence excess bandwidth allocation by basing the bandwidth-remaining ratio on factors other than speed.

With bandwidth-remaining ratios, service providers have more flexibility in assigning priority to subinterfaces and queues during congestion. In addition to speed, you can base the bandwidth-remaining ratio on alternative

factors, such as a service product or subscription rate. In this way, for example, you can give higher weight to subinterfaces that carry business services and lower weight to subinterfaces that carry residential services.

Bandwidth-Remaining Ratio Functionality

A bandwidth-remaining ratio, specified by the **bandwidth remaining ratio** command, is a value from 1 to 1000 that is used to determine the amount of unused (excess) bandwidth to allocate to a class-level queue or subinterface-level queue during congestion. The router allocates the excess bandwidth relative to the other class-level queues and subinterface-level queues configured on the physical interface. The bandwidth-remaining ratio value does not indicate a percentage. As the name implies, a ratio is used. For example, a subinterface with a bandwidth-remaining ratio of 100 receives 10 times the unused (excess) bandwidth during congestion than a subinterface with a bandwidth-remaining ratio of 10.

Without bandwidth-remaining ratios, the queueing mechanism or scheduler on the router allocates unused (excess) bandwidth equally among the classes or subinterfaces.

With bandwidth-remaining ratios, unused (excess) bandwidth allocation can be based on factors other than the bandwidth rate (for example, the service product or the subscription rate).

Using the bandwidth remaining ratio command, the bandwidth-remaining ratio can be configured differently on each subinterface or class. The bandwidth-remaining ratio can range from 1 to 1000. For example, if there are three subscribers, and the bandwidth-remaining ratios are configured as 9, 7, and 1, and if after priority traffic is served, there are 1700 kbps of excess bandwidth, the subscribers get 900 kbps, 700 kbps, and 100 kbps, respectively.

How to Configure Distribution of Remaining Bandwidth Using Ratio

You can apply bandwidth-remaining ratios to subinterfaces and/or classes queues.

Configuring and Applying Bandwidth-Remaining Ratios to Subinterfaces

Note You can apply bandwidth-remaining ratios to outbound subinterfaces only.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map** *child-policy-name*
4. **class** *class-map-name*
5. **bandwidth** *bandwidth-kbps*
6. Repeat steps 4 and 5 to configure the additional traffic classes, if needed.
7. **exit**
8. **exit**
9. **policy-map** *parent-policy-name*

10. **class class-default**
11. **bandwidth remaining ratio** *ratio*
12. **shape** {**average** | **peak**} *cir* [*bc*] [*be*]
13. **service-policy** *child-policy-name*
14. **exit**
15. **exit**
16. **interface** *type slot* / *module* / *port* **.** *subinterface* [**point-to-point** | **multipoint**]
17. **service-policy output** *parent-policy-name*
18. **end**

DETAILED STEPS

	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** *child-policy-name* **Example:** `Router(config)# policy-map Child`	Creates or modifies a child policy map and enters policy-map configuration mode. • Enter the name of the child policy map.
Step 4	**class** *class-map-name* **Example:** `Router(config-pmap)# class precedence_0`	Configures the class map and enters policy-map class configuration mode.
Step 5	**bandwidth** *bandwidth-kbps* **Example:** `Router(config-pmap-c)# bandwidth 10000`	Specifies the bandwidth, in kbps, to be allocated to this traffic class. • Enter the amount of bandwidth, in kilobits per second (kbps).
Step 6	Repeat steps 4 and 5 to configure the additional traffic classes, if needed.	
Step 7	**exit** **Example:** `Router(config-pmap-c)# exit`	Exits policy-map class configuration mode.

	Command or Action	Purpose
Step 8	**exit** **Example:** `Router(config-pmap)# exit`	Exits policy-map configuration mode.
Step 9	**policy-map** *parent-policy-name* **Example:** `Router(config)# policy-map Parent`	Creates or modifies a parent policy map and enters policy-map configuration mode. • Enter the name of the parent policy map.
Step 10	**class class-default** **Example:** `Router(config-pmap)# class class-default`	Configures the class-default class and enters policy-map class configuration mode. **Note** The router interprets any features that are configured under the class-default class as aggregate features on the subinterface.
Step 11	**bandwidth remaining ratio** *ratio* **Example:** `Router(config-pmap-c)# bandwidth remaining ratio 10`	Specifies the bandwidth-remaining ratio for the subinterface. • Enter the ratio. The ratio is the value used to determine the amount of unused bandwidth to allocate to each queue on the subinterface during periods of congestion. The scheduler allocates the excess bandwidth relative to other subinterfaces. Valid values are 1 to 1000. The default value is 1.
Step 12	**shape** {**average** | **peak**} *cir* [*bc*] [*be*] **Example:** `Router(config-pmap-c)# shape average 100000000`	(Optional) Shapes the average or peak rate to the rate that you specify. Enter either the **average** or **peak** keyword along with the CIR and any optional arguments. Note the following: • average--Specifies average-rate shaping. • peak--Specifies peak-rate shaping. • cir--Specifies the committed information rate (CIR), in bits per second (bps). • (Optional) bc--Specifies the committed burst size, in bits. • (Optional) be--Specifies the excess burst size, in bits.
Step 13	**service-policy** *child-policy-name* **Example:** `Router(config-pmap-c)# service-policy Child`	Applies the child policy map that you specify to the traffic class. • Enter the name of the previously configured child policy map.

	Command or Action	Purpose
		The router applies the QoS actions (features) specified in the child policy map to the traffic class. **Note** The **service-policy** command typically requires that you specify the direction of the traffic using the input or output keywords. However, when applying a child policy to a parent policy, do not specify a traffic direction.
Step 14	**exit** **Example:** `Router(config-pmap-c)# exit`	Exits policy-map class configuration mode.
Step 15	**exit** **Example:** `Router(config-pmap)# exit`	Exits policy-map configuration mode.
Step 16	**interface** *type slot / module / port* **.** *subinterface* [**point-to-point** | **multipoint**] **Example:** `Router(config)# interface GigabitEthernet 1/0/0.1`	Creates or modifies the interface that you specify and enters subinterface configuration mode. Enter the interface type. Note the following: • type--Specifies the interface type (for example, Gigabit Ethernet). • slot/module/port.subinterface--Specifies the number of the subinterface that identifies the subinterface (for example, 1/0/0.1). • (Optional) point-to-point--Indicates that the subinterface is a point-to-point subinterface. • (Optional) multipoint--Indicates that the subinterface is a point-to-multipoint subinterface.
Step 17	**service-policy output** *parent-policy-name* **Example:** `Router(config-subif)# service-policy output Parent`	Applies the parent policy map to the subinterface. • Enter the **output** keyword and the name of the parent policy map. **Note** The router shapes the subinterface traffic to the shaping rate specified in the parent class-default class and applies the QoS actions (features) specified in the child policy map. **Note** During periods of congestion, the router uses the bandwidth-remaining ratio specified in the parent policy map to allocate unused bandwidth on this subinterface relative to other subinterfaces.

	Command or Action	Purpose
Step 18	**end** **Example:** `Router(config-subif)# end`	Returns to privileged EXEC mode.

Configuring and Applying Bandwidth-Remaining Ratios to Class Queues

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map** *child-policy-name*
4. **class** *class-map-name*
5. **shape** {**average** | **peak**} *cir* [*bc*] [*be*]
6. **bandwidth remaining ratio** *ratio*
7. Repeat steps 4, 5 and 6 for each class queue that you want to define, specifying the bandwidth-remaining ratio as applicable.
8. **exit**
9. **exit**
10. **policy-map** *parent-policy-name*
11. **class class-default**
12. **shape** {**average** | **peak**} *cir* [*bc*] [*be*]
13. **bandwidth remaining ratio** *ratio*
14. **service-policy** *child-policy-name*
15. **exit**
16. **exit**
17. **interface** *type slot* / *module* / *port* **.** *subinterface* [**point-to-point** | **multipoint**]
18. **service-policy output** *parent-policy-name*
19. **end**

DETAILED STEPS

	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.

	Command or Action	Purpose
Step 3	**policy-map** *child-policy-name* **Example:** `Router(config)# policy-map Child`	Creates or modifies a child policy map and enters policy-map configuration mode. • Enter the name of the child policy map.
Step 4	**class** *class-map-name* **Example:** `Router(config-pmap)# class precedence_0`	Configures the class map and enters policy-map class configuration mode.

Step 5	**shape** {**average** | **peak**} *cir* [*bc*] [*be*]
	Example:
	`Router(config-pmap-c)# shape average 100000000`
		(Optional) Shapes the average or peak rate to the rate that you specify.
		• Enter either the **average** or **peak** keyword along with the CIR and any optional arguments. Note the following:
		  • average--Specifies average-rate shaping.
		  • peak--Specifies peak-rate shaping.
		  • cir--Specifies the committed information rate (CIR), in bits per second (bps).
		  • (Optional) bc--Specifies the committed burst size, in bits.
		  • (Optional) be--Specifies the excess burst size, in bits.

Step 6	**bandwidth remaining ratio** *ratio* **Example:** `Router(config-pmap-c)# bandwidth remaining ratio 10`	Specifies the bandwidth-remaining ratio for the traffic class. • Enter the bandwidth-remaining ratio. The ratio is the value used to determine the amount of unused bandwidth to allocate to each queue on the subinterface during periods of congestion. The queueing mechanism or scheduler allocates the excess bandwidth relative to other subinterfaces. Valid values are 1 to 1000. The default value is 1. **Note** In a hierarchical policy map structure, the **bandwidth remaining ratio***ratio* command must be used for at least one class. Using it in other classes is optional. When this command is not explicitly enabled in the other classes, the queueing mechanism uses 1 as the default.
Step 7	Repeat steps 4, 5 and 6 for each class queue that you want to define, specifying the bandwidth-remaining ratio as applicable.	

	Command or Action	Purpose
Step 8	**exit** **Example:** `Router(config-pmap-c)# exit`	Exits policy-map class configuration mode.
Step 9	**exit** **Example:** `Router(config-pmap)# exit`	Exits policy-map configuration mode.
Step 10	**policy-map** *parent-policy-name* **Example:** `Router(config)# policy-map Parent`	Creates or modifies a parent policy map and enters policy-map configuration mode. • Enter the name of the parent policy map.
Step 11	**class class-default** **Example:** `Router(config-pmap)# class class-default`	Configures the class-default class and enters policy-map class configuration mode. **Note** The router interprets any features that are configured under the class-default class as aggregate features on the subinterface.
Step 12	**shape** {**average** | **peak**} *cir* [*bc*] [*be*] **Example:** `Router(config-pmap-c)# shape average 100000000`	(Optional) Shapes the average or peak rate to the rate that you specify. • Enter either the **average** or **peak** keyword along with the CIR and any optional arguments. Note the following: • average--Specifies average-rate shaping. • peak--Specifies peak-rate shaping. • cir--Specifies the committed information rate (CIR), in bits per second (bps). • (Optional) bc--Specifies the committed burst size, in bits. • (Optional) be--Specifies the excess burst size, in bits.
Step 13	**bandwidth remaining ratio** *ratio* **Example:** `Router(config-pmap-c)# bandwidth remaining ratio 10`	(Optional for class-default or other classes in a hierarchical policy map structure) Specifies the bandwidth-remaining ratio for the subinterface. • Enter the bandwidth-remaining ratio. The ratio is the value used to determine the amount of unused bandwidth to allocate to each queue on the subinterface during periods of congestion. The queueing mechanism or scheduler allocates the excess

	Command or Action	Purpose
		bandwidth relative to other subinterfaces. Valid values are 1 to 1000. The default value is 1. **Note** In a hierarchical policy map structure, the **bandwidth remaining ratio***ratio* command must be used for at least one class. Using it in other classes is optional. When this command is not explicitly enabled in the other classes, the queueing mechanism uses 1 as the default.
Step 14	**service-policy** *child-policy-name* **Example:** `Router(config-pmap-c)# service-policy Child`	Applies the child policy map that you specify to the traffic class. • Enter the name of the child policy map. The router applies the QoS actions (features) specified in the child policy map to the traffic class. **Note** The **service-policy**command typically requires that you specify the direction of the traffic using the input or output keywords. However, when applying a child policy map to a parent policy map, do not specify traffic direction.
Step 15	**exit** **Example:** `Router(config-pmap-c)# exit`	Exits policy-map class configuration mode.
Step 16	**exit** **Example:** `Router(config-pmap)# exit`	Exits policy-map configuration mode.
Step 17	**interface** *type slot* / *module* / *port* **.** *subinterface* [**point-to-point** | **multipoint**] **Example:** `Router(config)# interface GigabitEthernet 1/0/0.1`	Creates or modifies the interface that you specify and enters subinterface configuration mode. • Enter the interface type. Note the following: • type--Specifies the interface type (for example, Gigabit Ethernet). • slot/module/port.subinterface--Specifies the number of the subinterface that identifies the subinterface (for example, 1/0/0.1). • (Optional) point-to-point--Indicates that the subinterface is a point-to-point subinterface. • (Optional) multipoint--Indicates that the subinterface is a point-to-multipoint subinterface.

	Command or Action	Purpose
Step 18	**service-policy output** *parent-policy-name* **Example:** `Router(config-subif)# service-policy output Parent`	Attaches the parent policy map to the subinterface. • Enter the **output**keyword and the name of the parent policy map. **Note** When congestion occurs, the class queues receive bandwidth according to the specified class-level bandwidth-remaining ratios.
Step 19	**end** **Example:** `Router(config-subif)# end`	Returns to privileged EXEC mode.

ConfigurationExamplesforDistributionofRemainingBandwidth Using Ratio

Example Configuring Bandwidth-Remaining Ratios on Ethernet Subinterfaces

The following example shows how to configure bandwidth-remaining ratios on an Ethernet subinterface using a hierarchical policy. In the example, Gigabit Ethernet subinterface 1/0/0.1 is shaped to 100 Mbps. During congestion, the router uses the bandwidth-remaining ratio of 10 to determine the amount of excess bandwidth (unused by priority traffic) to allocate to the nonpriority traffic on subinterface 1/0/0.1, relative to the other subinterface-level and class-level queues on the interface.

```
policy-map Child
 class precedence_0
  bandwidth 10000
 class precedence_1
  shape average 100000
  bandwidth 100
policy-map Parent
 class class-default
  bandwidth remaining ratio 10
  shape average 100000000
  service-policy Child
interface GigabitEthernet1/0/0.1
 encapsulation dot1Q 100
 ip address 10.1.0.1 255.255.255.0
 service-policy output Parent
```

Example Verifying Bandwidth-Remaining Ratios on Class Queues

In the following sample configuration, vlan10_policy is applied on the Gigabit Ethernet subinterface 1/0/0.10 and vlan20_policy is applied on the Gigabit Ethernet subinterface 1/0/0.20. During congestion on the interface, subinterface Gigabit Ethernet 1/0/0.20 has 10 times more available bandwidth than subinterface Gigabit Ethernet 1/0/0.10 because the bandwidth-remaining ratio for subinterface Gigabit Ethernet 1/0/0.20 is 10

times more than the bandwidth-remaining ratio for subinterface 1/0/0.10: 100 on subinterface 1/0/0.20 and 10 on subinterface 1/0/0.10.

When congestion occurs within a subinterface level, the class queues receive bandwidth according to the class-level bandwidth-remaining ratios. In the example, the bandwidth for classes precedence_0, precedence_1, and precedence_2 is allocated based on the bandwidth-remaining ratios of the classes: 20, 40, and 60, respectively.

Router# **show policy-map**

```
Policy Map child-policy
    Class precedence_0
      Average Rate Traffic Shaping
      cir 500000 (bps)
      bandwidth remaining ratio 20 <---- Class-level ratio
    Class precedence_1
      Average Rate Traffic Shaping
      cir 500000 (bps)
      bandwidth remaining ratio 40 <---- Class-level ratio
    Class precedence_2
      Average Rate Traffic Shaping
      cir 500000 (bps)
      bandwidth remaining ratio 60 <---- Class-level ratio
Policy Map vlan10_policy
    Class class-default
      Average Rate Traffic Shaping
      cir 1000000 (bps)
      bandwidth remaining ratio 10 <---- Subinterface-level ratio
      service-policy child-policy
Policy Map vlan20_policy
    Class class-default
      Average Rate Traffic Shaping
      cir 1000000 (bps)
      bandwidth remaining ratio 100 <---- Subinterface-level ratio
      service-policy child-policy
interface GigabitEthernet1/0/0.10
 encapsulation dot1Q 10
 snmp trap link-status
 service-policy output vlan10_policy
interface GigabitEthernet1/0/0.20
 encapsulation dot1Q 20
 snmp trap link-status
 service-policy output vlan20_policy
```

Example: Verifying Bandwidth Remaining Ratios

The following sample output from the show policy-map interface command indicates that bandwidth-remaining ratios are configured on class-level queues in the policy maps named vlan10_policy and child-policy, which are attached to Gigabit Ethernet subinterface 1/0/0.10.

```
Router# show policy-map interface GigabitEthernet 1/0/0.10
GigabitEthernet1/0/0.10
  Service-policy output: vlan10_policy
    Class-map: class-default (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
      Queueing
      queue limit 64 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
```

```
    (pkts output/bytes output) 0/0
    shape (average) cir 1000000, bc 4000, be 4000
    target shape rate 1000000
    bandwidth remaining ratio 10
    Service-policy : child-policy
      Class-map: precedence_0 (match-all)
        0 packets, 0 bytes
        5 minute offered rate 0 bps, drop rate 0 bps
        Match: ip precedence 0
        Queueing
        queue limit 64 packets
        (queue depth/total drops/no-buffer drops) 0/0/0
        (pkts output/bytes output) 0/0
        shape (average) cir 500000, bc 2000, be 2000
        target shape rate 500000
        bandwidth remaining ratio 20
      Class-map: precedence_1 (match-all)
        0 packets, 0 bytes
        5 minute offered rate 0 bps, drop rate 0 bps
        Match: ip precedence 1
        Queueing
        queue limit 64 packets
        (queue depth/total drops/no-buffer drops) 0/0/0
        (pkts output/bytes output) 0/0
        shape (average) cir 500000, bc 2000, be 2000
        target shape rate 500000
        bandwidth remaining ratio 40
      Class-map: precedence_2 (match-all)
        0 packets, 0 bytes
        5 minute offered rate 0 bps, drop rate 0 bps
        Match: ip precedence 2
        Queueing
        queue limit 64 packets
        (queue depth/total drops/no-buffer drops) 0/0/0
        (pkts output/bytes output) 0/0
        shape (average) cir 500000, bc 2000, be 2000
        target shape rate 500000
        bandwidth remaining ratio 60
      Class-map: class-default (match-any)
        0 packets, 0 bytes
        5 minute offered rate 0 bps, drop rate 0 bps
        Match: any

        queue limit 64 packets
        (queue depth/total drops/no-buffer drops) 0/0/0
        (pkts output/bytes output) 0/0
```

The following sample output from the show policy-map interface command indicates that bandwidth-remaining ratios are configured on class-level queues in the policy maps named vlan20_policy and child-policy, which are attached to Gigabit Ethernet subinterface 1/0/0.20.

```
Router# show policy-map interface GigabitEthernet 1/0/0.20
GigabitEthernet1/0/0.20
  Service-policy output: vlan20_policy
    Class-map: class-default (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
      Queueing
      queue limit 64 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 0/0
      shape (average) cir 1000000, bc 4000, be 4000
```

```
      target shape rate 1000000
      bandwidth remaining ratio 100
      Service-policy : child-policy
        Class-map: precedence_0 (match-all)
          0 packets, 0 bytes
          5 minute offered rate 0 bps, drop rate 0 bps
          Match: ip precedence 0
          Queueing
          queue limit 64 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
          (pkts output/bytes output) 0/0
          shape (average) cir 500000, bc 2000, be 2000
          target shape rate 500000
          bandwidth remaining ratio 20
        Class-map: precedence_1 (match-all)
          0 packets, 0 bytes
          5 minute offered rate 0 bps, drop rate 0 bps
          Match: ip precedence 1
          Queueing
          queue limit 64 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
          (pkts output/bytes output) 0/0
          shape (average) cir 500000, bc 2000, be 2000
          target shape rate 500000
          bandwidth remaining ratio 40
        Class-map: precedence_2 (match-all)
          0 packets, 0 bytes
          5 minute offered rate 0 bps, drop rate 0 bps
          Match: ip precedence 2
          Queueing
          queue limit 64 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
          (pkts output/bytes output) 0/0
          shape (average) cir 500000, bc 2000, be 2000
          target shape rate 500000
          bandwidth remaining ratio 60
        Class-map: class-default (match-any)
          0 packets, 0 bytes
          5 minute offered rate 0 bps, drop rate 0 bps
          Match: any

          queue limit 64 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
          (pkts output/bytes output) 0/0
```

The following sample output from the show policy-map command indicates that a bandwidth-remaining ratio of 10 is configured on the parent class-default class of the policy map named vlan10_policy.

```
Router# show policy-map vlan10_policy
  Policy Map vlan10_policy
    Class class-default
      Average Rate Traffic Shaping
      cir 1000000 (bps)
      bandwidth remaining ratio 10
      service-policy child-policy
```

The following sample output from the show policy-map command indicates that a bandwidth-remaining ratio of 100 is configured on the parent class-default class of the policy map named vlan20_policy.

```
Router# show policy-map vlan20_policy
  Policy Map vlan20_policy
    Class class-default
      Average Rate Traffic Shaping
```

```
      cir 1000000 (bps)
      bandwidth remaining ratio 100
      service-policy child-policy
```

The following sample output from the show policy-map command indicates that bandwidth-remaining ratios of 20, 40, and 60 are configured on the class queues precedence_0, precedence_1, and precedence_2, respectively.

```
Router# show policy-map child-policy
  Policy Map child-policy
    Class precedence_0
      Average Rate Traffic Shaping
      cir 500000 (bps)
      bandwidth remaining ratio 20
    Class precedence_1
      Average Rate Traffic Shaping
      cir 500000 (bps)
      bandwidth remaining ratio 40
    Class precedence_2
      Average Rate Traffic Shaping
      cir 500000 (bps)
      bandwidth remaining ratio 60
```

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*
Congestion avoidance	"Congestion Avoidance Overview" module
Class maps, policy maps, hierarchical policy maps, Modular Quality of Service Command-Line Interface (CLI) (MQC)	"Applying QoS Features Using the MQC" module
Traffic shaping, traffic policing	"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

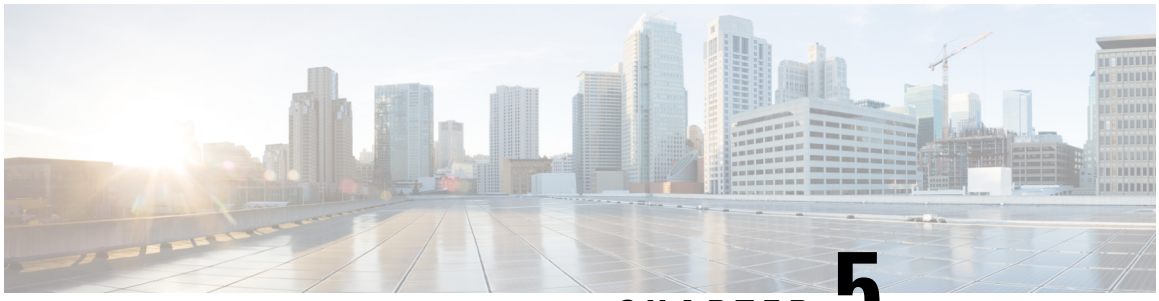
Feature Information for Distribution of Remaining Bandwidth Using Ratio

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

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

Table 2: Feature Information for Distribution of Remaining Bandwidth Using Ratio

Feature Name	Releases	Feature Information
MQC--Distribution of Remaining Bandwidth Using Ratio	Cisco IOS XE Release 2.1	The Distribution of Remaining Bandwidth Using Ratio feature allows service providers to configure a bandwidth-remaining ratio on subinterfaces and class queues. This ratio specifies the relative weight of a subinterface or queue with respect to other subinterfaces or queues. During congestion, the router uses this bandwidth-remaining ratio to determine the amount of excess bandwidth (unused by priority traffic) to allocate to a class of nonpriority traffic. In Cisco IOS XE Release 2.1, this feature was introduced on Cisco ASR 1000 Series Routers. The following commands were introduced or modified: **bandwidth remaining ratio**, **show policy-map**, **show policy-map interface**.



CHAPTER 5

QoS Percentage-Based Shaping

The QoS: Percentage-Based Shaping feature allows you to configure traffic shaping on the basis of a percentage of bandwidth available on the interface. This feature also allows you to specify the committed (conform) burst (bc) size and the excess (peak) burst (be) size (used for configuring traffic shaping) in milliseconds (ms). Configuring traffic shaping in this manner enables you to use the same policy map for multiple interfaces with differing amounts of bandwidth.

Finding Feature Information

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

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

Information About QoS Percentage-Based Shaping

Benefits for QoS Percentage-Based Shaping

This feature provides the ability to configure traffic shaping on the basis of a percentage of bandwidth available on an interface, and it allows you to specify burst sizes in milliseconds. Configuring traffic shaping in this manner enables you to use the same policy map for multiple interfaces with differing amounts of bandwidth. That is, you do not have to recalculate the bandwidth for each interface or configure a different policy map for each type of interface.

Class and Policy Maps for QoS Percentage-Based Shaping

To configure the QoS: Percentage-Based Shaping feature, you must define a traffic class, configure a policy map, and then attach that policy map to the appropriate interface.

In the MQC, the **class-map** command is used to define a traffic class (which is then associated with a traffic policy). The purpose of a traffic class is to classify traffic.

The MQC consists of the following three processes:

- Defining a traffic class with the **class-map** command.
- Creating a traffic policy by associating the traffic class with one or more QoS features (using the **policy-map** command).
- Attaching the traffic policy to the interface with the **service-policy** command.

A traffic class contains three major elements: a name, a series of match commands, and, if more than one **match** command exists in the traffic class, an instruction on how to evaluate these **match** commands (that is, match-all or match-any). The traffic class is named in the **class-map** command line; for example, if you enter the **class-map cisco** command while configuring the traffic class in the CLI, the traffic class would be named "cisco".

The **match** commands are used to specify various criteria for classifying packets. Packets are checked to determine whether they match the criteria specified in the **match** commands. If a packet matches the specified criteria, that packet is considered a member of the class and is forwarded according to the QoS specifications set in the traffic policy. Packets that fail to meet any of the matching criteria are classified as members of the default traffic class.

Traffic Regulation Mechanisms and Bandwidth Percentages

Cisco IOS XE quality of service (QoS) offers two kinds of traffic regulation mechanisms--traffic policing and traffic shaping. A traffic policer typically drops traffic that violates a specific rate. A traffic shaper typically delays excess traffic using a buffer to hold packets and shapes the flow when the data rate to a queue is higher than expected.

Traffic shaping and traffic policing can work in tandem and can be configured in a class map. Class maps organize data packets into specific categories ("classes") that can, in turn, receive a user-defined QoS treatment when used in policy maps (sometimes referred to as "service policies").

Before this feature, traffic policing and traffic shaping were configured on the basis of a user-specified amount of bandwidth available on the interface. Policy maps were then configured on the basis of that specific amount of bandwidth, meaning that separate policy maps were required for each interface.

This feature provides the ability to configure traffic policing and traffic shaping on the basis of a percentage of bandwidth available on the interface. Configuring traffic policing and traffic shaping in this manner enables customers to use the same policy map for multiple interfaces with differing amounts of bandwidth.

Configuring traffic policing and shaping on the basis of a percentage of bandwidth is accomplished by using the **police** (percent) and **shape** (percent) commands.

Burst Size Specified in Milliseconds Option

The purpose of the burst parameters (bc and be) is to specify the amount of traffic to anticipate under normal operating conditions before traffic is dropped or delayed. Setting sufficiently high burst values helps to ensure good throughput.

This feature allows you the option of specifying the committed (conform) burst (bc) size and the excess (peak) burst (be) as milliseconds (ms) of the class bandwidth when you configure traffic shaping. The number of milliseconds is used to calculate the number of bytes to be used by the QoS: Percentage-Based Shaping feature.

Specifying these burst sizes in milliseconds is accomplished by using the **bc** and **be** keywords (and their associated arguments) of the **shape** (percent) command.

How to Configure QoS Percentage-Based Shaping

Configuring a Class and Policy Map

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map** *policy-name*
4. **class** {*class-name*| **class-default**}
5. **shape** {**average** | **peak**} **percent** *percentage* [**be** *excess-burst-in-msec* **ms**] [**bc** *committed-burst-in-msec* **ms**]
6. **end**

DETAILED STEPS

	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-name* **Example:** `Router(config)# policy-map policy1`	Specifies the name of the policy map to be created. Enters policy-map configuration mode. • Enter the policy map name.
Step 4	**class** {*class-name*| **class-default**} **Example:**	Specifies the class so that you can configure or modify its policy. Enters policy-map class configuration mode.

	Command or Action	Purpose
	`Router(config-pmap)# class class1`	• Enter the class name or specify the default class (class-default).
Step 5	**shape** {**average** | **peak**} **percent** *percentage* [**be** *excess-burst-in-msec* **ms**] [**bc** *committed-burst-in-msec* **ms**] **Example:** `Router(config-pmap-c)# shape average percent 25 be 300 ms bc 400 ms`	Configures either average or peak rate traffic shaping on the basis of the specified bandwidth percentage and the optional burst sizes. • Enter the bandwidth percentage and optional burst sizes.
Step 6	**end** **Example:** `Router(config-pmap-c)# end`	Exits policy-map class configuration mode.

Attaching the Policy Map to an Interface

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **pvc** [*name*] *vpi* / *vci* [**ilmi** | **qsaal** | **smds**]
5. **service-policy** {**input**| **output**} *policy-map-name*
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables higher privilege levels, such as privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

Step 3	**interface** *type number*
	Example:
	`Router(config)#`
	`interface serial4/0/0`
		Configures an interface (or subinterface) type and enters interface configuration mode.
		• Enter the interface type number.

	Command or Action	Purpose
		Note Depending on the needs of your network, you may need to attach the policy map to a subinterface, an ATM PVC, a Frame Relay DLCI, or other type of interface.
Step 4	**pvc** [*name*] *vpi* / *vci* [**ilmi** | **qsaal** | **smds**] **Example:** `Router(config-if)# pvc cisco 0/16 ilmi`	(Optional) Creates or assigns a name to an ATM PVC and specifies the encapsulation type on an ATM PVC. Enters ATM VC configuration mode. **Note** This step is required only if you are attaching the policy map to an ATM PVC. If you are not attaching the policy map to an ATM PVC, skip this step and proceed with Step 5.

Step 5	**service-policy** {**input**| **output**} *policy-map-name*
	Example:
	`Router(config-if)#`
	`service-policy input policy1`
	Example:
		Specifies the name of the policy map to be attached to the input or output direction of the interface.
		Note Policy maps can be configured on ingress or egress routers. They can also be attached in the input or output direction of an interface. The direction (input or output) and the router (ingress or egress) to which the policy map should be attached varies according your network configuration. When using the **service-policy** command to attach the policy map to an interface, be sure to choose the router and the interface direction that are appropriate for your network configuration.
		Note Traffic shaping is supported on service policies attached to output interfaces or output VCs only.
		• Enter the policy map name.

Step 6	**end** **Example:** `Router(config-if)# end`	(Optional) Exits interface configuration mode.

Verifying the QoS Percentage-Based Shaping Configuration

SUMMARY STEPS

1. **enable**
2. **show class-map** [*class-map-name*]
3. **show policy-map interface** *interface-name*
4. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show class-map** [*class-map-name*] **Example:** `Router# show class-map class1`	Displays all information about a class map, including the match criterion. • Enter class map name.

Step 3	**show policy-map interface** *interface-name*
	Example:
	`Router#`
	`show policy-map interface serial4/0/0`
		Displays the packet statistics of all classes that are configured for all service policies either on the specified interface or subinterface or on a specific PVC on the interface.
		• Enter the interface type and number.

Step 4	**exit** **Example:** `Router# exit`	(Optional) Exits privileged EXEC mode.

Troubleshooting Tips

The commands in the Verifying the QoS Percentage-Based Shaping Configuration, on page 33 section allow you to verify that you achieved the intended configuration and that the feature is functioning correctly. If, after using the **show** commands listed above, you find that the configuration is not correct or the feature is not functioning as expected, perform these operations:

If the configuration is not the one you intended, complete the following procedures:

1. Use the **show running-config** command and analyze the output of the command.
2. If the policy map does not appear in the output of the **show running-config** command, enable the **logging console** command.
3. Attach the policy map to the interface again.

If the packets are not being matched correctly (for example, the packet counters are not incrementing correctly), complete the following procedures:

1. Run the **show policy-map**command and analyze the output of the command.
2. Run the **show running-config** command and analyze the output of the command.
3. Use the **show policy-map interface** command and analyze the output of the command. Check the the following findings:
    1. If a policy map applies queueing, and the packets are matching the correct class, but you see unexpected results, compare the number of the packets in the queue with the number of the packets matched.

2. If the interface is congested, and only a small number of the packets are being matched, check the tuning of the transmission (tx) ring, and evaluate whether the queueing is happening on the tx ring. To do this, use the **show controllers** command, and look at the value of the tx count in the output of the command.

Configuration Examples for QoS Percentage-Based Shaping

Example Specifying Traffic Shaping on the Basis of a Bandwidth Percentage

The following example configures traffic shaping using an average shaping rate on the basis of a percentage of bandwidth. In this example, 25 percent of the bandwidth has been specified. Additionally, an optional be value and bc value (300 ms and 400 ms, respectively) have been specified.

```
Router> enable
Router# configure terminal
Router(config)# policy-map policy1
Router(config-pmap)# class class1

Router(config-pmap-c)# shape average percent 25 be 300 ms bc 400 ms

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

After the policy map and class maps are configured, the policy map is attached to interface as shown in the following example:

```
Router> enable
Router# configure terminal
Router(config)#

interface serial4/0/0
Router(config-if)#

service-policy input policy1
Router(config-if)# end
```

Example Verifying the QoS Percentage-Based Shaping Configuration

This section contains sample output from the **show policy-map**command and the **show policy-map interface**command. The output from these commands can be used to verify and monitor the configuration on your network.

The following is sample output from the **show policy-map** command. This sample output displays the contents of a policy map called "policy3." In policy 3, average rate traffic shaping on the basis of an committed information rate (CIR) of 30 percent has been configured, and the bc and be have been specified in milliseconds.

```
Router# show policy-map
  Policy Map policy3
    Class class-default
      Average Rate Traffic Shaping
      cir 30% bc 10 (msec) be 10 (msec)
```

The following is sample output from the **show policy-map interface** command. This sample displays the statistics for the serial 2/0 interface on which average rate traffic shaping has been enabled.

```
Router# show policy-map interface serial2/0/0
 Serial2/0/0
  Service-policy output: policy3 (1032)
    Class-map: class-default (match-any) (1033/0)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any  (1034)
        0 packets, 0 bytes
        5 minute rate 0 bps
      Queueing
      queue limit 64 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts queued/bytes queued) 0/0
      shape (average) cir 614400 bc 6144 be 6144
      target shape rate 614400
```

In this example, the CIR is displayed in bps, and both the committed burst (bc) and excess burst (be) are displayed in bits.

The CIR, bc, and be are calculated on the basis of the formulas described below.

Formula for Calculating the CIR

When calculating the CIR, the following formula is used:

CIR percentage specified (as shown in the output of the **show policy-map**command) * bandwidth (BW) of the interface (as shown in the output of the **show interfaces** command) = total bits per second

On the serial 2/0 interface, the bandwidth (BW) is 2048 kbps. To see the bandwidth of the interface, use the **show interfaces** command. A sample is shown below:

```
Router # show interfaces serial2/0/0
Serial2/0 is administratively down, line protocol is down
  Hardware is M4T
  MTU 1500 bytes, BW 2048 Kbit, DLY 20000 usec, rely 255/255, load 1/255
```

Therefore, the following values are used in the formula:

30% * 2048 kbps = 614400 bps

Formula for Calculating the Committed Burst (bc) and the Excess Burst (be)

When calculating both the bc and the be, the following formula is used:

The bc (or be) in milliseconds (as shown in the **show policy-map** command) * the CIR in kilobytes (as shown in the **show policy-map** command) / 1000 = total number of bits

Therefore, the following values are used in the formula:

10 ms * 614400 bps = 6144 bits

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 QoS Command-Line Interface (CLI) (MQC) information about attaching policy maps to interfaces	"Applying QoS Features Using the MQC" module
Traffic shaping concepts and overview	"Policing and Shaping Overview" module
Traffic policing	"Traffic Policing" 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
RFC 2697	*A Single Rate Three Color Marker*
RFC 2698	*A Two Rate Three Color Marker*

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

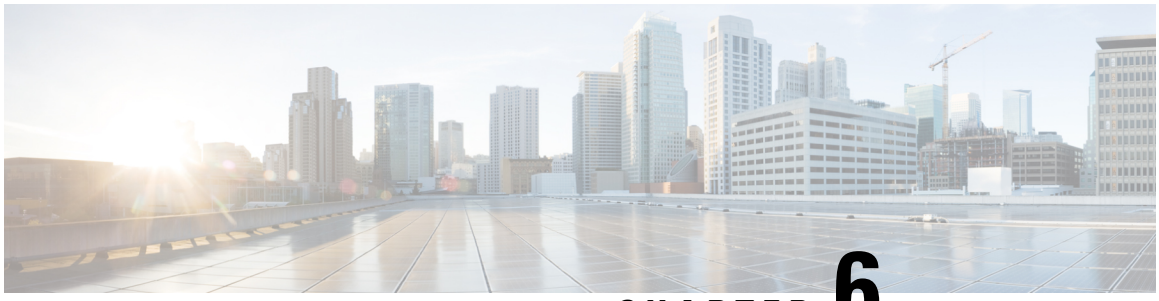
Feature Information for QoS Percentage-Based Shaping

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

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

Table 3: Feature Information for QoS: Percentage-Based Shaping

Feature Name	Releases	Feature Information
QoS: Percentage-Based Shaping	Cisco IOS XE Release 2.1	The QoS: Percentage-Based Shaping feature allows you to configure traffic shaping on the basis of a percentage of bandwidth available on the interface. This feature also allows you to specify the committed (conform) burst (bc) size and the excess (peak) burst (be) size (used for configuring traffic shaping) in milliseconds (ms). Configuring traffic shaping in this manner enables you to use the same policy map for multiple interfaces with differing amounts of bandwidth. This feature was introduced on Cisco ASR 1000 Series Routers. The following commands were introduced or modified: **shape (percent)**, **show policy-map**, **show policy-map interface**.



CHAPTER 6

Ethernet Overhead Accounting

The Ethernet Overhead Accounting feature enables the router to account for downstream Ethernet frame headers when applying shaping to packets.

Finding Feature Information

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

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

Restrictions for Ethernet Overhead Accounting

- Ethernet overhead accounting allows the automatic inclusion of downstream Ethernet frame headers in the shaped rate.
- If you enable overhead accounting on a child policy, you must enable overhead accounting on the parent policy.
- In a policy map, you must either enable overhead accounting for all classes in the policy or disable overhead accounting for all classes in the policy. You cannot enable overhead accounting for some classes and disable overhead accounting for other classes in the same policy.
- Overhead accounting is not reflected in any QoS counters (classification, policing, or queuing).
- Implicit ATM overhead accounting for policers are not supported.

- Implicit L2 overhead (ATM or otherwise) for policers are not supported for certain logical targets (tunnels) when the policy is applied to the logical target. The same limitation exists for queuing and scheduling overhead accounting.
- Police overhead cannot be configured on conditional policers (priority and rate), however, the priority queue it used will inherit the queueing overhead from parent shaper if configured.
- Police overhead is not added to the counters and are not reflected in statistics reported by the control plane.
- The overhead accounting type or value used by policing within a policy map and between the parent policy map and the child policy map (in a hierarchical policy map structure) must be consistent.
- The overhead accounting type or value used by queuing features within a policy map and between the parent policy map and the child policy map (in a hierarchical policy map structure) must be consistent.
- In releases preceding to Cisco IOS XE Release 3.9S, the router does not support overhead accounting updates on attached policies and the policy must be detached from the interface before the overhead can be modified, then the policy can be reattached to the interface.
- The router does not support overhead accounting for classes with fair-queue, which includes the following scenarios:
  - When used in conjunction with shape in the same class
  - When used in conjunction with bandwidth in the same class
  - When inherited from a parent or grandparent class through the Parent Level Overhead Accounting feature introduced in Cisco IOS XE Release 3.9S

Information About Ethernet Overhead Accounting

Benefits of Ethernet Overhead Accounting

The Ethernet Overhead Accounting feature enables the router to account for downstream Ethernet frame headers when applying shaping to packets. A user-defined offset specifies the number of overhead bytes that the router is to use when calculating the overhead per packet. Valid offset values are from +63 bytes to -63 bytes of overhead. Before applying shaping, the router calculates the overhead.

Any interface that supports QoS policies will support overhead accounting. Using the **policy-map**, **shape** or **bandwidth** command, you can configure accounting on the interfaces.

Subscriber Line Encapsulation Types

The *subscriber-encapsulation* argument of the **shape** and **bandwidth** commands specifies the encapsulation type at the subscriber line. The router supports the following subscriber line encapsulation types:

- snap-1483routed
- mux-1483routed
- snap-dot1q-rbe

- mux-dot1q-rbe
- snap-pppoa
- mux-pppoa
- snap-rbe
- mux-rbe

Overhead Calculation on the Router

When calculating overhead for traffic shaping, the router considers the encapsulation type used between the broadband aggregation system (BRAS) and the digital subscriber line access multiplexer (DSLAM) and between the DSLAM and the customer premises equipment (CPE).

The table below describes the fields that the router uses for the various encapsulation types when calculating ATM overhead.

Table 4: Overhead Calculation

Encapsulation Type	Number of Bytes	Description
802.1Q	18	6-byte destination MAC address + 6-byte source MAC address + 2-byte protocol ID (0x8100) + 2-byte VID/CFI/PRIORITY + 2-byte length/type
802.3	14	6-byte destination MAC address + 6-byte source MAC address + 2-byte protocol ID (0x8000)
AAL5 MUX plus 1483	8	8-byte AAL5 trailer
AAL5 MUX plus PPPoA	10	8-byte AAL5 trailer + 2-byte protocol ID (0x002
AAL5 SNAP plus 1483	18	8-byte AAL5 trailer + 3-byte LLC header (0xAAAA03) + 3-byte OUI (0x0080c2) + 2-byte protocol ID (0x0007) + 2-byte PAD (0x0000)
AAL5 SNAP plus PPPoA	12	8-byte AAL5 trailer + 3-byte LLC header (0xFEFE03) + 1-byte protocol ID (0xCF)
PPPoE	6	1-byte version/type (0x11) + 1-byte code (0x00) + 2-byte session ID + 2-byte lengt
qinq	22	6-byte destination MAC address + 6-byte source MAC address + 2-byte protocol ID (0x8100) + 2-byte VID/CFI/PRIORITY + 2-byte protocol ID + 2-byte inner tag + 2-byte length or type

Overhead Accounting and Hierarchical Policies

In hierarchical policies, you can configure overhead accounting for policing, shaping, and bandwidth on top-level parent policies, middle-level child policies, and bottom-level child policies. Overhead accounting

policies configured at the parent or grandparent level are inherited by the child queueing features. Overhead accounting configured on a child policy must also be configured on the parent policy; therefore configuring on the parent or grandparent level is easier.

The parent and child classes must specify the same encapsulation type when enabling overhead accounting and configuring an offset using the **user-defined** *offset* [**atm**] arguments of the **bandwidth** (policy-map class) command.

The table below summarizes the configuration requirements for overhead accounting.

Table 5: Overhead Accounting Configuration Requirements

Policy Map or Class	Current Configuration	Configuration Requirement
Parent	Enabled	Enabled on child policy
Child	Enabled	Enabled on parent policy
Child class	Enabled	Enabled on all classes in the child policy map, except priority classes with policing
Child class (nonpriority without policing)	Disabled	Disabled on all classes in the child policy map
Child class (priority with policing)	Disabled	Disabled or enabled on all nonpriority classes in the child policy map

Overhead Accounting and Priority Queues

Overhead accounting configuration is supported for queuing features (shape, bandwidth and priority) and non-queuing feature (police) separately. However, priority queue can be integrated with policer. When overhead accounting is configured on a priority queue, through inheritance, it operates in the following fashion:

- Overhead accounting is added to (or subtracted from) the priority packet for queuing features in the hierarchy (for example, shape in the parent class).
- Overhead accounting is not added to the packet for priority rate enforcement (**priority** {*bandwidth-kbps* | **percent** *percentage*} [**burst**]). Although policing overhead accounting is supported, it does not apply to the conditional policer (rate enforcement is implemented through this conditional policer).

How to Configure Ethernet Overhead Accounting

Configuring Ethernet Overhead Accounting in a Hierarchical Policy

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map** *policy-map-name*
4. **class** *class-map-name*

5. **bandwidth** {*bandwidth-kbps* | [**remaining**] **percent** *percentage*} **account** {**qinq** | **dot1q**} {**aal5** | **aal3**} *subscriber-encapsulation* **user-defined** *offset* [**atm**]
6. **exit**
7. **policy-map** *policy-map-name*
8. **class class-default**
9. **shape** [**average**] *rate* **account** {{**qinq** | **dot1q**} {**aal5** | **aal3**} *subscriber-encapsulation* | **user-defined** *offset* [**atm**]}
10. **service-policy** *policy-map-name*
11. **end**

DETAILED STEPS

	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 Business`	Creates or modifies the child policy. Enters policy-map configuration mode. • The *policy-map-name* argument represents the name of the child policy map.
Step 4	**class** *class-map-name* **Example:** `Router(config-pmap)# class video`	Assigns the traffic class you specify to the policy map. Enters policy-map class configuration mode. • The *class-map-name* argument represents the name of a previously configured class map.
Step 5	**bandwidth** {*bandwidth-kbps*	[**remaining**] **percent** *percentage*} **account** {**qinq**	**dot1q**} {**aal5**	**aal3**} *subscriber-encapsulation* **user-defined** *offset* [**atm**] **Example:** `Router(config-pmap-c)# bandwidth 8000 account dot1q aal5 snap-pppoa`	Enables class-based fair queueing and overhead accounting. • *bandwidth-kbps*—The minimum bandwidth allocated for a class belonging to a policy map. Valid values are from 8 to 2,488,320, which represents from 1 to 99 percent of the link bandwidth. • *percentage*—The maximum percentage of the link bandwidth allocated for a class belonging to a policy map. Valid values are from 1 to 99. • **remaining** *percentage*—The minimum percentage of unused link bandwidth allocated for a class belonging to a policy map. Valid values are from 1 to 99. • **account**—Enables ATM overhead accounting.

	Command or Action	Purpose
		• **qinq**—Specifies queue-in-queue encapsulation as the BRAS-DSLAM encapsulation type. • **dot1q**—Specifies IEEE 802.1Q VLAN encapsulation as the BRAS-DSLAM encapsulation type. • **aal5**—Specifies the ATM Adaptation Layer 5 that supports connection-oriented variable bit rate (VBR) services. • **aal3**—Specifies the ATM Adaptation Layer 5 that supports both connectionless and connection-oriented links. • *subscriber-encapsulation*—Specifies the encapsulation type at the subscriber line. For more information, see the "Configuring Ethernet Overhead Accounting in a Hierarchical Policy" section. • **user-defined**—Indicates that the router is to use the offset value that you specify when calculating ATM overhead. • *offset*—Specifies the number of bytes that the router is to use when calculating overhead. Valid values are from -63 to 63 bytes. • **atm**—(Optional) Applies the ATM cell tax in the ATM overhead calculation.
Step 6	**exit** **Example:** `router(config-pmap-c)# exit`	Exits policy-map class configuration mode.
Step 7	**policy-map** *policy-map-name* **Example:** `Router(config-pmap)# policy-map Test`	Creates or modifies the top-level parent policy. • *policy-map-name*—Specifies the name of the parent policy map.
Step 8	**class class-default** **Example:** `Router(config-pmap)# class class-default`	Specifies a default class.
Step 9	**shape** [**average**] *rate* **account** {{**qinq** | **dot1q**} {**aal5** | **aal3**} *subscriber-encapsulation* | **user-defined** *offset* [**atm**]} **Example:** `Router(config-pmap-c)# shape 8000 account qinq aal5 snap-dot1-rbe`	Shapes traffic to the indicated bit rate and enables overhead accounting. • **average** (Optional)—Is the committed burst (Bc) that specifies the maximum number of bits sent out in each interval. This option is only supported on the PRE3.

	Command or Action	Purpose
		• **rate**—Indicates the bit rate used to shape the traffic, in bits per second. When this command is used with backward explicit congestion notification (BECN) approximation, the bit rate is the upper bound of the range of bit rates that are permitted. • **account**—Enables ATM overhead accounting. • **qinq**—Specifies queue-in-queue encapsulation as the BRAS-DSLAM encapsulation type. • **dot1q**—Specifies IEEE 802.1Q VLAN encapsulation as the BRAS-DSLAM encapsulation type. • **aal5**—Specifies the ATM Adaptation Layer 5 that supports connection-oriented variable bit rate (VBR) services. • **aal3**—Specifies the ATM Adaptation Layer 5 that supports both connectionless and connection-oriented links. • *subscriber-encapsulation*—Specifies the encapsulation type at the subscriber line. For more information, see the "Configuring Ethernet Overhead Accounting in a Hierarchical Policy" section. • **user-defined**—Indicates that the router is to use the offset value that you specify when calculating ATM overhead. • *offset*—Specifies the number of bytes that the router is to use when calculating overhead. Valid values are from -63 to 63 bytes. • **atm**—(Optional) Applies the ATM cell tax in the ATM overhead calculation. Configuring both the offset and atm options adjusts the packet size to the offset size and then adds the ATM cell tax.
Step 10	**service-policy** *policy-map-name* **Example:** `Router(config-pmap-c)# service-policy map1`	Applies a child policy to the parent class-default class. *policy-map-name*—Specifies the name of a previously configured child policy map. **Note** Do not specify the input or output keywords when applying a child policy to a parent class-default class.
Step 11	**end** **Example:** `Router(config-pmap-c)# end`	Exits policy-map class configuration mode and returns to privileged EXEC mode.

Configuration Examples for Ethernet Overhead Accounting

Example: Enabling Ethernet Overhead Accounting

The following configuration example shows how to enable Ethernet overhead accounting. In the example, the configuration of the policy map named ethernet_ovrh shapes class-default traffic at a rate of 200,000 kbps and enables overhead accounting with a user-defined value of 18. The ethernet_ovrh policy is attached to Gigabit Ethernet subinterface 1/0/0.100, thereby enabling overhead accounting on the subinterface.

```
Router# configure-terminal
Router(config)# policy-map ethernet_ovrh
Router(config-pmap)# class class-default
Router(config-pmap-c)# shape average 200000 account user-defined 18
!
Router(config)# interface GigabitEthernet1/0/0.100
Router(config-subif)# service-policy output ethernet_ovrh
!
Router# show running-config | begin 1/0/0.100

interface GigabitEthernet1/0/0.100
encapsulation dot1Q 101
pppoe enable group group_pta
service-policy output ethernet_ovrh
```

Example: Verifying Ethernet Overhead Accounting with User-Defined Option

The following sample output for the policy map named ethernet_ovrh indicates that Ethernet overhead accounting is enabled for shaping and that the user-defined offset is 18 bytes. The sample output from the **show policy-map** command indicates that the ethernet_ovrh policy map is attached to the Gigabit Ethernet subinterface 1/0/0.100, enabling overhead accounting on the subinterface.

```
Router# show policy-map ethernet_ovrh

Policy Map ethernet_ovrh
Class class-default
Average Rate Traffic Shaping
cir 200000 (bps) account user-defined 18
Router# show policy-map interface GigabitEthernet1/0/0.100
GigabitEthernet1/0/0.100
Service-policy output: ethernet_ovrh
Class-map: class-default (match-any)
0 packets, 0 bytes
30 second offered rate 0 bps, drop rate 0 bps
Match: any
0 packets, 0 bytes
30 second rate 0 bps
Queueing
queue limit 8 packets
(queue depth/total drops/no-buffer drops) 0/0/0
(pkts output/bytes output) 0/0
shape (average) cir 200000, bc 800, be 800
target shape rate 200000
Overhead Accounting Enabled
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
QoS commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	Cisco IOS Quality of Service Solutions 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

Standards

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

RFCs

RFC	Title
No new or modified RFCs are supported, and support for existing RFCs has not been modified.	—

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

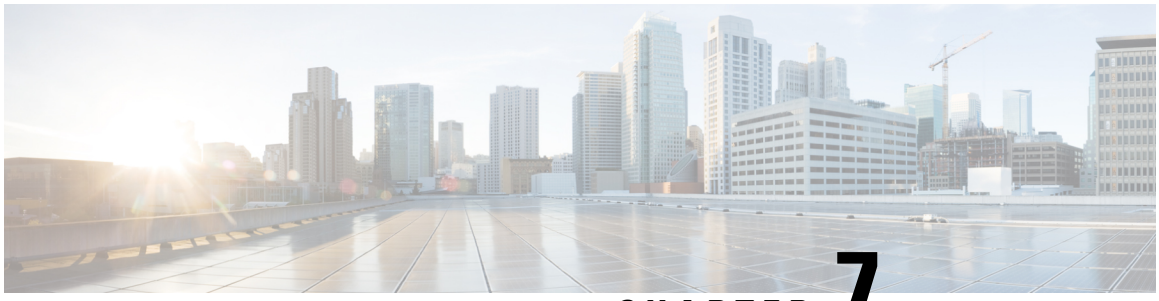
Feature Information for Ethernet Overhead Accounting

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

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

Table 6: Feature Information for Ethernet Overhead Accounting

Feature Name	Releases	Feature Information
Ethernet Overhead Accounting	Cisco IOS XE Release 2.4	The Ethernet Overhead Accounting feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers. It enables the router to account for downstream Ethernet frame headers when applying shaping to packets.
Ethernet Overhead Accounting (Policing) for MEF 2.0 Certification	Cisco IOS XE Release 3.17S	This feature adds support for user-defined overhead accounting to QoS MQC policers on the Cisco ASR 1000 Series Aggregation Services Routers.



CHAPTER 7

MQC Traffic Shaping Overhead Accounting for ATM

The MQC Traffic Shaping Overhead Accounting for ATM feature enables a broadband aggregation system (BRAS) to account for various encapsulation types when applying quality of service (QoS) functionality to packets. Typically, in Ethernet digital subscriber line (DSL) environments, the encapsulation from the router to the digital subscriber line access multiplexer (DSLAM) is Gigabit Ethernet and the encapsulation from the DSLAM to the customer premises equipment (CPE) is ATM. ATM overhead accounting enables the router to account for ATM encapsulation on the subscriber line and for the overhead added by cell segmentation. This functionality enables the service provider to prevent overruns at the subscriber line and ensures that the router executes QoS features on the actual bandwidth used by ATM packets.

Finding Feature Information

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

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

Prerequisites for Traffic Shaping Overhead Accounting for ATM

Traffic classes must be configured using the **class-map** command.

Restrictions for Traffic Shaping Overhead Accounting for ATM

- The overhead accounting type or value used within a policy map and between the parent policy map and the child policy map (in a hierarchical policy map structure) must be consistent.
- You must attach a policy map that is configured with ATM overhead accounting to only an Ethernet interface (or an IP session on an Ethernet interface).
- Ethernet overhead accounting allows the automatic inclusion of downstream Ethernet frame headers in the shaped rate.
- If you enable overhead accounting on a child policy, you must enable overhead accounting on the parent policy.
- In a policy map, you must either enable overhead accounting for all classes in the policy or disable overhead accounting for all classes in the policy. You cannot enable overhead accounting for some classes and disable overhead accounting for other classes in the same policy.
- Overhead accounting is not reflected in any QoS counters (classification, policing, or queuing).
- Implicit ATM overhead accounting for policers are not supported.
- Implicit L2 overhead (ATM or otherwise) for policers are not supported for certain logical targets (tunnels) when the policy is applied to the logical target. The same limitation exists for queuing and scheduling overhead accounting.
- Police overhead cannot be configured on conditional policers (priority and rate), however, the priority queue it used will inherit the queueing overhead from parent shaper if configured.
- Police overhead is not added to the counters and are not reflected in statistics reported by the control plane.
- The overhead accounting type or value used by policing within a policy map and between the parent policy map and the child policy map (in a hierarchical policy map structure) must be consistent.
- The overhead accounting type or value used by queuing features within a policy map and between the parent policy map and the child policy map (in a hierarchical policy map structure) must be consistent.
- In releases preceding to Cisco IOS XE Release 3.9S, the router does not support overhead accounting updates on attached policies and the policy must be detached from the interface before the overhead can be modified, then the policy can be reattached to the interface.
- The router does not support overhead accounting for classes with fair-queue, which includes the following scenarios:
  - When used in conjunction with shape in the same class
  - When used in conjunction with bandwidth in the same class
  - When inherited from a parent or grandparent class through the Parent Level Overhead Accounting feature introduced in Cisco IOS XE Release 3.9S

Information About Traffic Shaping Overhead Accounting for ATM

Benefits of Traffic Shaping Overhead Accounting for ATM

The Traffic Shaping Overhead Accounting for ATM feature enables the broadband aggregation system (BRAS) to account for various encapsulation types when applying QoS to packets. Typically, in Ethernet digital subscriber line (DSL) environments, the encapsulation from the BRAS to the DSLAM is Gigabit Ethernet and the encapsulation from the DSLAM to the CPE is ATM. ATM overhead accounting enables the BRAS to account for ATM encapsulation on the subscriber line and for the overhead added by cell segmentation. This functionality enables the service provider to prevent overruns at the subscriber line and ensures that the router executes QoS features on the actual bandwidth used by ATM subscriber traffic.

BRAS and Encapsulation Types

Broadband aggregation system (BRAS) uses the encapsulation type that is configured for the DSLAM-CPE side to calculate the ATM overhead per packet.

DSLAM-CPE encapsulation types are based on Subnetwork Access Protocol (SNAP) and multiplexer (MUX) formats of ATM adaptation layer 5 (AAL5), followed by routed bridge (RBE), x-1483, x-dot1q-rbe, IP, PPP over Ethernet (PPPoE), or PPP over ATM (PPPoA) encapsulations. Because the DSLAM treats IP and PPPoE packets as payload, the BRAS does not account for IP and PPPoE encapsulations.

On the BRAS-DSLAM side, encapsulation is IEEE 802.1Q VLAN or Q-in-Q (qinq). However, because the DSLAM removes the BRAS-DSLAM encapsulation, the BRAS does not account for 802.1Q or qinq encapsulation.

AAL5 segmentation processing adds the additional overhead of the 5-byte cell headers, the AAL5 Common Part Convergence Sublayer (CPCS) padding, and the AAL5 trailer. For more information, see the ATM Overhead Calculation, on page 52.

Subscriber Line Encapsulation Types

The router supports the following subscriber line encapsulation types:

- snap-rbe
- mux-rbe
- snap-dot1q-rbe
- mux-dot1q-rbe
- snap-pppoa
- mux-pppoa
- snap-1483routed
- mux-1483routed

- snap-rbe-dot1q
- mux-rbe-dot1q

Note The encapsulation types listed above are for AAL5, qinq, and dot1q encapsulations. User-defined encapsulations with offsets based on the platform in use are also supported.

ATM Overhead Calculation

The Traffic Shaping Overhead Accounting for ATM feature prevents oversubscription of a subscriber line by accounting for the ATM encapsulation overhead at the BRAS. When calculating the ATM overhead, the Traffic Shaping Overhead Accounting for ATM feature considers the following:

- The encapsulation type used by the BRAS
- The CPCS trailer overhead
- The encapsulation type used between the DSLAM and the CPE

The offset size (a parameter used to calculate ATM overhead accounting) is calculated using the following formula:

Offset size in bytes = (CPCS trailer overhead) + (DSLAM to CPE) - (BRAS encapsulation type)

See the table below for the offset sizes, in bytes, derived from this formula.

This offset size, along with the packet size and packet assembler/disassembler (PAD) byte overhead in the CPCS, is used by the router to calculate the ATM overhead accounting rate.

Note A CPCS trailer overhead of 8 bytes corresponds to AAL5. A CPCS trailer overhead of 4 bytes corresponds to AAL3, but AAL3 is not supported.

Table 7: Offset Sizes, in Bytes, Used for ATM Overhead Calculation

Encapsulation Type in Use	BRAS	CPCS Trailer Overhead	DSLAM to CPE	Offset Size
dot1q mux-1483routed	18	8	3	-7
dot1q snap-1483routed	18	8	6	-4
dot1q mux-rbe	18	8	14	4
dot1q snap-rbe	18	8	24	14
dot1q mux-dot1q-rbe	18	8	18	8
dot1q snap-dot1q-rbe	18	8	28	18
qot1q mux-pppoa	18 + 6	8	2	-14

Encapsulation Type in Use	BRAS	CPCS Trailer Overhead	DSLAM to CPE	Offset Size
qot1q snap-pppoa	18 + 6	8	4	-12
qinq mux-1483routed	22	8	3	-11
qinq snap-1483routed	22	8	6	-8
qinq mux-rbe	22	8	14	0
qinq snap-rbe	22	8	24	10
qinq mux-dot1q-rbe	22	8	18	4
qing snap-dot1q-rbe	22	8	28	14
qinq mux-pppoa	22 + 6	8	2	-18
qinq snap-pppoa	22 + 6	8	4	-16

ATM Overhead Accounting and Hierarchical Policies

In hierarchical policies, you can enable ATM overhead accounting for shaping and bandwidth on parent policies and child policies. You are not required to enable ATM overhead accounting on a traffic class that does not contain the **bandwidth** or **shape** command. If you enable ATM overhead accounting on a child policy, then you must enable ATM overhead accounting on the parent policy. The parent and child classes must specify the same encapsulation type when ATM overhead accounting is enabled.

Overhead Accounting and Priority Queues

Overhead accounting configuration is supported for queuing features (shape, bandwidth and priority) and non-queuing feature (police) separately. However, priority queue can be integrated with policer. When overhead accounting is configured on a priority queue, through inheritance, it operates in the following fashion:

- Overhead accounting is added to (or subtracted from) the priority packet for queuing features in the hierarchy (for example, shape in the parent class).
- Overhead accounting is not added to the packet for priority rate enforcement (**priority** {*bandwidth-kbps* | **percent** *percentage*} [**burst**]). Although policing overhead accounting is supported, it does not apply to the conditional policer (rate enforcement is implemented through this conditional policer).

How to Configure Traffic Shaping Overhead Accounting for ATM

Configuring Traffic Shaping Overhead Accounting for ATM in a Hierarchical Policy

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map** *policy-map-name*
4. **class** *class-map-name*
5. bandwidth {bandwidth-kbps | percent percentage | remaining percent percentage} account {{qinq | dot1q} {**aal5** | **aal3**} {subscriber-encapsulation}} | {user-defined offset [atm]}}
6. **bandwidth remaining ratio** *ratio* [**account** {**qinq** | **dot1q**} [**aal5**|**aal3**] {*subscriber-encapsulation* | **user-defined***offset*[atm]}]
7. **shape** [**average** |**peak**] mean-*rate*[*burst-size*] [*excess-burst-size*] account {{{qinq | dot1q} {aal5 | aal3} {subscriber-encapsulation}} | {user-defined offset [atm]}}
8. **end**

DETAILED STEPS

	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 Business`	Creates or modifies the child policy and enters policy-map configuration mode. • Enter the policy map name. This is the name of the child policy.
Step 4	**class** *class-map-name* **Example:** `Router(config-pmap)# class video`	Assigns the traffic class that you specify for the policy map and enters policy-map class configuration mode. • Enter the traffic class name. This is the name of the previously configured class map.

	Command or Action	Purpose
Step 5	bandwidth {bandwidth-kbps | percent percentage | remaining percent percentage} account {{qinq | dot1q} {**aal5** | **aal3**} {subscriber-encapsulation}} | {user-defined offset [atm]}} **Example:** `Router(config-pmap-c)# bandwidth 8000 account dot1q aal5 snap-pppoa`	Enables Class-Based Weighted Fair Queueing (CBWFQ) on the basis of the keywords and arguments specified, such as the following: • *bandwidth-kbps* --Specifies or modifies the minimum bandwidth allocated for a class that belongs to a policy map. Valid values are from 8 to 2488320, which represents from 1 to 99 percent of the link bandwidth. • **percent** *percentage* --Specifies or modifies the minimum percentage of the link bandwidth allocated for a class that belongs to a policy map. Valid values are from 1 to 99. • **remaining percent** *percentage* --Specifies or modifies the minimum percentage of unused link bandwidth allocated for a class that belongs to a policy map. Valid values are from 1 to 99. • **account** --Enables ATM overhead accounting. • **qinq** --Specifies queue-in-queue encapsulation as the BRAS-DSLAM encapsulation type. • **dot1q** --Specifies IEEE 802.1Q VLAN encapsulation as the BRAS-DSLAM encapsulation type. • **aal5** --Specifies the ATM adaptation layer 5 that supports connection-oriented variable bit rate (VBR) services. • **aal3** --Specifies the ATM adaptation layer 5 that supports both connectionless and connection-oriented links. • *subscriber-encapsulation* --Specifies the encapsulation type at the subscriber line. For more information, see the Subscriber Line Encapsulation Types, on page 51. • **user-defined** --Specifies the offset size that the router uses when calculating the ATM overhead. • *offset* --Specifies the offset size when calculating ATM overhead. Valid values are from -63 to +63 bytes. • **atm** --(Optional) Applies the ATM cell tax in the ATM overhead calculation.
Step 6	**bandwidth remaining ratio** *ratio* [**account** {**qinq** | **dot1q**} [**aal5**|**aal3**] {*subscriber-encapsulation* | **user-defined***offset*[atm]}] **Example:**	(Optional) Specifies the bandwidth-remaining ratio for the subinterface along with ATM accounting parameters: • *ratio* --Specifies the bandwidth-remaining ratio for the subinterface. Valid values are 1 to 100. The default value is 1.

	Command or Action	Purpose
	`Router(config-pmap-c)# bandwidth remaining ratio 10 account dot1q aal5 snap-pppo`	**Note** For the Cisco 7600 series router, valid values are from 1 to 10000. The default value is 1. • **account** --Enables ATM overhead accounting. • **qinq** --Specifies queue-in-queue encapsulation as the BRAS-DSLAM encapsulation type. • **dot1q** --Specifies IEEE 802.1Q VLAN encapsulation as the BRAS-DSLAM encapsulation type. • **aal5** --Specifies the ATM adaptation layer 5 that supports connection-oriented VBR services. • **aal3** --Specifies the ATM adaptation layer 5 that supports both connectionless and connection-oriented links. • *subscriber-encapsulation* --Specifies the encapsulation type at the subscriber line. For more information, see the Subscriber Line Encapsulation Types, on page 51. • **user-defined** --Specifies the offset size that the router uses when calculating the ATM overhead. • *offset* --Specifies the offset size, in bytes, when calculating ATM overhead. Valid values are from -63 to +63. • **atm** --(Optional) Applies the ATM cell tax in the ATM overhead calculation.
Step 7	**shape** [**average** |**peak**] mean-*rate*[*burst-size*] [*excess-burst-size*] account {{{qinq | dot1q} {aal5 | aal3} {subscriber-encapsulation}} | {user-defined offset [atm]}} **Example:** `Router(config-pmap-c)# shape 8000 account qinq aal5 snap-dot1q-rbe`	Shapes traffic to the indicated bit rate and enables ATM overhead accounting on the basis of the keywords and arguments specified, such as the following: • **average** --(Optional) The committed burst (Bc) that specifies the maximum number of bits sent out in each interval. • **peak** --(Optional) Specifies the maximum number of bits sent out in each interval (the Bc + excess burst [Be]). The Cisco 10000 router and the SIP400 (on the Cisco 7600 series router) do not support this option. • *mean-rate* --Also called committed information rate (CIR). Indicates the bit rate used to shape the traffic, in bits per second. • *burst-size* --(Optional) The number of bits in a measurement interval (Bc). • *excess-burst-size* --(Optional) The acceptable number of bits permitted to go over the Be.

	Command or Action	Purpose
		• **account** --Enables ATM overhead accounting. • **qinq** --Specifies queue-in-queue encapsulation as the BRAS-DSLAM encapsulation type. • **dot1q** --Specifies IEEE 802.1Q VLAN encapsulation as the BRAS-DSLAM encapsulation type. • **aal5** --The ATM adaptation layer 5 that supports connection-oriented variable bit rate (VBR) services. • **aal3** --Specifies the ATM Adaptation Layer 5 that supports both connectionless and connection-oriented links. You must specify either aal3 or aal5. • *subscriber-encapsulation* --Specifies the encapsulation type at the subscriber line. For more information, see the Subscriber Line Encapsulation Types, on page 51. • **user-defined** --Specifies the offset size that the router uses when calculating the ATM overhead. • *offset* --Specifies the offset size when calculating ATM overhead. Valid values are from -63 to +63 bytes. • **atm** --(Optional) Applies ATM cell tax in the ATM overhead calculation. Configuring both the *offset* and the **atm** options adjusts the packet size to the offset size and then adds ATM cell tax.
Step 8	**end** **Example:** `Router(config-pmap-c)# end`	Exits policy-map class configuration mode and returns to privileged EXEC mode.

Verifying the Configuration of Traffic Shaping Overhead Accounting for ATM

SUMMARY STEPS

1. **enable**
2. **show policy-map** [*policy-map-name*]
3. **show policy-map session**
4. **show running-config**
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router> enable`	• Enter your password if prompted.
Step 2	**show policy-map** [*policy-map-name*] **Example:** `Router# show policy-map unit-test`	(Optional) Displays the configuration of all classes for a specified policy map or of all classes for all existing policy maps. • (Optional) Enter the policy map name.
Step 3	**show policy-map session** **Example:** `Router# show policy-map session`	(Optional) Displays the QoS policy map in effect for an IPoE/PPPoE session.
Step 4	**show running-config** **Example:** `Router# show running-config`	(Optional) Displays the contents of the currently running configuration file.
Step 5	**exit** **Example:** `Router# exit`	Exits privileged EXEC mode.

Configuration Examples for Traffic Shaping Overhead Accounting for ATM

Example Enabling Traffic Shaping Overhead Accounting for ATM

The following example shows how to enable ATM overhead accounting using a hierarchical policy map structure. The Child policy map has two classes: Business and Non-Business. The Business class has priority and is policed at 128,000 kbps. The Non-Business class has ATM overhead accounting enabled and has a bandwidth of 20 percent of the available bandwidth. The Parent policy map shapes the aggregate traffic to 256,000 kbps and enables ATM overhead accounting.

Notice that Layer 2 overhead accounting is not explicitly configured for the Business traffic class. If the class-default class of a parent policy has ATM overhead accounting enabled, you are not required to enable ATM overhead accounting on a child traffic class that does not contain the **bandwidth** or **shape** command. Therefore, in this example, the Business priority queue implicitly has ATM overhead accounting enabled because its parent class-default class has overhead accounting enabled.

```
policy-map Child
 class Business
  priority
  police 128000
 class Non-Business
```

```
  bandwidth percent 20 account dot1q aal5 snap-rbe-dot1q
  exit
 exit
policy-map Parent
 class class-default
  shape 256000 account dot1q aal5 snap-rbe-dot1q
  service-policy Child
```

In the following example, overhead accounting is enabled for bandwidth on the gaming and class-default class of the child policy map named subscriber_classes and on the class-default class of the parent policy map named subscriber_line. The voip and video classes do not have accounting explicitly enabled; these classes have ATM overhead accounting implicitly enabled because the parent policy has overhead accounting enabled. Notice that the features in the parent and child policies use the same encapsulation type.

```
policy-map subscriber_classes
 class voip
  priority level 1
  police 8000
 class video
  priority level 2
  police 8000
 class gaming
  bandwidth remaining percent 80 account dot1q aal5 snap-rbe-dot1q
 class class-default
  bandwidth remaining percent 20 account dot1q aal5 snap-rbe-dot1q
policy-map subscriber_line
 class class-default
  bandwidth remaining ratio 10 account dot1q aal5 snap-rbe-dot1q
  shape average 512 account aal5 dot1q snap-rbe-dot1q
  service policy subscriber_classes
```

Example Verifying Traffic Shaping Overhead Accounting for ATM

```
Router# show policy-map interface

Service-policy output:unit-test
Class-map: class-default (match-any)
100 packets, 1000 bytes
30 second offered rate 800 bps, drop rate 0 bps
Match: any
shape (average) cir 154400, bc 7720, be 7720
target shape rate 154400
overhead accounting: enabled
bandwidth 30% (463 kbps)
overhead accounting: disabled
queue limit 64 packets
(queue depth/total drops/no-buffer drops) 0/0/0
(packets output/bytes output) 100/1000

Router# show policy-map session output

SSS session identifier 2 -
Service-policy output:  ATM_OH_POLICY
    Class-map: class-default (match-any)
      0 packets, 0 bytes
      30 second offered rate 0 bps, drop rate 0 bps
      Match: any
      Queueing
      queue limit 2500 packets
```

```
(queue depth/total drops/no-buffer drops) 0/0/0
(pkts output/bytes output) 0/0
shape (average) cir 10000000, bc 40000, be 40000
target shape rate 10000000
 Overhead Accounting Enabled
```

The following output from the **show running-config** command indicates that ATM overhead accounting is enabled for shaping. The BRAS-DSLAM encapsulation is dot1q and the subscriber line encapsulation is snap-rbe based on the AAL5 service.

```
subscriber policy recording rules limit 64
no mpls traffic-eng auto-bw timers frequency 0
call rsvp-sync
!
controller T1 2/0
framing sf
linecode ami
!
controller T1 2/1
framing sf
linecode ami
!
!
policy-map unit-test
class class-default
shape average percent 10 account dot1q aal5 snap-rbe
!
```

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, 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

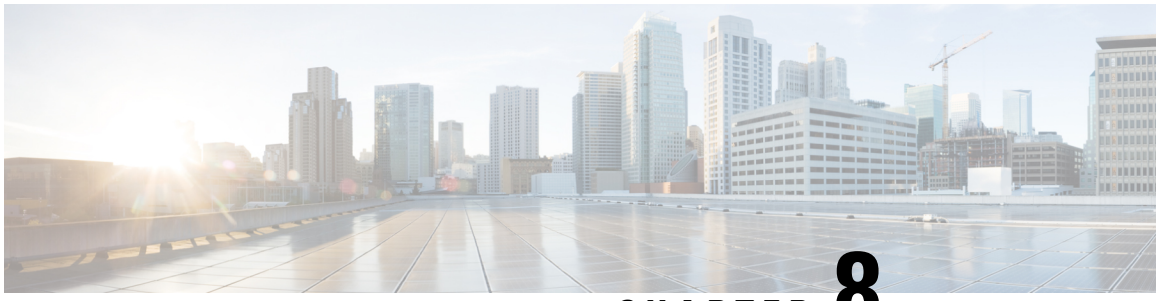
Feature Information for MQC Traffic Shaping Overhead Accounting for ATM

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

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

Table 8: Feature Information for MQC Traffic Shaping Overhead Accounting for ATM

Feature Name	Releases	Feature Information
MQC Traffic Shaping Overhead Accounting for ATM	Cisco IOS XE Release 2.4	The MQC Traffic Shaping Overhead Accounting for ATM feature enables a broadband aggregation system (BRAS) to account for various encapsulation types when applying QoS functionality to packets. The following commands were introduced or modified: **bandwidth (policy-map class)**, **bandwidth remaining ratio**, **shape (policy-map class)**, **show policy-map interface**, **show policy-map session**, **show running-config**.



CHAPTER 8

QoS Policy Accounting

The QoS Policy Accounting feature helps you accurately account for traffic on your system. It also provides greater flexibility in assigning quality of service (QoS) configurations to subscribers. In addition, the QoS Accounting High Availability feature ensures that QoS accounting statistics persist, and that the RADIUS accounting billing server continues to report accounting counters during planned and unexpected Route Processor (RP) switchovers. This module describes how to configure QoS policy accounting, use subscriber templates, and activate subscriber accounting accuracy.

Finding Feature Information

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

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

Prerequisites for QoS Policy Accounting

- PPP over Ethernet (PPPoE) or PPP over Ethernet over ATM (PPPoEoA) sessions are enabled.
- The RADIUS server is configured.
- Authentication, authorization, and accounting (AAA) is enabled.
- The subscriber's user profile on the RADIUS server has been created.

- A policy map is configured.
- A service template is configured.
- Traffic classes have been created.
- Stateful switchover (SSO) and In-service Software Upgrade (ISSU) prerequisites must be met. For more information, see the *Cisco IOS High Availability Configuration Guide*.

Restrictions for QoS Policy Accounting

- In system failover, the following occurs:
  - For QoS accounting configured statically at the policy map, QoS accounting statistics are reset to zero.
  - For QoS accounting configured dynamically using service templates, sessions no longer exist on the new active Route Processor (RP).

Note In Cisco IOS XE Release 3.5S and later releases, high availability (HA) support is available for accounting services enabled through a service template. Therefore, QoS accounting statistics and service sessions are preserved during a system failover and are available on the new active RP.

- Multicasting is not supported for QoS policy accounting services.
- The following QoS actions are not supported in service templates:
  - account
  - fair-queue
  - netflow-sampler
  - random-detect
- The following QoS filters are not supported in service templates:
  - atm
  - class-map
  - cos
  - destination-address
  - discard-class
  - fr-de
  - fr-dlci
  - input-interface
  - mpls
  - not
  - packet
  - source-address
  - vlan

- Service template definition lines may not exceed maximum configuration line length allowed by the Cisco IOS CLI. You may need to shorten shell variable names to stay within this limit.
- A template service activated on a session cannot be changed. Instead, you can deactivate it and activate a different template service.
- When a template service is active, a legacy complex parameterized string may not be used to change the QoS policy active on a session.
- IP address parameterization is supported only for IPv4 and only for named ACLs without remarks. IP addresses specified in the parameterized service activation are always added to the cloned ACL in this fixed pattern: "permit ip network mask any" and "permit ip any network mask".
- Service templates are supported only for PPP sessions and may not be activated on subinterfaces.
- Only one turbo button service can be active on a session at any given time. Turbo button service is any service that changes a QoS action other than “service-policy xxxx” (changing the child policy) in the class-default of the parent policy.
- Shell variables, QoS class map, and Access Control List (ACL) names may not have the following characters:
  - !
  - $
  - #
  - -
  - ,
  - >
  - <
- Service names are echoed back in the accounting records only for group accounting (when you use $_acctgrp in the service template).
- The IN/OUT QoS policy name active on a session is formed by concatenating the previously active QoS policy (or the static QoS policy specified in the last multiservice Change of Authorization (CoA) or Access-Accept).
- Two template services instantiated from the same service template may not be activated on the session at the same time. However, multiple template services instantiated from unrelated service templates can be active on a session at the same time.
- Template service support is available only for locally terminated PPP and PPP forwarded sessions on the Layer 2 Tunneling Protocol (L2TP) Access Concentrator (LAC).
- For PPP forwarded sessions on the LAC, to apply template services via Access-Accept, use the following configurations:
  - vpdn authen-before-forward.
  - Specify template services only in the user authorization profile (Access-Accept that is received after PPP authentication), not in the authentication profile.
- Only activate template services on the child policy under the parent class-default (only two levels) and on the parent policy (Turbo Button service).
- The default QoS policy can be only two levels deep (Parent + Child under class-default) and should not have a child policy configured under any class other than the class-default.

- A child policy should be configured under the default parent policy class-default in order for template services to be activated at the child level.
- Only rollback due to syntax error checking is supported.
- When multiple service activations or deactivations are included in a single CoA message, the failure of any operation (activation or deactivation) means that the CoA must roll back (undo) all previous operations to restore the session state to what it was before the CoA processing started. In other words, either all the operations must be processed successfully in a CoA or none at all. A CoA negative ACK (NACK) is sent to the RADIUS.
- For rollback to work during Access-Accept processing, subscriber service multiple-accept processing must be configured. The failure to process a service in an Access-Accept should roll back (undo) all previous services in the Access-Accept. The session will come up even if Access-Accept service processing fails.
- Errors originating in the platform or data plane will not trigger rollback which can result in an incomplete service.
- Do not modify a service template if its template services are in use or active on sessions. Use the **show subscriber policy ppm-shim-db** command to display which template services are in use.

Information About QoS Policy Accounting

RADIUS is a networking protocol that provides AAA management. Among other things, each RADIUS accounting message includes ingress and egress counters. The QoS Policy Accounting feature helps you resolve any inaccuracies between counters.

QoS Policy Accounting Feature in Groups

The QoS Policy Accounting feature collects and reports the following information to the RADIUS server per-session:

- Acct-Session-Id
- Ingress and egress packets/bytes/gigawords, packets, and bytes of successfully transmitted packets
- Parent-Session-Id
- Policy name and class or group name (if the QoS Policy Accounting feature is enabled on the group)
- Service name
- Username

When you enable the QoS Policy Accounting feature on a group and assign it a group name, this feature aggregates packets that meet the following criteria:

- Classified by traffic classes in the same group
- Included in the ingress or egress QoS policy applied on the same target

Separate Accounting Streams

If you do not assign a traffic class to a group, but instead assign it to an AAA method list, separate QoS policy accounting streams are created for each traffic class. Separate accounting streams allow you to differentiate between traffic that matches more than one class. Each unique target, direction, policy name, and class name has a unique RADIUS Acct-Session-Id value.

Service Templates

Service templates allow you to dynamically change QoS parameters without defining a new QoS policy on the CLI. You can change QoS policy when a session begins or any time after the session is established. Before you dynamically modify an active QoS deactivate the current service.

To understand service templates, learn the following terms:

- Service templates:
  - Are Cisco IOS shell functions
  - Have IN QoS policy-map definitions
  - Have OUT QoS policy-map definitions
  - Are programmatically invoked
  - Specify default values for shell variables
- Template services:
  - Are QoS service names with a parenthesis in them
  - Have a matching shell-map template definition
  - Are created dynamically during service template shell function execution
- IN Net effect policy map
- OUT Net effect policy map

The QoS Policy Accounting feature, describes how the Cisco IOS shell overrides default values of variables used in service template shell functions. QoS policy definitions inside a shell map may have shell variables in place of QoS action parameter values.

Using Service Templates

To create a service template, you write the service template in a text editor and you then copy the template to the CLI. The contents of a shell map block are treated as text.

When you define the service-template policy maps (policy map $_outgoing/$_incoming), there is no CLI help or prompts available. For example you cannot access the following CLI aids:

- Parser auto completion
- Command options
- Range help
- Syntax checking

Note There is no editor available to you in the CLI, if you make a mistake you must delete the entire service template and then configure it again from the start.

Verifying Service Templates

When you write a service template in a text editor you do not have a syntax checking facility. Therefore, before you activate your service template, you must verify its syntax. The following code sample shows how to verify the *voice-service1* service template. To verify your own template, replace *voice-service1* with your service template name.

```
(shell map voice-service1 police_rate=100000 prec_value=4 queue_size=1)
configure terminal
no policy-map test-svc_IN <-------- Removes previous service template verifications.
no policy-map test-svc_OUT <-------- Removes previous service template verifications.
no aaa-accounting group test_svc_GRP <-------- Removes previous service template
verifications.
end
trigger voice-service1 _incoming=test-svc_IN _outgoing=test-svc_OUT _acctgrp=test-svc_GRP
show policy-map test-svc-IN <--------
Ensure that the output matches the expected service template template service with default
 values.
show policy-map test-svc-OUT <--------
Ensure that the output matches the expected service template template service with default
 values.
```

Removing Service Templates

To remove a service template, at the command line enter:

```
no shell map voice-service1 police_rate=100000 prec_value=4 queue_size=1 in_h=class-default
 out_h=class-default
```

Where voice-service1 is the name of your service template.

Sample Service Templates

Service Template

This example shows a sample service template:

```
{
    configure terminal
    accounting group $_acctgrp list default
    policy-map $_outgoing
      class voip
       police $police_rate 60625 0 conform-action transmit exceed-action drop violate-action
 drop
 exit
        priority level 1
        queue-limit 8 packets
        set precedence $prec_value
        set cos 6
        aaa-accounting group $_acctgrp
      class voip-control
       police 112000 1000 0 conform-action transmit exceed-action drop violate-action drop
```

```
        queue-limit $queue_size packets
        set precedence 6
        aaa-accounting group $_acctgrp
    policy-map $_incoming
      class voip
        police 200000 9216 0 conform-action transmit exceed-action transmit violate-action
 drop
        set precedence 5
        aaa-accounting group $_acctgrp
      class voip-control
       police 112000 21000 0 conform-action transmit exceed-action transmit violate-action
 drop
        set precedence 7
        aaa-accounting group $_acctgrp
}
```

Action Parameter Override

Action Parameter Override is a type of service template where shell variables are used in place of parameters for QoS actions such as police, shape, and bandwidth, configurations entered under a class in a QoS policy.

If you deactivate a template service, the system restores the previously active QoS policy. The QoS policy name may be different but is structurally and functionally identical to the QoS policy active before the template service was activated.

This example generates the service with the following parameters:

```
Reserved variable initialization before executing the service template shell function:
$_incoming = voice-service1>police_rate=200000#prec_value=5#queue_size=32<_IN
$_outgoing = voice-service1>police_rate=200000#prec_value=5#queue_size=32<_OUT
$_acctgrp = aaa-accounting group
voice-service1>police_rate=200000#prec_value=5#queue_size=32<_GRP list default
```

OUT QoS policy active on the session:

```
policy-map output_parent
 class class-default
   shape average 10000000
   service-policy output_child
policy-map output_child
class class-default
```

IN QoS policy active on the session:

```
policy-map input_parent
 class class-default
   police 10000000
   service-policy input_child
policy-map input_child
 class-default
```

After you activate voice-service1(police_rate=200000,prec_value=5,queue_size=32) on the target session, this is the active OUT policy:

```
policy-map
output_parent$class-default$voice-service1>police_rate=200000#prec_value=5#queue_size=32<_OUT$class-default

 class class-default
   shape average 10000000
   service-policy
```

```
output_child$voice-service1>police_rate=200000#prec_value=5#queue_size=32<_OUT$class-default
policy-map
output_child$voice-service1>police_rate=200000#prec_value=5#queue_size=32<_OUT$class-default

      class voip
        police 200000 60625 0 conform-action transmit exceed-action drop violate-action
drop
        priority level 1
        queue-limit 8 packets
        set precedence 5
        set cos 6
       aaa-accounting group voice-service1>police_rate=200000#prec_value=5#queue_size=32<_GRP

      class voip-control
       police 112000 1000 0 conform-action transmit exceed-action drop violate-action drop

        queue-limit 32 packets
        set precedence 6
       aaa-accounting group voice-service1>police_rate=200000#prec_value=5#queue_size=32<_GRP
class class-default
```

After you activate voice-service1(police_rate=200000,prec_value=5,queue_size=32) on the target session, this is the active IN policy:

```
policy-map
input_parent$class-default$voice-service1>police_rate=200000#prec_value=5#queue_size=32<_IN$class-default

 class class-default
   police cir 10000000 bc 312500 conform-action transmit exceed-action drop
   service-policy
input_child$voice-service1>police_rate=200000#prec_value=5#queue_size=32<_IN$class-default
policy-map
input_child$voice-service1>police_rate=200000#prec_value=5#queue_size=32<_IN$class-default
      class voip
        police 200000 9216 0 conform-action transmit exceed-action transmit violate-action
 drop
        set precedence 5
       aaa-accounting group voice-service1>police_rate=200000#prec_value=5#queue_size=32<_GRP

      class voip-control
       police 112000 21000 0 conform-action transmit exceed-action transmit violate-action
 drop
        set precedence 7
       aaa-accounting group voice-service1>police_rate=200000#prec_value=5#queue_size=32<_GRP

 class-default
```

Action Parameterization Default Parameters

Action Parameterization Default Paramters is a type of service template where shell variables are used in place of parameters for QoS actions such as police, shape, and bandwidth, configurations entered under a class in a QoS policy.

If you deactivate a template service, the system restores the previously active QoS policy. The QoS policy name maybe different but is structurally and functionally identical to the QoS policy active before the template service was activated.

OUT QoS policy active on the session:

```
policy-map output_parent
class class-default
   shape average 10000000
```

```
   service-policy output_child
policy-map output_child
class class-default
```

IN QoS policy active on the session:

```
policy-map input_parent
 class class-default
   police 10000000
   service-policy input_child
policy-map input_child
 class-default
ip access-list extended voip-acl
 permit ip 10.1.1.0 0.0.0.255 any
ip access-list extended voip-control-acl
 permit ip 10.2.2.0 0.0.0.255 any
class-map match-any voip
 match access-group name voip-acl
!
class-map match-any voip-control
 match access-group name voip-control-acl
!
shell map voice-service1 police_rate=100000 prec_value=4 queue_size=1 in_h=class-default
out_h=class-default
{
    configure terminal
    accounting group $_acctgrp list default
    policy-map $_outgoing
      class voip
       police $police_rate 60625 0 conform-action transmit exceed-action drop violate-action
 drop
 exit
       priority level 1
       queue-limit 8 packets
       set precedence $prec_value
       set cos 6
       aaa-accounting group $_acctgrp
      class voip-control
       police 112000 1000 0 conform-action transmit exceed-action drop violate-action drop

       queue-limit $queue_size packets
       set precedence 6
       aaa-accounting group $_acctgrp
    policy-map $_incoming
      class voip
       police 200000 9216 0 conform-action transmit exceed-action transmit violate-action
 drop
       set precedence 5
       aaa-accounting group $_acctgrp
      class voip-control
       police 112000 21000 0 conform-action transmit exceed-action transmit violate-action
 drop
       set precedence 7
       aaa-accounting group $_acctgrp
}
```

After you activate voice-service1 on the target session, this is the active OUT policy:

```
policy-map output_parent$class-default$voice-service1><_OUT$class-default class
  class-default
  shape average 10000000
  service-policy output_child$voice-service1><_OUT$class-default
policy-map output_child$voice-service1><_OUT$class-default
  class voip
   police 10000 60625 0 conform-action transmit exceed-action drop violate-action drop
```

```
   priority level 1
   queue-limit 8 packets
   set precedence 4
   set cos 6
   aaa-accounting group voice-service1><_GRP
  class voip-control
   police 112000 1000 0 conform-action transmit exceed-action drop violate-action drop
   queue-limit 16 packets
   set precedence 6
   aaa-accounting group voice-service1><GRP
 class class-default
```

After you activate voice-service1 on the target session, this is the active IN policy:

```
policy-map input_parent$class-default$voice-service1><_IN$class-default
 class class-default
 police cir 10000000 bc 312500 conform-action transmit exceed-action drop
 service-policy input_child$voice-service1><_IN$class-default
policy-map input_child$voice-service1><_IN$class-default
 class voip
  police 200000 9216 0 conform-action transmit exceed-action transmit violate-action drop
  set precedence 5
  aaa-accounting group voice-service1><_GRP
 class voip-control
  police 112000 21000 0 conform-action transmit exceed-action transmit violate-action drop
  set precedence 7
  aaa-accounting group voice-service1><_GRP
 class-default
```

Class Name Override

Class name override is a type of service template where shell variables are used in place of parameters for QoS actions such as police, shape, and bandwidth, configurations entered under a class in a QoS policy. Shell variables may also be used in place of class names in service template policy definitions. Shell variables may completely substitute a class name or may be configured as a variable suffix with a constant prefix.

If you deactivate a template service, the system restores the previously active QoS policy. The QoS policy name may be different but is structurally and functionally identical to the QoS policy active before the template service was activated.

OUT QoS policy active on the session:

```
policy-map output_parent
 class class-default
   shape average 10000000
   service-policy output_child
policy-map output_child
class class-default
```

IN QoS policy active on the session:

```
policy-map input_parent
 class class-default
   police 10000000
   service-policy input_child
policy-map input_child
 class-default
! Pre-configured ACLs/class-maps
ip access-list extended aol_classifier_acl         ! Locally pre-configured
 permit ip host 10.1.30.194 any
class-map match-all voice-control-aol_classifier_reference      ! Locally pre-configured
  match access-group name aol_classifier_acl
! Other pre-configured ACLs/classes here (e.g., voice-aol_classifier_reference,
voice-t_online, etc.)
```

```
! Service template:
shell map voice-aol-service1 prec_value=3 police_rate=100000 class_ref=t_online
in_h=class-default out_h=class-default
{
    configure terminal
    accounting group $_acctgrp list default
    policy-map $_outgoing
      class voice-control-$class_ref
       police 112000 1000 0 conform-action transmit exceed-action drop violate-action drop

        queue-limit 16 packets
        set precedence 6
        aaa-accounting group $_acctgrp
      class voice-$class_ref
       police $poice_rate 60625 0 conform-action transmit exceed-action drop violate-action
 drop
        priority level 1
        queue-limit 8 packets
        set precedence $prec_value
        set cos 6
        aaa-accounting group $_acctgrp
    policy-map $_incoming
      class voice-control-$class_ref
       police 112000 21000 0 conform-action transmit exceed-action transmit violate-action
 drop
        set precedence 7
        aaa-accounting group $_acctgrp
      class voice-$class_ref
        police 200000 9216 0 conform-action transmit exceed-action transmit violate-action
 drop
        set precedence $prec_value
        aaa-accounting group $_acctgrp
}
```

After you activate voice-aol-service1(class_ref=aol_classifier_reference) on the target session, this is the active OUT policy:

```
policy-map
output_parent$class-default$voice-aol-service1<class_ref=aol_classifier_reference>_OUT$class-default

 class class-default
    shape average 10000000
   service-policy
output_child$voice-aol-service1<class_ref=aol_classifier_reference>_OUT$class-default
policy-map
output_child$voice-aol-service1<class_ref=aol_classifier_reference>_OUT$class-default
      class voice-control-aol_classifier_reference     ! Reference to pre-configured class
        police 112000 1000 0 conform-action transmit exceed-action drop violate-action drop

        queue-limit 16 packets
        set precedence 6
        aaa-accounting group voice-aol-service1<class_ref=aol_classifier_reference>_GRP
      class voice-aol_classifier_reference     ! reference to pre-configured class
        police 100000 60625 0 conform-action transmit exceed-action drop violate-action
drop
        priority level 1
        queue-limit 8 packets
        set precedence 3
        set cos 6
        aaa-accounting group voice-aol-service1<class_ref=aol_classifier_reference>_GRP
class class-default
```

After you activate voice-aol-service1(class_ref=aol_classifier_reference) on the target session, this is the active IN policy:

```
policy-map
input_parent$class-default$voice-aol-service1<class_ref=aol_classifier_reference>_IN$class-default

 class class-default
    police cir 10000000 bc 312500 conform-action transmit exceed-action drop
   service-policy
input_child$voice-aol-service1<class_ref=aol_classifier_reference>_IN$class-default
policy-map input_child$voice-aol-service1<class_ref=aol_classifier_reference>_IN$class-default

      class voice-control-aol_classifier_reference     ! reference to pre-configured class
       police 112000 21000 0 conform-action transmit exceed-action transmit violate-action
 drop
        set precedence 7
        aaa-accounting group voice-aol-service1<class_ref=aol_classifier_reference>_GRP
      class voice-aol_classifier_reference     ! reference to pre-configured class
        police 200000 9216 0 conform-action transmit exceed-action transmit violate-action
 drop
        set precedence 3
        aaa-accounting group voice-aol-service1<class_ref=aol_classifier_reference>_GRP
       class-default
```

IP Address Parameterization

IP Address Parameterization is a type of Action Parameterization service template in which classifiers may be dynamically modified by adding more entries to ACLs. The entries to be added in an ACL are a list of IP addresses in a shell variable.

If you deactivate a template service, the system restores the previously active QoS policy. The QoS policy name may be different but is structurally and functionally identical to the QoS policy active before the template service was activated.

Note Classes must be predefined; they are not dynamically created.

OUT QoS policy active on the session:

```
policy-map output_parent
 class class-default
   shape average 10000000
   service-policy output_child
policy-map output_child
class class-default
```

IN QoS policy active on the session:

```
policy-map input_parent
 class class-default
   police 10000000
   service-policy input_child
policy-map input_child
 class-default
! Base ACLs:
ip access-list extended IPOne-control-acl     ! Base ACL locally pre-configured
  permit ip any host 10.0.132.118
  permit ip host 10.0.132.118 any
  permit ip any host 10.1.245.122
  permit ip host 10.1.245.122 any
```

```
ip access-list extended IPOne-combined-acl      ! Base ACL pre-configured
 permit ip any 10.0.132.0 0.0.0.127
 permit ip 10.0.132.0 0.0.0.127 any
 permit ip any 10.1.245.64 0.0.0.63
 permit ip 10.1.245.64 0.0.0.63 any
! Base class-maps:
class-map match-any voice-control      ! Base class map pre-configured
  match access-list name IPOne-control-acl      !   Match on the base ACL
class-map match-any voice      ! base class-map pre-configured
  match access-list name IPOne-combined-acl      !   Match on the base ACL
! Service template:
shell map voice-toi  prec_value=3 police_rate=100000 ip_list=10.2.1.0/28,10.2.1.0/29
in_h=class-default out_h=class-default
{
    configure terminal
    ! Class-map templates:
    classmap-template voice-control  $ip_list
    classmap-template voice  $ip_list
    ! Service parameter templates:
    policy-map $_outgoing
      class voice-control-$ip_list     ! class names MUST end with -$ip_list
        police 112000 1000 0 conform-action transmit exceed-action drop violate-action drop

        queue-limit 16 packets
        set precedence 6
        aaa-accounting group IPOne-aol
      class voice-$ip_list
       police $police_rate 60625 0 conform-action transmit exceed-action drop violate-action
 drop
        priority level 1
        queue-limit 8 packets
        set precedence $prec_value
        aaa-accounting group IPOne-aol
   policy-map $_incoming
      class voice-control-$ip_list
       police 112000 21000 0 conform-action transmit exceed-action transmit violate-action
 drop
        set precedence 7
        aaa-accounting group IPOne-aol
      class voice-$ip_list
        police 200000 9216 0 conform-action transmit exceed-action transmit violate-action
 drop
        set precedence $prec_value
        aaa-accounting group IPOne-aol
```

After you activate voice-toi(ip_list=10.1.30.0/28,10.1.40.0/29) on the target session, this is the active OUT QoS policy :

```
policy-map output_parent$class-default$
voice-toi>ip_list=10.1.30.0/28,10.1.40.0/29<_OUT$class-default
 class class-default
    shape average 10000000
   service-policy output_child$voice-toi>ip_list=10.1.30.0/28,10.1.40.0/29<_OUT$class-default
policy-map output_child$voice-toi>ip_list=10.1.30.0/28,10.1.40.0/29<_OUT$class-default
      class voice-control-10.1.30.0/28,10.1.40.0/29
        police 112000 1000 0 conform-action transmit exceed-action drop violate-action drop

        queue-limit 16 packets
        set precedence 6
        aaa-accounting group IPOne-aol
      class voice-10.1.30.0/28,10.1.40.0/29
        police 100000 60625 0 conform-action transmit exceed-action drop violate-action
drop
        priority level 1
        queue-limit 8 packets
```

```
        set precedence 3
        aaa-accounting group IPOne-aol
class class-default
```

After you activate voice-toi(ip_list=10.1.30.0/28,10.1.40.0/29) on the target session, this is the active IN QoS policy :

```
policy-map
input_parent$class-default$voice-toi>ip_list=10.1.30.0/28,10.1.40.0/29<_IN$class-default
 class class-default
    police cir 10000000 bc 312500 conform-action transmit exceed-action drop
   service-policy input_child$voice-toi>ip_list=10.1.30.0/28,10.1.40.0/29<_IN$class-default
policy-map input_child$voice-toi>ip_list=10.1.30.0/28,10.1.40.0/29<_IN$class-default
      class voice-control-10.1.30.0/28,10.1.40.0/29
       police 112000 21000 0 conform-action transmit exceed-action transmit violate-action
 drop
        set precedence 7
        aaa-accounting group IPOne-aol
      class voice-10.1.30.0/28,10.1.40.0/29
        police 200000 9216 0 conform-action transmit exceed-action transmit violate-action
 drop
        set precedence 3
        aaa-accounting group IPOne-aol
 class-default
```

Note The following configurations are dynamically created.

```
! Internally created ACLs:
ip access-list extended IPOne-control-acl-10.1.30.0/28,10.1.40.0/29
  permit ip any host 10.0.132.118
  permit ip host 10.0.132.118 any
  permit ip any host 10.1.245.122
  permit ip host 10.1.245.122 any
  permit ip 10.1.30.0 0.0.0.15 any  ! ACEs derived from $ip_list
  permit ip any  10.1.30.0 0.0.0.15
  permit ip 10.1.40.0 0.0.0.7 any
  permit ip any 10.1.40.0 0.0.0.7
ip access-list extended IPOne-combined-acl-10.1.30.0/28,10.1.40.0/29
  permit ip any 10.0.132.0 0.0.0.127
  permit ip 10.0.132.0 0.0.0.127 any
  permit ip any 10.1.245.64 0.0.0.63
  permit ip 10.1.245.64 0.0.0.63 any
  permit ip 10.1.30.0 0.0.0.15 any  ! ACEs derived from $ip_list
  permit ip any 10.1.30.0 0.0.0.15
  permit ip 10.1.40.0 0.0.0.7 any
  permit ip any 0.0.0.7 10.1.40.0
! internally created class-maps:
class-map match-any voice-control-10.1.30.0/28,10.1.40.0/29
   match access-group name IPOne-control-acl-10.1.30.0/28,10.1.40.0/29
class-map match-any voice-10.1.30.0/28,10.1.40.0/29
   match access-group name IPOne-combined-acl-10.1.30.0/28,10.1.40.0/29
```

Turbo Button Service

Turbo Button service is a type of Action Parameterization service template in which only policy parameters in the INPUT parent class-default and shape parameters in the OUT parent class-default can be dynamically modified.

This example shows how to create a service template for the Turbo Button service:

OUT QoS policy active on the session:

```
policy-map output_parent
 class class-default
   shape average 10000000
   service-policy output_child
policy-map output_child
class class-default
```

IN QoS policy active on the session:

```
policy-map input_parent
 class class-default
   police 10000000
   service-policy input_child
policy-map input_child
 class-default
```

```
shell map turbo-button in_police_val=20000000 $out_shape=20000000
configure terminal
accounting group $_acctgrp list default
policy-map $_outgoing
class class-default
shape average $out_shape
aaa-accounting group $_acctgrp
policy-map $_incoming
class class-default
police $in_police_val
aaa-accounting group $_acctgrp
```

Turbo Button Activation

This example shows how to activate the Turbo Button service using the default values.

OUT QoS policy active on the session:

```
policy-map output_parent
 class class-default
   shape average 10000000
   service-policy output_child
policy-map output_child
class class-default
```

IN QoS policy active on the session:

```
policy-map input_parent
 class class-default
   police 10000000
   service-policy input_child
policy-map input_child
 class-default
```

```
accounting group turbo-button>< list default

accounting group turbo-button>< list default
! Service outgoing:
 policy-map  turbo-button><_OUT
 class class-default
 shape average 20000000
 aaa-accounting group turbo-button>< list default
! Service incoming:
 policy-map  turbo-button><_IN
 class class-default
```

```
 police 20000000
aaa-accounting group turbo-button>< list default
```

After you activate the service on the target session, this is the active OUT policy:

```
policy-map output_parent$turbo-button><_OUT$
class-default$voice-service1>police_rate=200000#prec_value=5#queue_size=32<_OUT$class-default

 class class-default
 shape average 20000000
aaa-accounting group turbo-button>< list default
service-policy
output_child$voice-service1>police_rate=200000#prec_value=5#queue_size=32<_OUT$class-default
policy-map
output_child$voice-service1>police_rate=200000#prec_value=5#queue_size=32<_OUT$class-default
class voip
police 200000 60625 0 conform-action transmit exceed-action drop violate-action drop
 priority level 1
 queue-limit 8 packets
 set precedence 5
 set cos 6

aaa-accounting group voice-service1>police_rate=200000#prec_value=5#queue_size=32<_GRP
 class voip-control
 police 112000 1000 0 conform-action transmit exceed-action drop violate-action drop
 queue-limit 32 packets
 set precedence 6
aaa-accounting group voice-service1>police_rate=200000#prec_value=5#queue_size=32<_GRP
class class-default
```

After you activate the service on the target session, this is the active IN policy:

```
policy-map input_parent$turbo-button>
<_IN$class-default$voice-service1>police_rate=200000#prec_value=5#queue_size=32<_IN$class-default
class class-default
   police cir 20000000 bc 312500 conform-action transmit exceed-action drop
   aaa-accounting group turbo-button>< list default

service-policy
input_child$voice-service1>police_rate=200000#prec_value=5#queue_size=32<_IN$class-default
policy-map
input_child$voice-service1>police_rate=200000#prec_value=5#queue_size=32<_IN$class-default

   class voip
        police 200000 9216 0 conform-action transmit exceed-action transmit violate-action
 drop
        set precedence 5
       aaa-accounting group voice-service1>police_rate=200000#prec_value=5#queue_size=32<_GRP

   class voip-control
        police 112000 21000 0 conform-action transmit exceed-action transmit violate-action
 drop
        set precedence 7
       aaa-accounting group voice-service1>police_rate=200000#prec_value=5#queue_size=32<_GRP
class-default
```

Turbo Button Deactivation

This example shows how to deactivate the Turbo Button service using the default values of VSA 252 0c turbo-button().

OUT QoS policy active on the session:

```
policy-map output_parent
 class class-default
   shape average 10000000
   service-policy output_child
policy-map output_child
class class-default
```

IN QoS policy active on the session:

```
policy-map input_parent
 class class-default
   police 10000000
   service-policy input_child
policy-map input_child
 class-default
```

After you activate the service on the target session, this is the active OUT policy:

```
policy-map
output_parent$class-default$voice-service1>police_rate=200000#prec_value=5#queue_size=32<_OUT$class-default
class class-default
  shape average 10000000
  service-policy
output_child$voice-service1>police_rate=200000#prec_value=5#queue_size=32<_OUT$class-default
policy-map
output_child$voice-service1>police_rate=200000#prec_value=5#queue_size=32<_OUT$class-default

  class voip
   police 200000 60625 0 conform-action transmit exceed-action drop violate-action drop
   priority level 1
   queue-limit 8 packets
   set precedence 5
   set cos 6
   aaa-accounting group voice-service1>police_rate=200000#prec_value=5#queue_size=32<_GRP
  class voip-control
   police 112000 1000 0 conform-action transmit exceed-action drop violate-action drop
   queue-limit 32 packets
   set precedence 6
   aaa-accounting group voice-service1>police_rate=200000#prec_value=5#queue_size=32<_GRP

class class-default
```

After you activate the service on the target session, this is the active IN policy:

```
policy-map
input_parent$class-default$voice-service1>police_rate=200000#prec_value=5#queue_size=32<_IN$class-default

   class class-default
   police cir 10000000 bc 312500 conform-action transmit exceed-action drop
   service-policy
input_child$voice-service1>police_rate=200000#prec_value=5#queue_size=32<_IN$class-default

policy-map
input_child$voice-service1>police_rate=200000#prec_value=5#queue_size=32<_IN$class-default
  class voip
   police 200000 9216 0 conform-action transmit exceed-action transmit violate-action drop
   set precedence 5
   aaa-accounting group voice-service1>police_rate=200000#prec_value=5#queue_size=32<_GRP
  class voip-control
   police 112000 21000 0 conform-action transmit exceed-action transmit violate-action drop

   set precedence 7
   aaa-accounting group voice-service1>police_rate=200000#prec_value=5#queue_size=32<_GRP
  class-default
```

Turbo Button Override

This example shows how to activate the Turbo Button service using the default values of VSA 250 Aturbo-button(in_police_val=30000000, out_shape_val=30000000) (Activation from Access-Accept) or VSA 252 0b turbo-button(in_police_val=30000000, out_shape_val=30000000) (Activation from CoA).

OUT QoS policy active on the session:

```
policy-map output_parent
 class class-default
   shape average 10000000
   service-policy output_child
policy-map output_child
class class-default
```

IN QoS policy active on the session:

```
policy-map input_parent
 class class-default
   police 10000000
   service-policy input_child
policy-map input_child
 class-default
```

```
accounting group turbo-button>in_police_val=30000000#out_shape_val=30000000 list default

! Service outgoing:
 policy-map turbo-button>in_police_val=30000000#out_shape_val=30000000<_OUT
 class class-default
  shape average 30000000
  accounting group turbo-button>in_police_val=30000000#out_shape_val=30000000
! Service incoming:
  policy-map turbo-button>in_police_val=30000000#out_shape_val=30000000<_IN
  class class-default
   police 30000000
   accounting group turbo-button>in_police_val=30000000#out_shape_val=30000000
```

After you activate the service on the target session, this is the active OUT policy:

```
policy-map output_parent$turbo-button>
in_police_val=30000000#out_shape_val=30000000<_OUT$class-default$voice-service1>police_rate=200000#prec_value=5#queue_size=32<_OUT$class-default
class class-default
 shape average 20000000
 accounting group turbo-button>in_police_val=30000000#out_shape_val=30000000
 service-policy
output_child$voice-service1>police_rate=200000#prec_value=5#queue_size=32<_OUT$class-default

 policy-map
output_child$voice-service1>police_rate=200000#prec_value=5#queue_size=32<_OUT$class-default
class voip
 police 200000 60625 0 conform-action transmit exceed-action drop violate-action drop
 priority level 1
 queue-limit 8 packets
 set precedence 5
 set cos 6
 aaa-accounting group voice-service1>police_rate=200000#prec_value=5#queue_size=32<_GRP
class voip-control
 police 112000 1000 0 conform-action transmit exceed-action drop violate-action drop
 queue-limit 32 packets
 aaa-accounting group voice-service1>police_rate=200000#prec_value=5#queue_size=32<_GRP
class class-default
```

After you activate the service on the target session, this is the active IN policy:

```
policy-map
input_parent$turbo-button>in_police_val=30000000#out_shape_val=30000000<_IN$class-default$voice-service1>police_rate=200000#prec_value=5#queue_size=32<_IN$class-default
class class-default
 police cir 20000000 bc 312500 conform-action transmit exceed-action drop
 accounting group turbo-button>in_police_val=30000000#out_shape_val=30000000
 service-policy
input_child$voice-service1>police_rate=200000#prec_value=5#queue_size=32<_IN$class-default
policy-map
input_child$voice-service1>police_rate=200000#prec_value=5#queue_size=32<_IN$class-default
 class voip
  police 200000 9216 0 conform-action transmit exceed-action transmit violate-action drop
  set precedence 5
  aaa-accounting group voice-service1>police_rate=200000#prec_value=5#queue_size=32<_GRP
 class voip-control
  police 112000 21000 0 conform-action transmit exceed-action transmit violate-action drop
  set precedence 7
  aaa-accounting group voice-service1>police_rate=200000#prec_value=5#queue_size=32<_GRP
 class-default
```

Example Turbo Button Override Deactivation

This example shows how to deactivate the Turbo Button override using the default values of VSA 252 0c turbo-button (in_police_val=30000000, out_shape_val=30000000).

OUT QoS policy active on the session:

```
policy-map output_parent
 class class-default
   shape average 10000000
   service-policy output_child
policy-map output_child
class class-default
```

IN QoS policy active on the session:

```
policy-map input_parent
 class class-default
   police 10000000
   service-policy input_child
policy-map input_child
 class-default
```

After you activate the service on the target session, this is the active OUT policy:

```
policy-map
output_parent$class-default$voice-service1>police_rate=200000#prec_value=5#queue_size=32<_OUT$class-default


 class class-default
  shape average 10000000
  service-policy
output_child$voice-service1>police_rate=200000#prec_value=5#queue_size=32<_OUT$class-default
policy-map
output_child$voice-service1>police_rate=200000#prec_value=5#queue_size=32<_OUT$class-default

  class voip
   police 200000 60625 0 conform-action transmit exceed-action drop violate-action drop
   priority level 1
   queue-limit 8 packets
   set precedence 5
   set cos 6
   aaa-accounting group voice-service1>police_rate=200000#prec_value=5#queue_size=32<_GRP
  class voip-control
   police 112000 1000 0 conform-action transmit exceed-action drop violate-action drop
   queue-limit 32 packets
```

```
   set precedence 6
   aaa-accounting group voice-service1>police_rate=200000#prec_value=5#queue_size=32<_GRP
  class class-default
```

After you activate the service on the target session, this is the active IN policy:

```
policy-map
input_parent$class-default$voice-service1>police_rate=200000#prec_value=5#queue_size=32<_IN$class-default

  class class-default
  police cir 10000000 bc 312500 conform-action transmit exceed-action drop
  service-policy
input_child$voice-service1>police_rate=200000#prec_value=5#queue_size=32<_IN$class-default
  policy-map
input_child$voice-service1>police_rate=200000#prec_value=5#queue_size=32<_IN$class-default
  class voip
   police 200000 9216 0 conform-action transmit exceed-action transmit violate-action drop
   set precedence 5
   aaa-accounting group voice-service1>police_rate=200000#prec_value=5#queue_size=32<_GRP
  class voip-control
   police 112000 21000 0 conform-action transmit exceed-action transmit violate-action drop

   set precedence 7
   aaa-accounting group voice-service1>police_rate=200000#prec_value=5#queue_size=32<_GRP
  class-default
```

Example Overriding Interim Accounting Interval

Overriding Interim Accounting Interval is a type of Action Parameterization service template in which you can use the shell variables in place of interim interval values in the accounting method list definition, allowing the account interim value to be dynamically modified.

This example shows how to do an accounting group override using the default values of: VSA 252 0b voice-service1(police_rate=200000,prec_value=5,acct_interval=600).

This example generates a service with the following parameters:

```
! Global AAA method list and accounting group parameters
aaa accounting network list-600
 action-type start-stop periodic interval 600
  accounting group voice-service1>policy_rate=200000#prec_value=5#acct_interval=600 <_GRP
list list-600
! OUT policy-map:
 policy-map voice-service1>policy_rate=200000#prec_value-5#acct_interval=600 <_OUT
  class voip
   police 200000 60625 0 conform-action transmit exceed-action drop violate-action drop
   priority level 1
   queue-limit 8 packets
   set precedence 5
   set cos 6
   aaa-accounting group voice-service1>policy_rate=200000#prec_value=5#acct_interval=600
<_GRP
  class voip-control
   police 112000 1000 0 conform-action transmit exceed-action drop violate-action drop
   queue-limit 32 packets
   set precedence 6
   aaa-accounting group


OUT:
policy-map output_parent
 class class-default
```

```
   shape average 10000000
   service-policy output_child
policy-map output_child
class class-default
IN:
policy-map input_parent
 class class-default
   police 10000000
   service-policy input_child
policy-map input_child
 class-default
```

After you activate the service on the target session, this is the active OUT policy:

```
policy-map
output_parent$class-default$voice-service1>policy_rate=200000#prev_value=5#acct_interval=600
 <_OUT$class-default
 class class-default
 shape average 10000000
 service-policy output_child$voice-service1>policy_rate=200000#prev_value=5#acct_interval=600
 <_OUT$class-default
 policy-map output_child$voice-service1>policy_rate=200000#prev_value=5#acct_interval=600
<_OUT$class-default
 class voip
  police 200000 60625 0 conform-action transmit exceed-action drop violate-action drop
  priority level 1
  queue-limit 8 packets
  set precedence 5
  set cos 6
  aaa-accounting group voice-service1>policy_rate=200000#prec_value=5#acct_interval=600
<_GRP
  class voip-control
  police 112000 1000 0 conform-action transmit exceed-action drop violate-action drop
  queue-limit 32 packets
  set precedence 6
  aaa-accounting group voice-service1>policy_rate=200000#prec_value=5#acct_interval=600
<_GRP
 class class-default
```

After you activate the service on the target session, this is the active IN policy:

```
policy-map
input_parent$class-default$voice-service1>policy_rate=200000#prec_value-5#acct_interval=600
 <_IN$class-default
class class-default
 police cir 10000000 bc 312500 conform-action transmit exceed-action drop
 service-policy input_child$voice-service1>policy_rate=200000#prec_value=5#acct_interval=600
 <_IN$class-default
policy-map input_child$voice-service1>policy_rate=200000#prec_value=5#acct_interval=600
<_IN$class-default
 class voip
  police 200000 9216 0 conform-action transmit exceed-action transmit violate-action drop
  set precedence 5
  aaa-accounting group voice-service1>policy_rate=200000#prec_value=5#acct_interval=600
<_GRP
 class voip-control
  police 112000 21000 0 conform-action transmit exceed-action transmit violate-action drop
  set precedence 7
  aaa-accounting group voice-service1>policy_rate=200000#prec_value=5#acct_interval=600
<_GRP
 class class-default
```

Subscriber Accounting Accuracy

The Subscriber Accounting Accuracy feature guarantees that the I/O packet/byte statistics in the Accounting-Stop record are accurate to within one second.

Subscriber accounting data is sent to authentication, authorization, and accounting (AAA) servers during the following events:

- Configured intervals during the lifetime of the session or service
- Service logoff
- Session tear down

Use the **subscriber accounting accuracy** *milliseconds* command to set the value for the Subscriber Accounting Accuracy feature.

Change of Authorization (CoA) ACK Ordering

CoA ACK ordering sends a CoA-ACK for each CoA event before a QoS accounting record is sent for that CoA. A CoA may contain activation or deactivation of single or multiple services.

If a service fails to install on a session the following happens:

- The entire CoA fails.
- The Policy Manager sends a CoA-NAK to the RADIUS server.
- The previous service configuration is restored

If one or more services install before a failure is detected the following happens:

- The entire CoA fails.
- Services are backed out.
- The Policy Manager sends a CoA-NAK to the RADIUS server.
- The previous service configuration is restored.

Multiservice CoAs can compose up of either of the following:

- QoS services—The Policy Manager combines the services into one net-effect policy map. Only one QoS policy is applied to the session for all services. If the policy fails to install, the system restores the session to use the previous policy map. In effect the session is restored to the state prior to the CoA.
- QoS and Intelligent Services Gateway (ISG) services—The Policy Manager applies the ISG service first, then the QoS service. If the QoS policy fails to install, the system restores the session to the previous policy map. Both the ISG and QoS service are rolled back to the previous state.

For multiservice CoA only one CoA-ACK is sent when all services successfully install.

Change of Authorization Rollback

The CoA Rollback feature restores QoS policy accounting to its state before the CoAs were issued. CoA Rollback also properly acknowledges the RADIUS server using a CoA-NAK.

The CoA Rollback feature applies to syntax mistakes and policy install failures such as admission control and resource allocation failure.

If CoA fails, the system sends a CoA-NAK and does not send QoS accounting records. The accounting record for existing services keeps previous counters and continues to count new packets.

QoS Accounting High Availability

When QoS accounting is enabled in a class the policy accounting feature supports three types of events:

- Start—Indicates a new accounting flow. The start record contains statistics and attributes specific to this flow.
- Interim—Indicates how often flow statistics are reported.
- Stop—Indicates the end of an accounting flow. The stop record also contains statistics and attributes specific to this flow.

The policy accounting feature collects the statistics for the accounting flows and sends the information to the RADIUS accounting billing server.

The QoS accounting high availability feature ensures that the start, interim, and stop accounting records are not affected if a planned or unexpected failover occurs. When a planned or unexpected failover occurs the QoS accounting HA feature ensures that the RP switchover occurs without interrupting the flow of information to the RADIUS accounting billing server. The feature also ensures that all QoS services on all active sessions continue without any interruption and that the service accounting counters persist across the RP switchover.

Persistence of Policy Accounting States

To ensure that start, stop, and interim accounting is not affected by a stateful switchover (SSO) or an in-service software upgrade (ISSU), the Policy Manager synchronizes all QoS services and parameterized CoA functionality with the standby RP at the time of the failover. In addition, the dynamic QoS configurations and the polling interval are synchronized between the active and standby RPs.

To synchronize a parameterized CoA event to a standby RP, the Policy Manager performs the following functions:

- Manages the CoA replay to synchronize provisioning events on the standby RP.
- Uses the same service template on both the active and standby RP.
- Creates the same policy map and class map names to apply to the session on both the active ad standby RP.
- Uses predefined QoS policy maps and class maps during service template activation.

Persistence of Policy Accounting Counters

The QoS Accounting HA feature ensures that the policy accounting counters persist across an SSO or failover. After a switchover occurs, the standby RP becomes the active RP and accumulates the statistics from the previously active RP. If the newly active RP receives a periodic update after the switchover it generates an interim record using the statistics it accumulated plus the values from the periodic update. If the newly active RP does not receive a periodic update after the switchover, it generates the interim record using only the statistics it accumulated from the previously active RP.

For more information on SSOs and ISSUs, see the *Cisco IOS High Availability Configuration Guide*.

How to Use QoS Policy Accounting

To use QoS Policy Accounting you must assign a group or AAA method list to a traffic class, then you configure the service template for policy accounting, and finally you activate the subscriber accounting accuracy functionality.

Note By default, QoS Policy Accounting is not assigned to traffic classes.

Assigning a Group or AAA Method List to a Traffic Class

Before you begin

Ensure the group or AAA method list already exists. If you try to add an undefined group or AAA method list to a traffic class, you will receive an error message.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa authentication ppp** *list-name method1*
4. **aaa accounting network** *methodlist-name*
5. **action-type start-stop**
6. **periodic interval** *minutes*
7. **accounting group group_name** *list list-name*
8. **policy-map** *policy-map-name*
9. **class class-default**
10. **accounting aaa list** *list-name* [*group-name*]
11. **end**
12. **show policy-map session**
13. **show accounting group** *group-name*

DETAILED STEPS

	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.

	Command or Action	Purpose
Step 3	**aaa authentication ppp** *list-name method1* **Example:** `Router(config)# aaa authentication ppp group radius`	Specifies a valid AAA authentication method. • Group RADIUS enables global RADIUS authentication.
Step 4	**aaa accounting network** *methodlist-name* **Example:** `Router(config)# aaa accounting network list1`	Enables AAA of services when you use RADIUS. • The algorithm determining the interim interval for a class or group uses the method list specified here.
Step 5	**action-type start-stop** **Example:** `Router(config)# action-type start-stop`	Sends a start accounting notice at the beginning of a process and a stop accounting notice at the end of a process.
Step 6	**periodic interval** *minutes* **Example:** `Router(config)# periodic interval 1`	Adds the interim interval value (1 to 71,582 minutes) in the method list, if specified. • If you do not define an interim interval, the global value defined by AAA is used. • If the method list disables interim updates, the accounting flows using the method list do not generate an interim update.
Step 7	**accounting group group_name** *list list-name* **Example:** `Router(config)# accounting group group_name AAAmethodlist AAAmethodlist1`	Sets properties in the AAA method list. • You can make per-session changes to existing traffic classes by temporarily overwriting properties in the groups or AAA method lists to which they are assigned. This allows you to provide dynamic customized QoS configuration to each subscriber.
Step 8	**policy-map** *policy-map-name* **Example:** `Router(config)# policy-map p1`	Creates a policy map.
Step 9	**class class-default** **Example:** `Router(config)# class class-default`	Creates a traffic class.
Step 10	**accounting aaa list** *list-name* [*group-name*] **Example:** `Router(config)# accounting aaa list AAAmethodlist1`	Assigns the traffic class to a group or an AAA method list. • This example shows the QoS Policy Accounting feature enabled for instances of a traffic class using list AAAmethodlist1 with no group.

	Command or Action	Purpose
Step 11	**end** **Example:** `Router(config)# end`	Exits interface configuration mode and returns to privileged EXEC mode.
Step 12	**show policy-map session** **Example:** `Router# show policy-map session`	(Optional) Displays QoS Policy Accounting feature information for traffic classes with a group or an AAA method list.
Step 13	**show accounting group** *group-name* **Example:** `Router# show accounting group acc-group1`	(Optional) Displays all group-to-method list associations. • Enter a group name to view information specific to that group.

Activating Subscriber Accounting Accuracy

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **subscriber accounting accuracy** *milliseconds*
4. **end**

DETAILED STEPS

	Command or Action	Purpose
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	**subscriber accounting accuracy** *milliseconds* **Example:** `Device(config)# subscriber accounting accuracy 1000`	Sets the value for the Subscriber Accounting Accuracy feature.
Step 4	**end** **Example:**	Enters privileged EXEC mode.

	Command or Action	Purpose
	`Device(config)# end`	

Troubleshooting Service Templates

To troubleshoot any service template issues, you can display usage information for all template service policy maps on your router.

SUMMARY STEPS

1. **enable**
2. **show subscriber policy ppm-shim-db**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show subscriber policy ppm-shim-db** **Example:** `Router(config)# show subscriber policy ppm-shim-db`	Displays reference counts (usage) of all template service policy-maps and Net Effect policy-maps on the router.

Configuration Examples for QoS Policy Accounting

Example: Using the QoS Policy Accounting Feature in Groups

The following example shows grouping:

```
policy-map my-policy
class voip
police
aaa-accounting group premium-services
class voip-control
police
aaa-accounting group premium-services
```

Example: Generating Separate Accounting Streams

The following example shows two classifiers called class voip and class voip-control. The classifiers are assigned to one policy associated with one target. This configuration generates two separate QoS policy accounting streams.

```
policy-map my-policy
class voip
police 200000
accounting aaa list AAA-LIST
class voip-control
police 100000
accounting aaa list AAA-LIST
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
QoS commands	*Cisco IOS QoS Command Reference*
Cisco IOS High Availability	*Cisco IOS High Availability Configuration Guide*

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 software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 2866	RADIUS Accounting

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

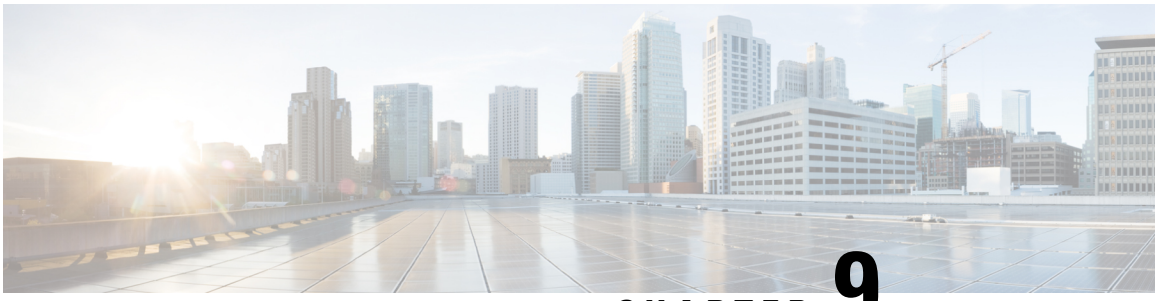
Feature Information for the QoS Policy Accounting Feature

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

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

Table 9: Feature Information for the QoS Policy Accounting Feature

Feature Name	Releases	Feature Information
QoS Accounting HA	Cisco IOS XE Release 3.5S	The QoS Accounting High Availability (HA) feature ensures that QoS accounting statistics persist, and that the RADIUS accounting billing server continues to report accounting counters during planned and unexpected Route Processor (RP) switchovers. In Cisco IOS XE Release 3.5S, this service was introduced on the Cisco ASR 1000 Series Aggregation Services Routers. The following command was modified: **debug qos accounting**
QoS Policy Accounting	Cisco IOS XE Release 2.6 Cisco IOS XE Release 3.2S Cisco IOS XE Release 3.8S	The QoS Policy Accounting feature helps you accurately account for traffic on your system. It also provides greater flexibility in assigning QoS configurations to subscribers. Static CLI-driven accounting is supported. In Cisco IOS XE Release 2.6, this feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers. In Cisco IOS XE Release 3.2S, the service template, subscriber subsecond accuracy, dynamic CoAs, and uninterrupted accounting in case of services untouched by the dynamic activation are supported. The following commands were added: **show subscriber policy ppm-shim-db** and **subscriber accounting accuracy**.



CHAPTER 9

PPP Session Queueing on ATM VCs

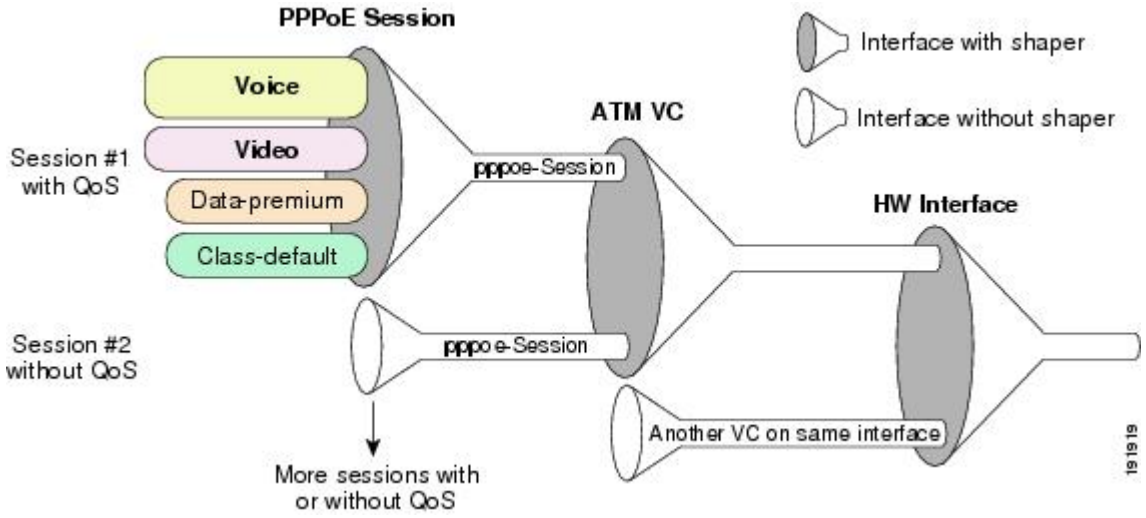
The PPP Session Queueing on ATM VCs feature enables you to shape and queue PPP over Ethernet over ATM (PPPoEoA) sessions to a user-specified rate. Multiple sessions can exist on any ATM VC and have Quality of Service (QoS) policies applied, or some of the sessions might have QoS policies. The router shapes the sum of allbandwidth used for PPPoEoA traffic on a VC so that the subscriber's connection to the Digital Subscriber Line Access Multiplexer (DSLAM) does not become congested. Queueing-related functionality provides different levels of service to the various applications that run over the PPPoEoA session.

A nested, two-level hierarchical service policy is used to configure session shaping directly on the router using the modular quality of service command-line interface (MQC). The hierarchical policy consists of the following:

- Child policy--Defines QoS actions using QoS commands such as the priority, bandwidth, and police commands.
- Parent policy--Contains only the class-default class with the shape or bandwidth remaining ratio command configured, or with both commands configured:
  - shape command--Shapes the session traffic to the specified bit rate, according to a specific algorithm.
  - bandwidth remaining ratio command--Specifies a ratio value that the router uses to determine how much unused bandwidth to allocate to the session during congestion.

Note The PPP Session Queueing on ATM VCs feature works with both PPP terminated aggregation (PTA) and L2TP access concentrator (LAC) configurations.

The figure below illustrates PPP session Queueing on ATM VCs.



Finding Feature Information

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

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

Prerequisites for PPP Session Queueing on ATM VCs

- PPPoEoA sessions must be enabled.
- Create traffic classes using the class-map command and specify the match criteria used to classify traffic.
- For dynamic PPPoEoA session queueing using RADIUS, you must:
  - Enable authentication, authorization, and accounting (AAA) on the router
  - Configure the RADIUS server for dynamic QoS
  - Create the subscriber's user profile on the RADIUS server

Restrictions for PPP Session Queueing on ATM VCs

- You cannot configure PPP session queueing on unshaped VCs--VCs without a specified peak cell rate (PCR) or sustained cell rate (SCR).
- VCs with session queueing polices cannot be part of a shaped virtual path (VP).
- If the same ATM category (for example, shaped unspecified bit rate (UBR)) contains both high and low bandwidth VCs, the SAR mechanism can cause low throughput for high bandwidth VCs. The workaround is to use different ATM classes for low and high bandwidth VCs. For example, configure low bandwidth VCs as shaped UBR and high bandwidth VCs as variable bit rate-nonreal-time (VBR-nrt) or constant bit rate (CBR).
- The CLASS-BASED QOS MIB does not include statistics for service policies applied to sessions.
- RADIUS accounting does not include queueing statistics.

Information About PPP Session Queueing on ATM VCs

Dynamically Applying QoS Policies to PPP Sessions on ATM VCs

The router allows you to dynamically apply QoS policy maps to PPPoEoA sessions using RADIUS. Although the actual configuration of the QoS policies occurs on the router, you can configure the following attribute-value (AV) pairs on RADIUS to specify the name of the policy map to dynamically apply to the session:

```
"ip:sub-qos-policy-in=<name of the QoS policy in ingress direction>"
"ip:sub-qos-policy-out=<name of egress policy>"
```

You define the AV pairs in one of the following RADIUS profiles:

- User profile--The user profile on the RADIUS server contains an entry that identifies the policy map name applicable to the user. The policy map name is the service that RADIUS downloads to the router after a session is authorized.
- Service profile--The service profile on the RADIUS server specifies a session identifier and an AV pair. The session identifier might be, for example, the IP address of the session. The AV pair defines the service (policy map name) to which the user belongs.

After receiving a service-logon request from the policy server, RADIUS sends a change of authorization (CoA) request to the router to activate the service for the subscriber, who is already logged in. If the authorization succeeds, the router downloads the name of the policy map from RADIUS using the ip:sub-qos-policy-in[out]= AV-pair and applies the QoS policy to the PPPoEoA session. Because the service policy contains queueing-related actions, the router sets up the appropriate class queues.

Note Although the router also supports the RADIUS vendor specific attribute (VSA) 38, Cisco-Policy-Down and Cisco-Policy-Up, we recommend that you use the ip:sub-qos-policy-in[out]= AV pairs for QoS policy definitions.

PPP Session Queueing Inheritance

PPP Sessions either inherit queues from their parent interface or they have their own queues. Each PPPoEoA session for which session queueing is configured has its own set of queues.

The table below describes the queues to which the router directs session traffic.

Table 10: PPP Session Queue Inheritance

Queueing Policy	Queue Used for Session Traffic
No policy	VC default queue
Applied to the VC	VC queues
Applied to the session	Session queues

Interfaces Supporting PPP Session Queueing

The router supports PPP session queueing on shaped ATM VCs for outbound traffic only.

The router does not support PPP session queueing on inbound ATM interfaces.

Mixed Configurations and Queueing

A mixed configuration is one in which all sessions do not have QoS applied to them. On some VCs, the queueing policy is applied at the VC level, and on other VCs the queueing policies are applied on the sessions. Some sessions have no policy applied at all. As a result, the router uses the hierarchical queueing framework (HQF) to direct traffic in the following ways:

- If no queueing policy is applied at the VC or session level, the router sends all traffic on the VC to the default queue, including traffic from sessions on the VC that have a policing-only policy applied or no policy applied.
- If a queueing policy is applied at the VC level, but not at the session level, the router sends traffic to the queues associated with the queueing policy on the VC.
- If queueing policies are applied to some sessions on a VC but not to other sessions, the router sends the traffic with a policing-only policy or with no policy applied to the VC's default queue. The router sends traffic with queueing policies to the queues associated with the queueing policy applied to the session.

Bandwidth Mode and ATM Port Oversubscription

An ATM port can operate in reserved bandwidth mode or shared bandwidth mode.

When a port is not oversubscribed (the sum of the bandwidths of all VCs on the port is less than the port bandwidth), the port operates in reserved bandwidth mode--a specific amount of bandwidth is reserved for each VC on the port. If a VC does not use all of its allocated bandwidth, the unused bandwidth is not shared among the VCs on the port.

When the ATM port is oversubscribed (the sum of the bandwidths of all VCs on the port is greater than the port bandwidth), the port operates in shared bandwidth mode. In this mode, any unused bandwidth is available

for reuse by the other VCs on the port, up to the VC's respective shape rate--traffic on a VC cannot exceed the shape rate of that VC.

Oversubscription at the Session Level

Oversubscription at the session level occurs after session traffic shaping and when the aggregate session traffic exceeds the subinterface shape rate. After all priority traffic is accounted for, the router distributes the remaining bandwidth on the VC to the sessions according to the value specified in the bandwidth remaining ratio command configured in the parent policy of the policy applied to the sessions. If the bandwidth remaining ratio command is not specified in the parent policy, the router uses a default ratio of 1.

How to Configure PPP Session Queueing on ATM VCs

Configuring PPP Session Queueing Using a Virtual Template

A virtual templat e is a logical interface whose configuration can specify generic configuration information for a specific purpose, user-specific configuration information, and router-dependent information. You configure a virtual template on an interface and apply QoS policy maps to the virtual template. The virtual template inherits the QoS features specified in the policy map. When the router establishes sessions on an interface, the router applies the QoS features specified in the virtual template configuration to the virtual access interfaces (VAIs) created for the sessions, including the QoS features specified in the policy map attached to the virtual template.

A broadband aggregation group (bba-group) configured on an ATM interface points to the virtual template the router uses to apply QoS policies to sessions. When a session arrives on an ATM interface, the router creates a virtual access interface (VAI) for the session and applies the policies associated with the virtual template to the sessions.

To configure PPPoEoA session queueing using a virtual template, perform the following configuration tasks:

Configuring an Hierarchical QoS Policy

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map** *policy-map-name*
4. **class** *class-map-name*
5. priority level level
6. **police** *bps* [*burst-normal burst-max*] [**conform-action** *action]* [**exceed-action** *action]* **violate-action** *action*
7. set cos value
8. bandwidth remaining ratio
9. exit
10. **policy-map** *policy-map-name*
11. **class** *class-default*
12. bandwidth remaining ratio

13. **shape** [**average**] *mean-rate*[*burst-size*] [*excess-burst-size*]
14. **service-policy** *policy-map-name*

DETAILED STEPS

	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 policy-map-name`	Creates or modifies the child policy. Enters policy-map configuration mode. policy-map-name is the name of the child policy map.
Step 4	**class** *class-map-name* **Example:** `Router(config-pmap)# class class-map-name`	Assigns the traffic class you specify to the policy map. Enters policy-map class configuration mode. class-map-name is the name of a previously configured class map and is the traffic class for which you want to define QoS actions. Repeat Steps 2 through 6 for each traffic class you want to include in the child policy map.
Step 5	priority level level **Example:** `Router(config-pmap-c)# priority level level`	(Optional) Defines multiple levels of a strict priority service model. When you enable a traffic class with a specific level of priority service, the implication is a single priority queue associated with all traffic enabled with the specified level of priority service. level is a number that indicates a specific priority level. Valid values are from 1 (high priority) to 4 (low priority). Default: 1
Step 6	**police** *bps* [*burst-normal burst-max*] [**conform-action** *action]* [**exceed-action** *action]* **violate-action** *action* **Example:** `Router(config-pmap-c)# police bps [burst-normal] [burst-max] [conform-action action] [exceed-action action] [violate-action action]`	(Optional) Configures traffic policing. bps is the average rate in bits per second. Valid values are 8000 to 200000000. (Optional) burst-normal is the normal burst size in bytes. Valid values are 1000 to 51200000. The default normal burst size is 1500 bytes. (Optional) burst-max is the excess burst size in bytes. Valid values are 1000 to 51200000.

	Command or Action	Purpose
		(Optional) conform-action action indicates the action to take on packets that conform to the rate limit. (Optional) exceed-action action indicates the action to take on packets that exceed the rate limit. (Optional) violate-action action indicates the action to take on packets that violate the normal and maximum burst sizes.
Step 7	set cos value **Example:** `Router(config-pmap-c)# set cos value`	(Optional) Sets the Layer 2 class of service (CoS) value of an outgoing packet. value is a specific IEEE 802.1Q CoS value from 0 to 7.
Step 8	bandwidth remaining ratio **Example:** `Router(config-pmap-c)# bandwidth remaining ratio`	(Optional) Specifies a bandwidth-remaining ratio for class-level or subinterface-level queues to be used during congestion to determine the amount of excess bandwidth (unused by priority traffic) to allocate to non-priority queues. ratio specifies the relative weight of this subinterface or queue with respect to other subinterfaces or queues. Valid values are from 1 to 1000.
Step 9	exit **Example:** `Router(config-pmap-c)# exit`	Exits policy-map class configuration mode.
Step 10	**policy-map** *policy-map-name* **Example:** `Router(config-pmap)# policy-map policy-map-name`	Creates or modifies the parent policy. policy-map-name is the name of the parent policy map.
Step 11	**class** *class-default* **Example:** `Router(config-pmap)# class class-default`	Configures or modifies the parent class-default class. You can configure only the class-default class in a parent policy. Do not configure any other traffic class.
Step 12	bandwidth remaining ratio **Example:** `Router(config-pmap-c)# bandwidth remaining ratio`	(Optional) Specifies a bandwidth-remaining ratio for class-level or subinterface-level queues to be used during congestion to determine the amount of excess bandwidth (unused by priority traffic) to allocate to non-priority queues. ratio specifies the relative weight of this subinterface or queue with respect to other subinterfaces or queues. Valid values are from 1 to 1000.

	Command or Action	Purpose
Step 13	**shape** [**average**] *mean-rate*[*burst-size*] [*excess-burst-size*] **Example:** **Router(config-pmap-c)# shape** [**average**] *mean-rate* [*burst-size*] [*excess-burst-size*]	Shapes traffic to the indicated bit rate and enables ATM overhead accounting. (Optional) average is the committed burst (Bc) that specifies the maximum number of bits sent out in each interval. This option is only supported on the PRE3. mean-rate is also called committed information rate (CIR). Indicates the bit rate used to shape the traffic, in bits per second. When this command is used with backward explicit congestion notification (BECN) approximation, the bit rate is the upper bound of the range of bit rates that are permitted. (Optional) burst-size is the number of bits in a measurement interval (Bc). (Optional) excess-burst-size is the acceptable number of bits permitted to go over the Be.
Step 14	**service-policy** *policy-map-name* **Example:** Router(config-pmap-c)# **service-policy** *policy-map-name*	Applies the child policy to the parent class-default class. policy-map-name is the name of the child policy map configured in step 1.

Example

The following example shows how to configure a hierarchical QoS policy. In the example, the child-policy configures QoS features for two traffic classes: Premium and Silver. Premium traffic has priority and is policed at 40 percent. The router sets the IP precedence of Premium traffic to precedence level 3. Silver traffic is policed at 80000 bps and IP precedence level 3 is set. The child-policy is applied to the Parent policy class-default class, which shapes traffic to 200,000 Kbps.

```
Router(config)# policy-map child-policy
Router(config-pmap)# class Premium
Router(config-pmap-c)# priority
Router(config-pmap-c)# police percent 40
Router(config-pmap-c)# set ip precedence 3
Router(config-pmap-c)# class Silver
Router(config-pmap-c)# police 80000 10000 conform-action transmit exceed-action drop
Router(config-pmap-c)# set ip precedence 5
Router(config-pmap-c)# exit
Router(config-pmap)# policy-map Parent
Router(config-pmap)# class class-default
Router(config-pmap-c)# shape 200000
Router(config-pmap-c)# service-policy output child-policy
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)#
```

Associating the Hierarchical Policy Map with a Virtual Template

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface virtual-template template-** *number*
4. **service-policy {input | output} policy-map-name**
5. exit

DETAILED STEPS

	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	**interface virtual-template template-** *number* **Example:** `Router(config)# interface virtual-template template-number`	Creates a virtual template and enters interface configuration mode. template-number is the number you assign to the virtual template interface to identify it. Valid values are from 1 to 200. You can configure up to 200 virtual template interfaces on the router.
Step 4	**service-policy {input | output} policy-map-name** **Example:** `Router(config-if)# service-policy {input | output} policy-map-name`	Attaches the policy map you specify to the virtual template interface in the inbound or outbound direction that you specify. input specifies to apply the policy map to inbound traffic. output specifies to apply the policy map to outbound traffic. policy-map-name is the name of a previously configured policy map.
Step 5	exit **Example:** `Router(config-if)# exit`	Exits interface configuration mode.

Example

The following example shows how to associate a policy map with a virtual template. In this example, the policy map named Parent is associated with the virtual template named VirtualTemplate1.

```
Router(config)# interface virtual-template1
Router(config-if)# service-policy output Parent
Router(config-if)# exit
Router(config)#
```

Applying the Virtual Template to an ATM Subinterface

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **bba-group pppoe group-name**
4. **virtual-template template-number**
5. exit
6. interface atm number.subinterface [point-to-point]
7. pvc [name] vpi/vci
8. protocol pppoe group group-name
9. exit
10. exit

DETAILED STEPS

	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	**bba-group pppoe group-name** **Example:** `Router(config)# bba-group pppoe group-name`	Creates a PPP over Ethernet (PPPoE) profile. Enters BBA group configuration mode. group-name is the name of the PPPoE profile.
Step 4	**virtual-template template-number** **Example:**	Associates a BBA group to the virtual template to be used for cloning virtual access interfaces.

	Command or Action	Purpose
	`Router(config-bba-grp)# virtual-template template-number`	template-number is the identifying number of the virtual template.
Step 5	exit **Example:** `Router(config-bba-grp)# exit`	Exits BBA group configuration mode.
Step 6	interface atm number.subinterface [point-to-point] **Example:** `Router(config)# interface atm number.subinterface [point-to-point]`	Creates or modifies a subinterface. Enters subinterface configuration mode. atm is the interface type. number is the slot, module, and port number of the interface (for example 1/0/0). .subinterface is the number of the subinterface (for example, 1/0/0.1). (Optional) point-to-point indicates that the subinterface connects directly with another subinterface.
Step 7	pvc [name] vpi/vci **Example:** `Router(config-subif) pvc [name] vpi/vci`	Creates or modifies an ATM permanent virtual circuit (PVC). Enters ATM virtual circuit configuration mode. (Optional) name identifies the PVC and can contain up to 15 characters. vpi/ specifies the ATM network virtual path identifier (VPI) for this PVC. You must specify the slash. Valid values are from 0 to 255. The router treats a value that is outside the range of valid values as the connection ID. The default value is 0. **Note** The arguments vpi and vci cannot both be set to 0; if one is 0, the other cannot be 0. vci specifies the ATM network virtual channel identifier (VCI) for this PVC. Valid values are from 0 to 1 less than the maximum value set for this interface by the atm vc-per-vp command. A value that is out of range causes an " unrecognized command" error message. The VCI value has local significance only and, therefore, is unique only on a single link, not throughout the ATM network. Typically, lower values from 0 to 31 are reserved for specific traffic (for example, F4 OAM, SVC signaling, ILMI, and so on) and should not be used.
Step 8	protocol pppoe group group-name **Example:**	Enables PPP over Ethernet (PPPoE) sessions to be established on permanent virtual circuits (PVCs). group specifies a PPPoE profile (bba-group) to be used by PPPoE sessions on the interface.

	Command or Action	Purpose
	`Router(config-atm-vc)# protocol pppoe group group-name`	group-name is the name of the PPPoE profile (bba-group) to be used by PPPoE sessions on the interface. The group group-name points to the bba-group to be used for applying a virtual template interface with QoS policies to sessions.
Step 9	exit **Example:** `Router(config-atm-vc)# exit`	Exits ATM virtual circuit configuration mode.
Step 10	exit **Example:** `Router(config-subif)# exit`	Exits subinterface configuration mode.

Examples

The following example shows how to associate a virtual template interface with an ATM interface and apply the policies in the virtual template to the sessions on the interface. In the example, the service policy named Parent is applied to the Virtual-Template 8, which is associated with the bba-group named pppoeoa-group. The bba-group is applied to PVC 101/210 on ATM subinterface 4/0/1.10.

```
bba-group pppoe pppoeoa-group
Virtual-Template 8
interface ATM4/0/1.10 point-to-point
pvc 101/210
vbr-nrt 4000 2000 50
no dbs enable
encapsulation aal5snap
protocol pppoe group pppoeoa-group
!
interface Virtual-Template8
ip unnumbered Loopback5555
no logging event link-status
peer default ip address pool pool-1
ppp authentication chap
service-policy output Parent
```

Configuring PPP Session Queueing Using Radius

To configure PPPoEoA session queueing using RADIUS, perform the following configuration tasks:

Configuring the Policy Map

The router allows you to use RADIUS to apply QoS policy maps to PPPoEoA sessions.

Adding the Cisco QoS AV Pairs to the RADIUS Profile

Cisco attribute-value (AV) pairs are vendor-specific attributes (VSAs) that allow vendors such as Cisco to support their own extended attributes. RADIUS attribute 26 is a Cisco VSA used to communicate vendor-specific information between the router and the RADIUS server.

The RADIUS user profile contains an entry for each user that the RADIUS server authenticates. Each entry establishes an attribute the user can access. When configuring PPPoEoA session queueing using RADIUS, enter the following Cisco AV-pair in the appropriate user profile:

```
Cisco-AVPair = "ip:sub-qos-policy-out=<name of egress policy>"
```

The Cisco AV-pair identifies the policy map the router is to use when applying QoS features to a PPPoEoA session. After receiving a service-logon request from the policy server, RADIUS sends a change of authorization (CoA) request to the router to activate the service for the user, who is already logged in. If the authorization succeeds, the router downloads the name of the policy map from RADIUS using the Cisco AV-pair and applies the QoS policy to the session.

Note Although the router also supports the RADIUS vendor specific attribute (VSA) 38, Cisco-Policy-Down and Cisco-Policy-Up, we recommend that you use the above attribute for QoS policy definitions.

Verifying PPP Session Queueing on ATM VCs

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **show policy-map [interface interface]**
4. show policy-map session [uid uid-number] [input | output [class class-name]]
5. **show running-config**

DETAILED STEPS

	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	**show policy-map [interface interface]** **Example:**	Displays information about the policy map attached to the interface you specify. If you do not specify an interface, it

	Command or Action	Purpose
	`Router# show policy-map [interface interface]`	displays information about all of the policy maps configured on the router. interface interface is the interface type and number (for example, atm 4/0/0).
Step 4	show policy-map session [uid uid-number] [input | output [class class-name]] **Example:** `Router# show policy-map session [uid uid-number] [input | output [class class-name]]`	Displays the QoS policy map in effect for subscriber sessions. (Optional) uid defines a unique session ID. (Optional) uid-number is a unique session ID. Valid values are from 1 to 65535. (Optional) input displays the upstream traffic of the unique session. (Optional) output displays the downstream traffic of the unique session. (Optional) class identifies the class that is part of the QoS policy-map definition. (Optional) class-name provides a class name that is part of the QoS policy-map definition.
Step 5	**show running-config** **Example:** `Router# show running-config`	Displays the running configuration on the router. The output shows the AAA setup and the configuration of the policy map, ATM VCs, PPPoEoA, dynamic bandwidth selection, virtual template, and RADIUS server.

Configuration Examples for PPP Session Queueing on ATM VCs

Example Configuring PPP Session Queueing on ATM VCs

The following example shows how to configure PPPoEoA session queueing. In the example, a hierarchical QoS policy named pm_hier2_0_2 is associated with Virtual-Template555, which is applied to the broadband aggregation group named pppoeoa-group.

```
bba-group pppoe pppoeoa-group
Virtual-Template 555
!
policy-map pm_hier2_child_0_2
class cm_0
priority level 1
police percent 5 2 ms 0 ms conform-action transmit exceed-action drop violate-action drop
queue-limit 77 packets
class cm_1
shape average percent 80
bandwidth remaining ratio 80
class class-default
shape average percent 50
bandwidth remaining ratio 20
```

```
policy-map pm_hier2_0_2
class class-default
shape average percent 100
bandwidth remaining ratio 100
service-policy pm_hier_child_0_2
interface ATM2/0/7.5555 point-to-point
pvc 1/5555
vbr-nrt 4000 2000 50
no dbs enable
encapsulation aal5snap
protocol pppoe group pppoeoa-group
!
!
interface Virtual-Template555
ip unnumbered Loopback5555
no logging event link-status
peer default ip address pool pool-1
ppp authentication chap
service-policy output pm_hier2_0_2
```

Example Configuring and Applying an Hierarchical Policy Map

The example belo shows how to configure a hierarchical policy and apply it to a virtual template. The example contains a child policy map named child1 with QoS features defined for the gold and bronze traffic classes. The child1 policy is applied to the parent policy map, which is shaped to 512000 bps. The hierarchical policy is applied to the virtual template named virtual-template 1.

```
Router(config)# policy-map child1
Router(config-pmap)# class gold
Router(config-pmap-c)# priority
Router(config-pmap-c)# police percent 40
Router(config-pmap-c)# class bronze
Router(config-pmap-c)# police 8000
Router(config-pmap-c)# exit
Router(config-pmap)# policy-map parent
Router(config-pmap)# class class-default
Router(config-pmap-c)# shape 512000
Router(config-pmap-c)# service-policy child1
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface virtual-template 1
Router(config-if)# service-policy output parent
```

Example Setting Up RADIUS for PPP Session Queueing on ATM VCs

This section shows how to define the Cisco AV pairs used to download the policy map name to the router. The first three lines of a subscriber's sample user profile contain the user password, service type, and protocol type. This information is entered into the subscriber's user profile when the user profile is first created. The last line is an example of the Cisco QoS AV-pair added to the user profile. The policy map name downloaded to the router is p23.

```
userid Password = "cisco"
Service-Type = Framed,
Framed-Protocol = PPP,
cisco-avpair = "sub-qos-policy-out=p23"
```

Example Verifying PPP Session Queueing on ATM VCs

Displaying PPP Session Information--show pxf cpu queue session Command

Use the `show pppoe session` command to display the sessions established on the router. In the example below, one session is active with a session ID (SID) of 6.

```
Router# show pppoe session
1 session in LOCALLY_TERMINATED (PTA) State
1 session total
Uniq ID PPPoE RemMAC Port VT VA State
 SID LocMAC VA-st Type
 14 6 0009.b68d.bb37 ATM2/0/7.5555 555 Vi3.1 PTA
   0009.b68d.bc37 VC: 1/5555    UP
```

Displaying PPP Session Information--show policy-map session Command

Use the `show policy-map session` command to display QoS policy map statistics for traffic in the downstream direction. The example below also shows the policy map configurations.

```
Router# show pppoe session
1 session in LOCALLY_TERMINATED (PTA) State
1 session total
Uniq ID PPPoE RemMAC Port VT VA State
 SID LocMAC VA-st Type
 14 6 0009.b68d.bb37 ATM2/0/7.5555 555  Vi3.1  PTA
 0009.b68d.bc37 VC: 1/5555 UP
Router#
Router#
Router# show policy-map session uid 14
SSS session identifier 14 -
 Service-policy output: pm_hier2_0_2
Class-map: class-default (match-any)
0 packets, 0 bytes
30 second offered rate 0 bps, drop rate 0 bps
Match: any
0 packets, 0 bytes
30 second rate 0 bps
Queueing
queue limit 50 packets
(queue depth/total drops/no-buffer drops) 0/0/0
(pkts output/bytes output) 0/0
shape (average) cir 2000000, bc 8000, be 8000
target shape rate 2000000
bandwidth remaining ratio 100
 Service-policy : pm_hier2_child_0_2
queue stats for all priority classes:
Queueing
priority level 1
queue limit 77 packets
(queue depth/total drops/no-buffer drops) 0/0/0
(pkts output/bytes output) 0/0
Class-map: cm_0 (match-any)
0 packets, 0 bytes
30 second offered rate 0 bps, drop rate 0 bps
Match: ip precedence 0
0 packets, 0 bytes
30 second rate 0 bps
Priority: 0% (0 kbps), burst bytes 4470, b/w exceed drops: 0
Priority Level: 1
```

```
Police:
104000 bps, 1536 limit, 0 extended limit
conformed 0 packets, 0 bytes; action: transmit
exceeded 0 packets, 0 bytes; action: drop
violated 0 packets, 0 bytes; action: drop
Class-map: cm_1 (match-any)
0 packets, 0 bytes
30 second offered rate 0 bps, drop rate 0 bps
Match: ip precedence 1
0 packets, 0 bytes
30 second rate 0 bps
Queueing
queue limit 237 packets
(queue depth/total drops/no-buffer drops) 0/0/0
(pkts output/bytes output) 0/0
shape (average) cir 1600000, bc 6400, be 6400
target shape rate 1600000
bandwidth remaining ratio 80
Class-map: class-default (match-any)
0 packets, 0 bytes
30 second offered rate 0 bps, drop rate 0 bps
Match: any
0 packets, 0 bytes
30 second rate 0 bps
Queueing
queue limit 77 packets
(queue depth/total drops/no-buffer drops) 0/0/0
(pkts output/bytes output) 0/0
shape (average) cir 1000000, bc 4000, be 4000
target shape rate 1000000
bandwidth remaining ratio 20
Router# show policy-map pm_hier2_0_2
Policy Map pm_hier2_0_2
Class class-default
Average Rate Traffic Shaping
cir 100%
bandwidth remaining ratio 100
service-policy pm_hier2_child_0_2
Router# show policy-map pm_hier2_child_0_2
Policy Map pm_hier2_child_0_2
Class cm_0
priority level 1
police percent 5 2 ms 0 ms conform-action transmit exceed-action drop violate-action drop
queue-limit 77 packets
Class cm_1
Average Rate Traffic Shaping
cir 80%
bandwidth remaining ratio 80
Class class-default
Average Rate Traffic Shaping
cir 50%
bandwidth remaining ratio 20
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases

Related Topic	Document Title
QoS commands	*Cisco IOS QoS Command Reference*

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

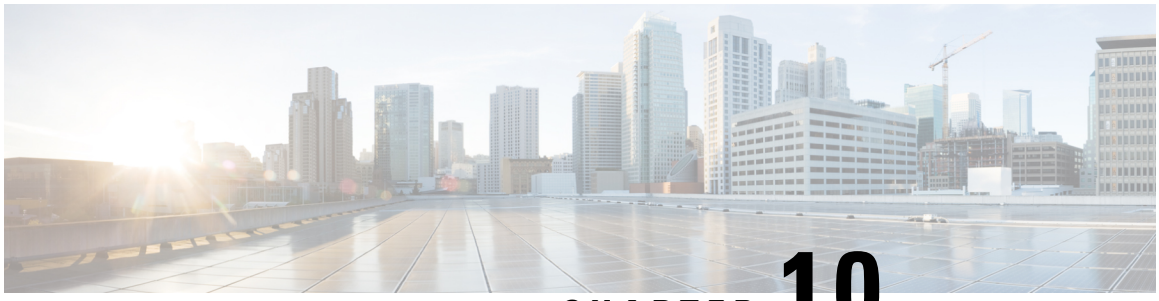
Feature Information for PPP Session Queueing on ATM VCs

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

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

Table 11: Feature Information for PPP Session Queueing on ATM VCs

Feature Name	Releases	Feature Information
PPP Session Queueing on ATM VCs	Cisco IOS XE Release 2.5	PPP Session Queueing on ATM Virtual Circuits (VCs) enables you to shape and queue PPP over Ethernet over ATM (PPPoEoA) sessions to a user specified rate. In Cisco IOS Release XE 2.5, this feature was introduced on the Cisco ASR 1000 series routers.



CHAPTER 10

VP/VC Shaping for PPPoEoA/PPPoA

The current Cisco ASR 1000 Series Aggregation Services Routers platform software supports virtual circuit (VC) shaping but not ATM virtual path (VP) shaping for VCs with broadband sessions. This feature adds support for ATM VP shaping for VCs with underlying broadband sessions. Per VC and per VP traffic shaping controls or modifies the flow of traffic on an interface. Traffic shaping limits throughput by buffering excess traffic instead of dropping packets. It ensures that traffic from one VC does not adversely impact another VC, thus preventing loss of data. Providing traffic shaping on a per VC and per VP basis allows flexibility and control over every VC and VP configured.

The VP and VC Shaping for PPPoEoA and PPPoA feature is supported for the following ATM traffic service categories:

- Variable bit rate Non-Real-Time (VBR-nRT)
- Unspecified bit rate (UBR)

Finding Feature Information

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

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

Prerequisites for VP/VC Shaping for PPPoEoA/PPPoA

- Dynamic changes to VP shaper rate should be enabled.

- The ATM VC create-on-demand functionality (with the VP shaper configured) should be enabled.
- PPP over Ethernet over ATM (PPPoEoA) sessions must be enabled.

Restrictions for VP/VC Shaping for PPPoEoA/PPPoA

- All the VCs parented by a given VP with shaping applied must be of the same type. For example, if a VP shaper is applied to virtual path identifier (VPI) 10, all the virtual circuit identifiers (VCIs) with a VP of 10 must be vbr-nrt or all must be ubr+.
- The **atm pvp rate** command cannot be added or removed if any of the VCs on that ATM interface that are in VP are in the active state. This is not supported in a nonbroadband configuration.
- Configuration of Modular QoS CLI (MQC) policy maps on VPs is not supported. Only configuration of the VP rate using the **atm pvp** command is supported.
- Quality of Service (QoS) on the VP and VC session is supported.
- The sum of the VC shaper rates can oversubscribe the VP shaper rate configured.
- The sum of all the VP shaper rates can oversubscribe the physical rate of the ATM interface.
- VP shapers are supported for any combination of VCs with or without broadband sessions. They may or may not have queuing QoS policies attached.
- On a given ATM interface, there may be mixed VPs with and without shapers.
- When there are multiple VCs in a VP, class-of-service change is not allowed.
- When there is only one VC in a VP, class-of-service change is allowed.
- IP sessions and the existing Intelligent Services Gateway (ISG) on ATM functionality are supported.

Configuring VP/VC Shaping for PPPoEoA/PPPoA

Before you begin

Before you configure VP/VC shaping for PPoEoA/PPPoA, ensure that you configure the ATM interface and define the attributes for each session. A broadband aggregation group (bba-group) configured on an ATM interface points to the virtual template the router will use to apply QoS policies to the sessions.

To configure VP/VC shaping for PPPoEoA/PPPoA on an ATM interface, perform the following configuration task.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface atm** *slot/module/port*
4. **mac-address** *mac-address*
5. **no ip address**

6. **atm clock internal**
7. **atm oam flush**
8. **no atm ilmi-keepalive**
9. **exit**
10. **bba-group pppoe** {*group-name* | **global**}
11. **virtual-template** *template-number*
12. **sessions per-vc limit** *per-vc-limit* [**threshold** *threshold-value*]
13. **sessions per-mac limit** *per-mac-limit*
14. **sessions per-vlan limit** *per-vlan-limit*
15. **sessions per-vc throttle** *per-vc-throttle*
16. **exit**
17. **interface atm** *slot/subslot/port* [*subinterface*][**point-to-point** | **multipoint**]
18. **atm pvp** *vpi [peak-rate]*
19. **pvc** *vpi/vci*
20. **vbr-nrt** *output-pcr output-scr[output-maxburstsize]*
21. **dbs enable** [**aggregated** | **maximum**]
22. **encapsulation aal5snap**
23. **protocol pppoe group** {*group-name* | **global**}
24. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables the privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters the global configuration mode.
Step 3	**interface atm** *slot/module/port* **Example:** `Router(config)# interface atm slot/module/port`	Creates or modifies an ATM interface. Enters the interface configuration mode. Here: *slot/module/port* is the interface number.
Step 4	**mac-address** *mac-address* **Example:** `Router(config-if)# mac-address mac-address`	Specifies the mac address for an interface.
Step 5	**no ip address** **Example:** `Router(config-if)# no ip address`	Disables IP processing on the interface by removing its IP address.

	Command or Action	Purpose
Step 6	**atm clock internal** **Example:** `Router(config-if)#atm clock internal`	Synchronizes the timer between two back-to-back ATM interfaces.
Step 7	**atm oam flush** **Example:** `Router(config-if)# atm oam flush`	Drops all the current and future Operation, Administration, and Maintenance (OAM) cells received on the ATM interface.
Step 8	**no atm ilmi-keepalive** **Example:** `Router(config-if)# no atm ilmi-keepalive`	Disables the Interim Local Management Interface (ILMI) keepalives.
Step 9	**exit** **Example:** `Router(config-if)# exit`	Exits the interface configuration mode.
Step 10	**bba-group pppoe** {*group-name* | **global**} **Example:** `Router(config)# bba-group pppoe group-name`	Defines a PPPoE profile, and enters the BBA group configuration mode. The **global** keyword creates a profile that serves as the default profile for any PPPoE port that is not assigned a specific profile.
Step 11	**virtual-template** *template-number* **Example:** `Router(config-bba-group)# virtual-template template-number`	Specifies which virtual template will be used to clone virtual access interfaces.
Step 12	**sessions per-vc limit** *per-vc-limit* [**threshold** *threshold-value*] **Example:** `Router(config-bba-group)# sessions per-vc limit per-vc-limit`	Specifies the maximum number of PPPoE sessions that can be established over an ATM permanent virtual circuit (PVC)
Step 13	**sessions per-mac limit** *per-mac-limit* **Example:** `Router(config-bba-group)# sessions per-mac limit per-mac limit`	Sets the maximum number of PPPoE sessions permitted per MAC address in a PPPoE profile.
Step 14	**sessions per-vlan limit** *per-vlan-limit* **Example:**	Specifies the maximum number of PPPoE sessions permitted per VLAN in a PPPoE profile.

	Command or Action	Purpose
	`Router(config-bba-group)# sessions per-vlan limit per-vlan-limit`	
Step 15	**sessions per-vc throttle** *per-vc-throttle* **Example:** `Router(config-bba-group)# sessions per-vc throttle per-vc-throttle`	Configures PPPoE connection throttling, which limits the number of PPPoE session requests that can be made from a VC.
Step 16	**exit** **Example:** `Router(config-bba-group)# exit`	Exits the BBA group configuration mode and returns to the global configuration mode.
Step 17	**interface atm** *slot/subslot/port* [*subinterface*][**point-to-point** | **multipoint**] **Example:** `Router(config)# interface atm slot/subslot/port multipoint`	Configures the ATM interface and enters the subinterface configuration mode.
Step 18	**atm pvp** *vpi [peak-rate]* **Example:** `Router(config-subif)# atm pvp vpi[peak-rate]`	Creates a permanent virtual path (PVP) used to multiplex (or bundle) one or more VCs.
Step 19	**pvc** *vpi/vci* **Example:** `Router(config-subif)# atm pvp vpi[peak-rate]`	Creates or assigns a name to an ATM PVC and enters ATM virtual circuit configuration mode.
Step 20	**vbr-nrt** *output-pcr output-scr[output-maxburstsize]* **Example:** `Router(config-if-atm-vc)# vbr-nrt output-pcr output-scr [output-maxburstsize]`	Configures the VBR-nRT QoS and specifies output peak cell rate (PCR), output sustainable cell rate (SCR), and output maximum burst cell size for an ATM PVC, PVC range, switched virtual circuit (SVC), VC class, or VC bundle member.
Step 21	**dbs enable** [**aggregated** | **maximum**] **Example:** `Router(config-if-atm-vc)# dbs enable`	Applies the Dynamic Subscriber Bandwidth Selection QoS parameters.
Step 22	**encapsulation aal5snap** **Example:** `Router(config-if-atm-vc)# encapsulation aal5snap`	Configures the ATM adaptation layer (AAL) and encapsulation type for an ATM VC.
Step 23	**protocol pppoe group** {*group-name* | **global**}	Enables PPPoE sessions to be established on PVCs.

	Command or Action	Purpose
	Example: `Router(config-if-atm-vc)# protocol pppoe group group-name`	**group** specifies a PPPoE profile (bba-group) to be used by the PPPoE sessions on the interface. *group-name* is the name of the PPPoE profile (bba-group) to be used by the PPPoE sessions on the interface. **group** *group-name* points to the bba-group to be used for applying a virtual template interface with QoS policies to sessions.
Step 24	**end** **Example:** `Router(config-if-atm-vc)# end`	Ends the session and returns to the privileged EXEC mode.

Example

The following example shows how to configure VP/VC shaping for PPPoEoA/PPPoA:

```
Router(config)#interface ATM1/0/0
Router(config-if)#mac-address 0000.b001.0001
Router(config-if)#no ip address
Router(config-if)#atm clock INTERNAL
Router(config-if)#atm oam flush
Router(config-if)#no atm ilmi-keepalive
Router(config-if)#exit
Router(config)#bba-group pppoe group_basic
Router(config-bba-group)#virtual-template 2
Router(config-bba-group)#sessions per-vc limit 1
Router(config-bba-group)#sessions per-mac limit 1
Router(config-bba-group)#sessions per-vlan limit 1
Router(config-bba-group)#sessions per-vc throttle 1 2 3
Router(config-bba-group)#exit
Router(config)#interface ATM1/0/0.64001 multipoint
Router(config-subif)#atm pvp 1 50000
Router(config-subif)#pvc 1/32
Router(config-if-atm-vc)#vbr-nrt 40000 40000 1
Router(config-if-atm-vc)#dbs enable
Router(config-if-atm-vc)#encapsulation aal5snap
Router(config-if-atm-vc)#protocol pppoe group group_1
Router(config-if-atm-vc)#end
```

Configuration Examples for VP/VC Shaping for PPPoEoA/PPPoA

Example: Configuring VP/VC Shaping for PPPoEoA/PPPoA

The following example shows how to configure VP/VC shaping for PPPoEoA/PPPoA:

```
interface ATM1/0/0
mac-address 0000.b001.0001
no ip address
```

```
atm clock INTERNAL
atm oam flush
no atm ilmi-keepalive
!
bba-group pppoe group_basic
virtual-template 2
sessions per-vc limit 1
sessions per-mac limit 1
sessions per-vlan limit 1
sessions per-vc throttle 1 2 3
!
interface ATM1/0/0.1 multipoint
atm pvp 1 1000
pvc 1/10000
 vbr-nrt 500 500 1
 dbs enable
 encapsulation aal5snap
 protocol pppoe group group_basic
```

Example: Verifying VP/VC Shaping for PPPoEoA/PPPoA

The following example shows how to display configuration of a particular PVC.

```
Router# Show ATM pvc
Keys:  A = ATM1/0/0, B = ATM1/0/1, C = ATM1/0/2,
          VCD /                                          Peak Av/Min Burst
Interface  Name          VPI   VCI Type    Encaps     SC     Kbps   Kbps Cells St
A.64001    1             1     3 PVC     F4-OAM     UBR   50000               UP
A.64001    2             1     4 PVC     F4-OAM     UBR   50000               UP
A.64001    11            1    32 PVC     SNAP       VBR   40000  40000     1 UP
A.64001    12            1    33 PVC     SNAP       VBR   40000  40000     1 UP
A.64001    13            1    34 PVC     SNAP       VBR   40000  40000     1 UP
A.64001    14            1    35 PVC     SNAP       VBR   40000  40000     1 UP
A.64001    15            1    36 PVC     SNAP       VBR   40000  40000     1 UP
A.64001    16            1    37 PVC     SNAP       VBR   40000  40000     1 UP
A.64001    17            1    38 PVC     SNAP       VBR   40000  40000     1 UP
A.64001    18            1    39 PVC     SNAP       VBR   40000  40000     1 UP
A.64001    19            1    40 PVC     SNAP       VBR   40000  40000     1 UP
A.64001    20            1    41 PVC     SNAP       VBR   40000  40000     1 UP
A.64001    3             2     3 PVC     F4-OAM     UBR   50000               UP
A.64001    4             2     4 PVC     F4-OAM     UBR   50000               UP
A.64001    21            2    32 PVC     SNAP       VBR   40000  40000     1 UP
A.64001    22            2    33 PVC     SNAP       VBR   40000  40000     1 UP
A.64001    23            2    34 PVC     SNAP       VBR   40000  40000     1 UP
A.64001    24            2    35 PVC     SNAP       VBR   40000  40000     1 UP
```

The following example shows how to display configuration of the traffic parameters for a PVC.

```
Router# Show ATM vc
Keys:  A = ATM1/0/0, B = ATM1/0/1, C = ATM1/0/2,
Codes: DN - DOWN, IN - INACTIVE

          VCD /                                          Peak Av/Min Burst
Interface  Name          VPI   VCI Type    Encaps     SC     Kbps   Kbps Cells St
A.64001    1             1     3 PVC     F4-OAM     UBR   50000               UP
A.64001    2             1     4 PVC     F4-OAM     UBR   50000               UP
A.64001    11            1    32 PVC     SNAP       VBR   40000  40000     1 UP
A.64001    12            1    33 PVC     SNAP       VBR   40000  40000     1 UP
A.64001    13            1    34 PVC     SNAP       VBR   40000  40000     1 UP
A.64001    14            1    35 PVC     SNAP       VBR   40000  40000     1 UP
A.64001    15            1    36 PVC     SNAP       VBR   40000  40000     1 UP
```

```
A.64001    16             1    37 PVC     SNAP       VBR   40000  40000     1 UP
A.64001    17             1    38 PVC     SNAP       VBR   40000  40000     1 UP
A.64001    18             1    39 PVC     SNAP       VBR   40000  40000     1 UP
A.64001    19             1    40 PVC     SNAP       VBR   40000  40000     1 UP
A.64001    20             1    41 PVC     SNAP       VBR   40000  40000     1 UP
A.64001    3              2     3 PVC     F4-OAM     UBR   50000             UP
A.64001    4              2     4 PVC     F4-OAM     UBR   50000             UP
A.64001    21             2    32 PVC     SNAP       VBR   40000  40000     1 UP
A.64001    22             2    33 PVC     SNAP       VBR   40000  40000     1 UP
A.64001    23             2    34 PVC     SNAP       VBR   40000  40000     1 UP
A.64001    24             2    35 PVC     SNAP       VBR   40000  40000     1 UP
A.64001    25             2    36 PVC     SNAP       VBR   40000  40000     1 UP
A.64001    26             2    37 PVC     SNAP       VBR   40000  40000     1 UP
A.64001    27             2    38 PVC     SNAP       VBR   40000  40000     1 UP
A.64001    28             2    39 PVC     SNAP       VBR   40000  40000     1 UP
```

The following example shows how to display configuration for VP mode cell relay.

```
Router# Show ATM vp
Keys:  A = ATM1/0/0, B = ATM1/0/1, C = ATM1/0/2,
                            Data  CES     Peak      CES Avg/Min Burst      MCR
Interface     VPI SC         VCs  VCs     Kbps     Kbps    Kbps Cells     Kbps    CDVT  Status
A.64001         1 VBR-NRT     10    0    50000        0     N/A   N/A     N/A     N/A  ACTIVE

A.64001         2 VBR-NRT     10    0    50000        0     N/A   N/A     N/A     N/A  ACTIVE

A.64001         3 VBR-NRT     10    0    50000        0     N/A   N/A     N/A     N/A  ACTIVE

A.64001         4 VBR-NRT     10    0    50000        0     N/A   N/A     N/A     N/A  ACTIVE

A.64001         5 VBR-NRT     10    0    50000        0     N/A   N/A     N/A     N/A  ACTIVE

B.64001         6 VBR-NRT     10    0    40000        0     N/A   N/A     N/A     N/A  ACTIVE

B.64001         7 VBR-NRT     10    0    40000        0     N/A   N/A     N/A     N/A  ACTIVE

B.64001         8 VBR-NRT     10    0    40000        0     N/A   N/A     N/A     N/A  ACTIVE

B.64001         9 VBR-NRT     10    0    40000        0     N/A   N/A     N/A     N/A  ACTIVE

B.64001        10 VBR-NRT     10    0    40000        0     N/A   N/A     N/A     N/A  ACTIVE

C.64001        11 VBR-NRT     10    0    30000        0     N/A   N/A     N/A     N/A  ACTIVE

C.64001        12 VBR-NRT     10    0    30000        0     N/A   N/A     N/A     N/A  ACTIVE

C.64001        13 VBR-NRT     10    0    30000        0     N/A   N/A     N/A     N/A  ACTIVE

C.64001        14 VBR-NRT     10    0    30000        0     N/A   N/A     N/A     N/A  ACTIVE

C.64001        15 VBR-NRT     10    0    30000        0     N/A   N/A     N/A     N/A  ACTIVE
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
QoS commands	*Cisco IOS QoS Command Reference*

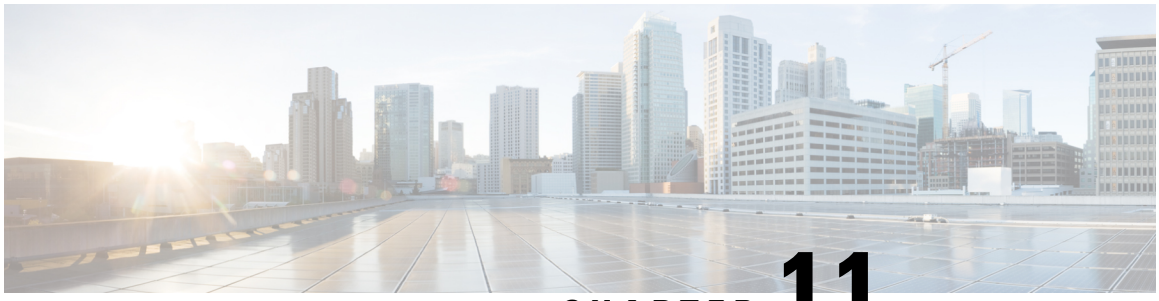
Technical Assistance

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

Feature Information for VP/VC Shaping for PPPoEoA/PPPoA

Table 12: Feature Information for VP/VC Shaping for PPPoEoA/PPPoA

Feature Name	Releases	Feature Information
VP/VC Shaping for PPPoEoA/PPPoA	Cisco IOS XE Release 3.10	VP/VC Shaping for PPPoEoA/PPPoA enables ATM VP shaping for VCs with underlying broadband sessions.



CHAPTER 11

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. Beginning in Cisco IOS XE Release 3.2S, this feature is enabled on the Cisco ASR 1000 series Aggregation Services Routers through the following support and changes:

- Reverse the order of dataplane policing in hierarchical policies so that they are evaluated from child to parent. In prior releases, the policies are evaluated from parent to child.
- Limited support for color-aware policing (RFC 2697 and RFC 2698) within Quality of Service (QoS) policies.

Finding Feature Information

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

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

Prerequisites for Hierarchical Color-Aware Policing

You must have Cisco IOS XE Release 3.2S or a later version installed and running on your Cisco ASR 1000 series 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 131 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.
- Only one filter (one match statement) per color-aware class is supported.
- Color-aware statistics are not supported, only existing policer statistics.
- Color-aware class map removal (using the **no class-map***class-map-name* command) is not allowed while the class map is being referenced in a color-aware policer. It must be removed from all color-aware policers (using either the **no conform-color***class-map-name* or **no exceed-color***class-map-name* command first).
- Hierarchical policer evaluation is permanently reversed (not configurable) to support child-to-parent ordering.

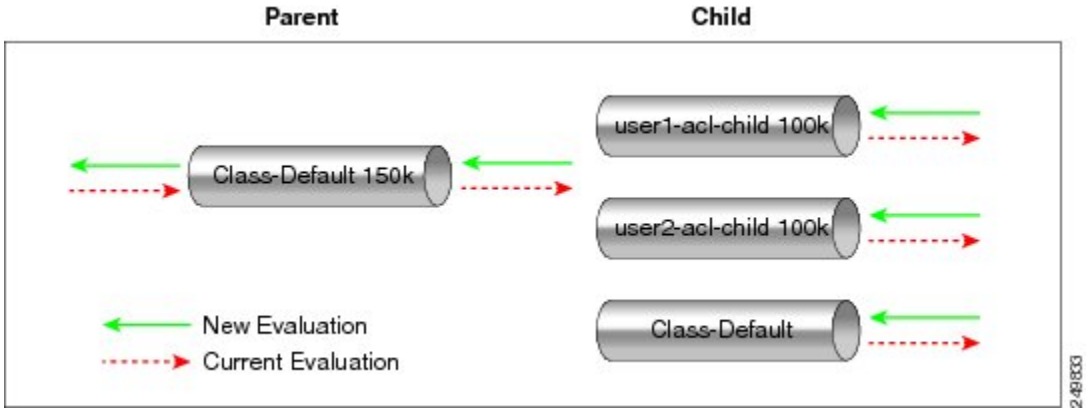
Information About Hierarchical Color-Aware Policing

Hierarchical Order Policing

Prior to Cisco IOS XE Release 3.2S, the Cisco ASR 1000 series platform supported policers in hierarchical policies with an evaluation order of parent to child. With the introduction of the Hierarchical Color-Aware Policing feature, the evaluation order is reversed so that policers are evaluated from child to parent in QoS policies. This ordering is a permanent change to the default behavior and is not configurable. The reverse order policer functionality is shared 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
```

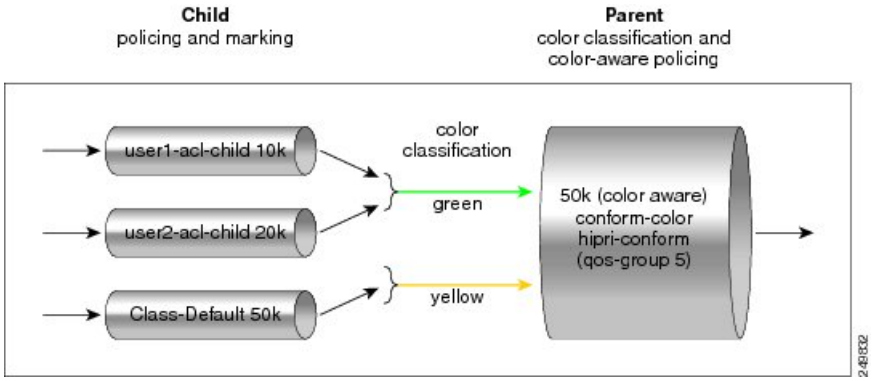


Limited Color-Aware Policing

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 1: Simple Two-Level Color-Aware Policer

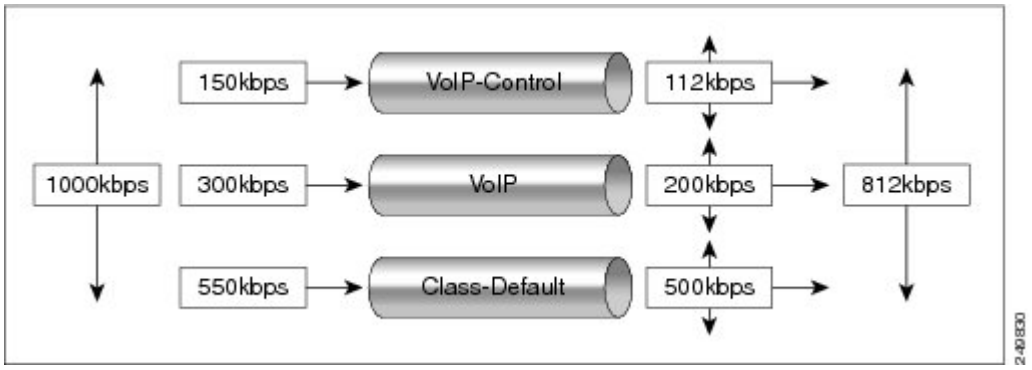


Note To avoid drops at the parent level for "conformed" child traffic, the parent policer must have a rate and burst that are equal to or greater than the sum of the child conform rates and burst sizes. There is no check for inappropriate (parent-to-child) rates and burst sizes in code. You must be aware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

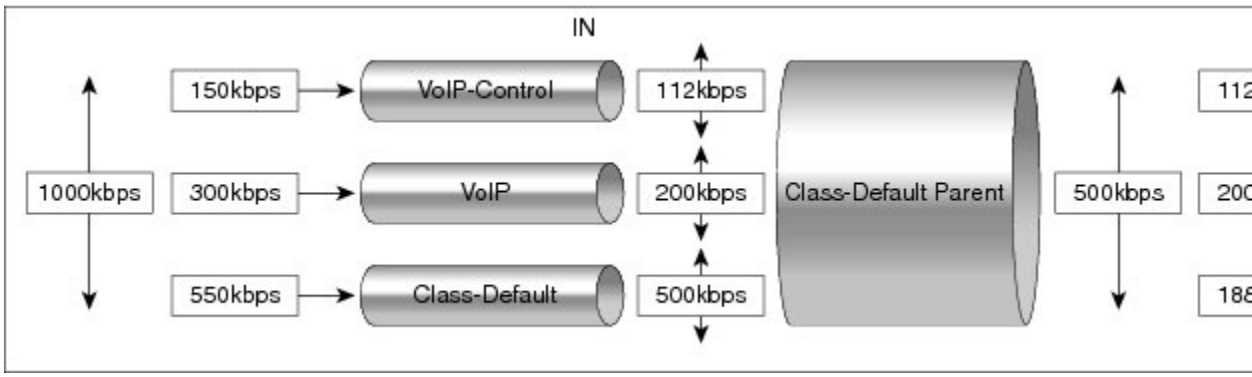
Prior to the release of the Hierarchical Color-Aware Policing feature, policing and marking were typically used as input QoS options. For example, a voice customer was limited to 112 kb/s for voice control and 200 kb/s for voice traffic. The class-default class has no policer. The only limit is the physical 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 2: 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 3: 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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router> enable`	• 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 parent-policy`	Enters policy-map configuration mode and creates a policy map.
Step 4	**class** {*class-name* | **class-default** [**fragment** *fragment-class-name*]} [**insert-before** *class-name*] [**service-fragment** *fragment-class-name*] **Example:** `Router(config-pmap)# class class-default`	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 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. • **fragment** *fragment-class-name* --(Optional) Specifies the default traffic class as a fragment, and names the fragment traffic class. • **insert-before** *class-name* --(Optional) Adds a class map between any two existing class maps. Inserting a new class map between two existing class maps provides more flexibility when modifying existing policy map configurations. Without this option, the class map is appended to the policy map. **Note** This keyword is supported only on flexible packet matching (FPM) policies. • **service-fragment** *fragment-class-name* --(Optional) Specifies that the class is classifying a collection of fragments. The fragments being classified by this class must all share the same fragment class name.

	Command or Action	Purpose

Step 5	**police** [**cir** *cir*][**bc** *conform-burst*] [**pir** *pir*][**be** *peak-burst*] [**conform-action** *action* [**exceed-action** *action* [**violate-action** *action*]]][**conform-color hipri-conform**]
	Example:
	`Router(config-pmap-c)# police 50000 bc 3000`
	`Router(config-pmap-c-police)# exceed-action transmit`
	Example:
	`Router(config-pmap-c-police)# violate-action drop`
	Example:
	`Router(config-pmap-c-police)# conform-color hipri-conform`
		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.

Step 6	**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 7	**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, showing the reverse order for policing:

```
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
exceed-action transmit
violate-action drop
conform-color hipri-conform
service-policy child-policy
```

Configuration Examples for Hierarchical Color-Aware Policing

Example Enable the Hierarchical Color-Aware Policing Feature

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

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# ip access-list extended user1-acl
Router(config-ext-nacl)# permit ip host 192.168.1.1 any
Router(config-ext-nacl)# permit ip host 192.168.1.2 any
Router(config-ext-nacl)# ip access-list extended user2-acl
Router(config-ext-nacl)# permit ip host 192.168.2.1 any
Router(config-ext-nacl)# permit ip host 192.168.2.2 any
Router(config-ext-nacl)# exit
Router(config)# class-map match-all user1-acl-child
Router(config-cmap)# match access-group name user1-acl
Router(config-cmap)# class-map match-all user2-acl-child
Router(config-cmap)# match access-group name user2-acl
Router(config-cmap)# class-map match-all hipri-conform
Router(config-cmap)# match qos-group 5
Router(config-cmap)# exit
Router(config)# policy-map child-policy
Router(config-pmap)# class user1-acl-child
Router(config-pmap-c)# police cir 10000 bc 1500
Router(config-pmap-c-police)# class user2-acl-child
Router(config-pmap-c)# police cir 20000 bc 1500
Router(config-pmap-c-police)# exit
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# policy-map parent-policy
Router(config-pmap)# class class-default
Router(config-pmap-c)# police cir 50000 bc 3000
Router(config-pmap-c-police)# exceed-action transmit
Router(config-pmap-c-police)# violate-action drop
Router(config-pmap-c-police)# conform-color hipri-conform
Router(config-pmap-c-police)# service-policy child-policy
```

Example Disallowing Multiple Entries in Class Map

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

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

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

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

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

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

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

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

Example Enabling Hierarchical Color-Aware Policing

The following example shows how to enable Hierarchical Color-Aware Policing:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# ip access-list extended user1-acl
Router(config-ext-nacl)# permit ip host 192.168.1.1 any
Router(config-ext-nacl)# permit ip host 192.168.1.2 any
Router(config-ext-nacl)# ip access-list extended user2-acl
Router(config-ext-nacl)# permit ip host 192.168.2.1 any
Router(config-ext-nacl)# permit ip host 192.168.2.2 any
Router(config-ext-nacl)# class-map match-all user1-acl-child
Router(config-cmap)# match access-group name user1-acl
Router(config-cmap)# class-map match-all user2-acl-child
Router(config-cmap)# match access-group name user2-acl
Router(config-cmap)# class-map match-all hipri-conform
Router(config-cmap)# match qos-group 5
```

```
Router(config-cmap)# policy-map child-policy
Router(config-pmap)# class user1-acl-child
Router(config-pmap-c)# police 10000 bc 1500
Router(config-pmap-c-police)# conform-action set-qos-transmit 5
Router(config-pmap-c-police)# class user2-acl-child
Router(config-pmap-c)# police 20000 bc 1500
Router(config-pmap-c-police)# conform-action set-qos-transmit 5
Router(config-pmap-c-police)# class class-default
Router(config-pmap-c)# police 50000 bc 1500
Router(config-pmap-c-police)# policy-map parent-policy
Router(config-pmap)# class class-default
Router(config-pmap-c)# police 50000 bc 3000
Router(config-pmap-c-police)# exceed-action transmit
Router(config-pmap-c-police)# violate-action drop
Router(config-pmap-c-police)# conform-color hipri-conform
Router(config-pmap-c-police)# service-policy child-policy
Router(config-pmap-c)# end
Router#
*Sep 16 12:31:11.536: %SYS-5-CONFIG_I: Configured from console by console
Router# show class-map
Class Map match-all user1-acl-child (id 4)
Match access-group name user1-acl
Class Map match-all user2-acl-child (id 5)
Match access-group name user2-acl
Class Map match-any class-default (id 0)
Match any
Class Map match-all hipri-conform (id 3)
Match qos-group 5
Router# show policy-map
Policy Map parent-policy
Class class-default
police cir 50000 bc 3000 be 3000
conform-color hipri-conform
conform-action transmit
exceed-action transmit
violate-action drop
service-policy child-policy
Policy Map police
Class prec1
priority level 1 20000 (kb/s)
Class prec2
bandwidth 20000 (kb/s)
Class class-default
bandwidth 20000 (kb/s)
Policy Map child-policy
Class user1-acl-child
police cir 10000 bc 1500
conform-action set-qos-transmit 5
exceed-action drop
Class user2-acl-child
police cir 20000 bc 1500
conform-action set-qos-transmit 5
exceed-action drop
Class class-default
police cir 50000 bc 1500
conform-action transmit
exceed-action drop
```

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	Cisco IOS Master Commands List, All Releases

Related Topic	Document Title
Quality of Service commands	*Cisco IOS Quality of Service Solutions Command Reference*
Quality of Service configuration information	*Cisco IOS QoS Configuration Guide, Cisco IOS XE Release 3S*

Standards

Standard	Title
No new or modified standards are supported by this feature.	--

MIBs

MIB	MIBs Link
• CISCO-CLASS-BASED-QOS-MIB • CISCO-CLASS-BASED-QOS-CAPABILITY-MIB	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 2697	*A Single Rate Three Color Marker*
RFC 2698	*A Two Rate Three Color Marker*

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

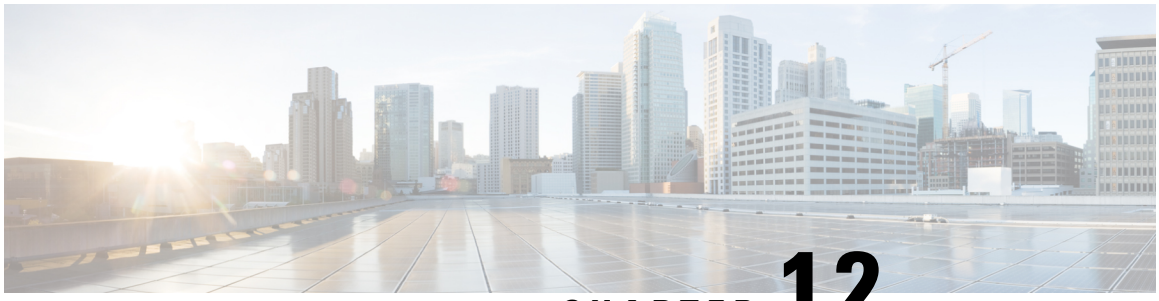
Feature Information for Hierarchical Color-Aware Policing

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

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

Table 13: Feature Information for Hierarchical Color-Aware Policing

Feature Name	Releases	Feature Information
Hierarchical Color-Aware Policing	Cisco IOS XE Release 3.2S	The Hierarchical Color-Aware Policing feature provides for 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.



CHAPTER 12

IPv6 QoS: MQC Traffic Policing

Configuration or command usage for policing are the same in IPv6 environments as for IPv4 environments.

Finding Feature Information

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

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

Information About IPv6 QoS: MQC Traffic Policing

Implementation Strategy for QoS for IPv6

IPv6 packets are forwarded by paths that are different from those for IPv4. QoS features supported for IPv6 environments include packet classification, queuing, traffic shaping, weighted random early detection (WRED), class-based packet marking, and policing of IPv6 packets. These features are available at both the process switching and Cisco Express Forwarding switching paths of IPv6.

All of the QoS features available for IPv6 environments are managed from the modular QoS command-line interface (MQC). The MQC allows you to define traffic classes, create and configure traffic policies (policy maps), and then attach those traffic policies to interfaces.

To implement QoS in networks that are running IPv6, follow the same steps that you would follow to implement QoS in networks running only IPv4. At a very high level, the basic steps for implementing QoS are as follows:

- Know which applications in your network need QoS.

- Understand the characteristics of the applications so that you can make decisions about which QoS features would be appropriate.
- Know your network topology so that you know how link layer header sizes are affected by changes and forwarding.
- Create classes based on the criteria that you establish for your network. In particular, if the same network is also carrying IPv4 traffic along with IPv6 traffic, decide if you want to treat both of them the same way or treat them separately and specify match criteria accordingly. If you want to treat them the same, use match statements such as **match precedence**, **match dscp**, **set precedence**, and **set dscp**. If you want to treat them separately, add match criteria such as **match protocol ip** and **match protocol ipv6** in a match-all class map.
- Create a policy to mark each class.
- Work from the edge toward the core in applying QoS features.
- Build the policy to treat the traffic.
- Apply the policy.

Traffic Policing in IPv6 Environments

Congestion management for IPv6 is similar to IPv4, and the commands used to configure queueing and traffic shaping features for IPv6 environments are the same commands as those used for IPv4. Traffic shaping allows you to limit the packet dequeue rate by holding additional packets in the queues and forwarding them as specified by parameters configured for traffic shaping features. Traffic shaping uses flow-based queueing by default. CBWFQ can be used to classify and prioritize the packets. Class-based policer and generic traffic shaping (GTS) or Frame Relay traffic shaping (FRTS) can be used for conditioning and policing traffic.

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, 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

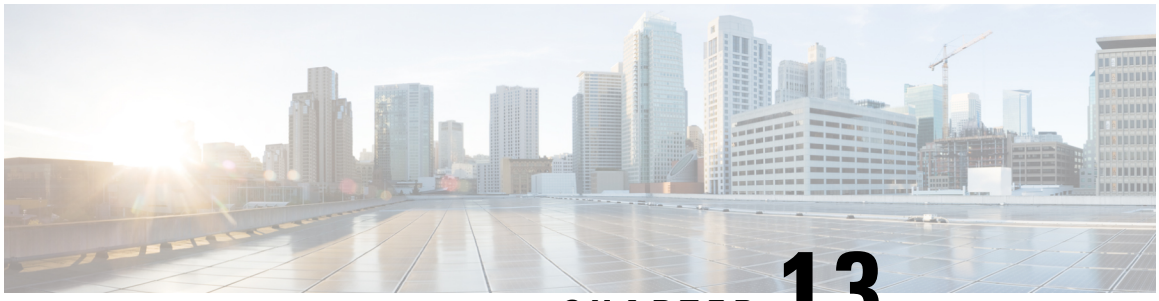
Feature Information for IPv6 QoS: MQC Traffic Policing

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

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

Table 14: Feature Information for IPv6 QoS: MQC Traffic Policing

Feature Name	Releases	Feature Information
IPv6 QoS: MQC Traffic Policing	Cisco IOS XE Release 2.1	Configuration or command usage for policing are the same in IPv6 environments as for IPv4 environments.



CHAPTER 13

Traffic Policing

This feature module describes the Traffic Policing feature. The Traffic 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.

Traffic policing allows you to control the maximum rate of traffic that is transmitted or received on an interface. The Traffic Policing feature is applied when a service-policy containing the feature is attached to an interface. A service-policy (traffic policy) is configured using the Modular Quality of Service (QoS) Command-Line Interface (CLI) (MQC).

Finding Feature Information

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

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

Restrictions for Traffic Policing

- Traffic policing can be configured on an interface or a subinterface.

- Traffic policing is not supported on the EtherChannel interfaces.

Benefits

Bandwidth Management Through Rate Limiting

Traffic policing allows you to control the maximum rate of traffic transmitted or received on an interface. Traffic policing is often configured on interfaces at the edge of a network to limit traffic into or out of the network. In most Traffic 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 traffic 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 traffic 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 Traffic Policing feature. If you want to mark traffic but do not want to use Traffic Policing, see the "Marking Network Traffic" module.

Packet Prioritization for Frame Relay Frames

The Traffic 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 Traffic 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.

How to Configure Traffic Policing

Configuring Traffic Policing

Command	Purpose
Router(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 Traffic 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.

Monitoring and Maintaining Traffic Policing

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

Configuration Examples for Traffic Policing

Example Configuring a Service Policy That Includes Traffic Policing

The following configuration shows how to define a traffic class (with the **class-map**command) and associate that traffic class with a traffic policy (with the **policy-map** command). Traffic policing is applied in the traffic policy. The **service-policy** command is then used to attach the traffic policy to the interface.

In this particular example, traffic policing is configured with the Committed Information Rate (CIR) at 8000 bits per second, the normal burst size at 2000 bytes, and the excess burst size at 4000 bytes. Packets coming into FastEthernet interface 1/1/1 are evaluated by the token bucket algorithm to analyze whether packets conform exceed, or violate the specified parameters. Packets that conform are transmitted, packets that exceed are assigned a QoS group value of 4 and are transmitted, and packets that violate are dropped.

```
Router(config)# class-map acgroup2
Router(config-cmap)# match access-group 2
Router(config-cmap)# exit
Router(config)# policy-map police
Router(config-pmap)# class acgroup2
```

```
Router(config-pmap-c)# police 8000 2000 4000 conform-action transmit exceed-action
set-qos-transmit 4 violate-action drop
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface fastethernet1/1/1
Router(config-if)# service-policy input police
Router(config-if)# end
```

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*
Conceptual information about policing and shaping	"Policing and Shaping Overview" module
MQC	"Applying QoS Features Using the MQC" module
Marking network traffic	"Marking Network Traffic" module
IPv6 Traffic Policing	“IPv6 QoS: MQC Traffic Policing” module in the *QoS: Policing and Shaping Configuration Guide*.

Standards

Standard	Title
None	--

MIBs

MIB	MIBs Link
• CISCO-CLASS-BASED-QOS-MIB • CISCO-CLASS-BASED-QOS-CAPABILITY-MIB	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
RFC 2697	*A Single Rate Three Color Marker*

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

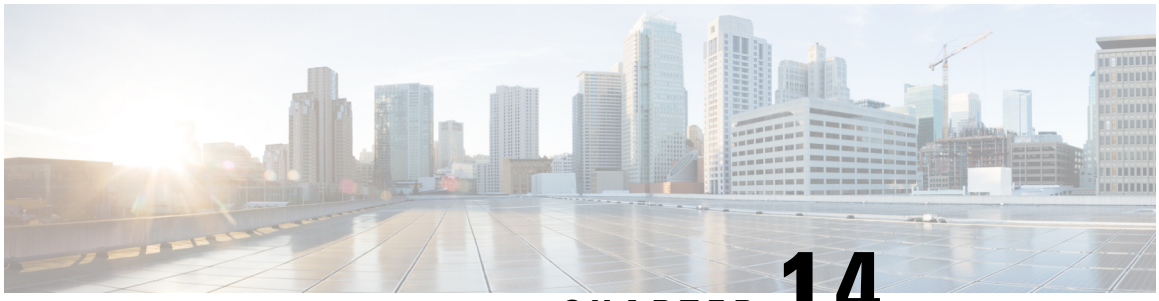
Feature Information for Traffic Policing

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

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

Table 15: Feature Information for Traffic Policing

Feature Name	Releases	Feature Information
Traffic Policing	Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers. The following commands were modified: **police**, s**how policy-map**, **show policy-map interface**.



CHAPTER 14

Policer Enhancement Multiple Actions

Feature History

Release	Modification
Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.

This document describes the Policer Enhancement Multiple Actions feature and includes the following sections:

Finding Feature Information

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

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

Feature Overview

This feature further extends the functionality of the Cisco IOS XE single-rate policer and the Two-Rate Policer feature. The Traffic Policing and Two-Rate Policer features are traffic policing mechanisms that allow you to control the maximum rate of traffic sent or received on an interface. Both of these traffic policing mechanisms mark packets as either conforming to, exceeding, or violating a specified rate. After a packet is marked, you can specify an action to be taken on the packet based on that marking.

With both the Traffic Policing feature and the Two-Rate Policer feature, you can specify only one conform action, one exceed action, and one violate action. Now with the new Policer Enhancement Multiple Actions feature, you can specify multiple conform, exceed, and violate actions for the marked packets.

You specify the multiple actions by using the *action* argument of the **police** command. The resulting actions are listed in the table below.

Table 16: police Command Action Arguments

Specified Action	Result
drop	Drops the packet.
set-clp-transmit	Sets the ATM Cell Loss Priority (CLP) bit from 0 to 1 on the ATM cell and transmits the packet.
set-cos-transmit	Sets the Class of Service (CoS) value and transmits the packet.
set-discard-class-transmit	Sets the discard-class value and transmits the packet.
set-dscp-transmit *new-dscp*	Sets the IP differentiated services code point (DSCP) value and transmits the packet with the ATM CLP bit set to 1.
set-frde-transmit	Sets the Frame Relay Discard Eligibility (DE) bit from 0 to 1 on the Frame Relay frame and transmits the packet.
set-mpls-exp-transmit	Sets the Multiprotocol Label Switching (MPLS) experimental (EXP) bits from 0 to 7 and transmits the packet.
set-mpls-exp-imposition-transmit	Sets the MPLS EXP bits from 0 to 7 at tag imposition and transmits the packet.
set-prec-transmit *new-prec*	Sets the IP Precedence level and transmits the packet.
set-qos-transmit *new-qos*	Sets the Quality of Service (QoS) group value and transmits the packet.
transmit	Transmits the packet.

Benefits

Before this feature, you could specify only *one* marking action for a packet, in addition to transmitting the packet. This feature provides enhanced flexibility by allowing you to specify *multiple* marking actions for a packet, as required. For example, if you know the packet will be transmitted through both a TCP/IP and a Frame Relay environment, you can change the DSCP value of the exceeding or violating packet, and also set the Frame Relay Discard Eligibility (DE) bit from 0 to 1 to indicate lower priority.

Restrictions

The **shape** (percent) command, when used in "child" (nested) policy maps, is not supported on the Cisco 7500, the Cisco 7200, or lower series routers. Therefore, the **shape** (percent) command cannot be configured for use in nested policy maps on these routers.

Related Features and Technologies

- Modular Quality of Service (QoS) Command-Line Interface (CLI) (MQC)
- Class-Based Weighted Fair Queueing (CBWFQ)
- Class-Based Packet Marking
- Traffic Policing
- Two-Rate Policing

Related Documents

- "Applying QoS Features Using the MQC" module
- "Configuring Weighted Fair Queueing" module
- "Marking Network Traffic" module
- "Policing and Shaping Overview" module
- "Traffic Policing" module
- "Two-Rate Policer" module
- "Policer Enhancements-Multiple Actions" module
- "Cisco Express Forwarding Overview" module
- Cisco IOS Quality of Service Solutions Command Reference
- Cisco IOS Switching Services Command Reference
- RFC 2697, *A Single Rate Three Color Marker*
- RFC 2698, *A Two Rate Three Color Marker*

Supported Standards MIBs and RFCs

Standards

None

MIBs

- CISCO-CLASS-BASED-QOS-MIB
- CISCO-CLASS-BASED-QOS-CAPABILITY-MIB

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

http://tools.cisco.com/ITDIT/MIBS/servlet/index

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

http://www.cisco.com/register

RFCs

None

Prerequisites

- On a Cisco 7500 series router, CEF or dCEF must be configured on the interface before you can use the Policer Enhancement -- Multiple Actions feature.
- To configure the Policer Enhancement -- Multiple Actions feature, a traffic class and a service policy must be created, and the service policy must be attached to a specified interface.

Configuration Tasks

Configuring Multiple Policer Actions

SUMMARY STEPS

1. Router(config)# **policy-map** *policy-map-name*
2. Router(config-pmap)# **class** *class-default*
3. Router(config-pmap-c)# **police** {**cir** *cir*}[**bc** *conform-burst*]{**pir** *pir*} [**be** *peak-burst*] [**conform-action** *action* [**exceed-action** *action* [**violate-action** *action*]]]

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **policy-map** *policy-map-name*	Creates a policy map. Enters policy-map configuration mode.
Step 2	Router(config-pmap)# **class** *class-default*	Specifies the default traffic class for a service policy. Enters policy-map class configuration mode.
Step 3	Router(config-pmap-c)# **police** {**cir** *cir*}[**bc** *conform-burst*]{**pir** *pir*} [**be** *peak-burst*] [**conform-action** *action* [**exceed-action** *action* [**violate-action** *action*]]]	Configures traffic policing and specifies multiple actions applied to packets marked as conforming to, exceeding, or violating a specific rate. Use one line per action that you

	Command or Action	Purpose
		want to specify. Enters policy-map class police configuration mode.

Verifying the Multiple Policer Actions Configuration

Command	Purpose
`Router# show policy-map interface`	Displays statistics and configurations of all input and output policies attached to an interface.

Troubleshooting Tips

- Check the interface type. Verify that your interface is not listed as a nonsupported interface.
- For input traffic policing on a Cisco 7500 series router, verify that Cisco Express Forwarding or Distributed Cisco Express Forwarding is configured on the interface on which traffic policing is configured.
- For output traffic policing on a Cisco 7500 series router, ensure that the incoming traffic is Cisco Express Forwarding-switched or Distributed Cisco Express Forwarding-switched. Traffic policing cannot be used on the switching path unless Cisco Express Forwarding or Distributed Cisco Express Forwarding switching is enabled.

Monitoring and Maintaining the Multiple Policer Actions

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

Configuration Examples

Example Multiple Actions in a Two-Rate Policer

In the following example, a policy map called police is configured to use a two-rate policer to police traffic leaving an interface. Two rates, a committed information rate (CIR) of 1 Mbps and a peak information rate (PIR) of 2 Mbps, have been specified.

```
Router(config)# policy-map police
Router(config-pmap)# class class-default
Router(config-pmap-c)# police cir 1000000 pir 2000000

Router(config-pmap-c-police)# conform-action transmit
Router(config-pmap-c-police)# exceed-action set-prec-transmit 4
Router(config-pmap-c-police)# exceed-action set-frde
Router(config-pmap-c-police)# violate-action set-prec-transmit 2
Router(config-pmap-c-police)# violate-action set-frde-transmit

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

The following actions will be performed on packets associated with the policy map called police:

- All packets marked as conforming to these rates (that is, packets conforming to the CIR) will be transmitted unaltered.
- All packets marked as exceeding these rates (that is, packets exceeding the CIR but not exceeding the PIR) will be assigned an IP Precedence level of 4, the DE bit will be set to 1, and then transmitted.
- All packets marked as violating the rate (that is, exceeding the PIR) will be assigned an IP Precedence level of 2, the DE bit will be set to 1, and then transmitted.

Example Verifying the Multiple Policer Actions

The following sample output of the **show policy-map**command displays the configuration for a service policy called police. In this service policy, multiple actions for packets marked as exceeding the specified CIR rate have been configured. For those packets, the IP Precedence level is set to 4, the DE bit is set to 1, and the packet is transmitted. Multiple actions for packets marked as violating the specified PIR rate have also been configured. For those packets, the IP Precedence level is set to 2, the DE bit is set to 1, and the packet is transmitted.

```
Router# show policy-map police
  Policy Map police
    Class class-default
     police cir 1000000 bc 31250 pir 2000000 be 31250
       conform-action transmit
       exceed-action set-prec-transmit 4
       exceed-action set-frde-transmit
       violate-action set-prec-transmit 2
       violate-action set-frde-transmit
```

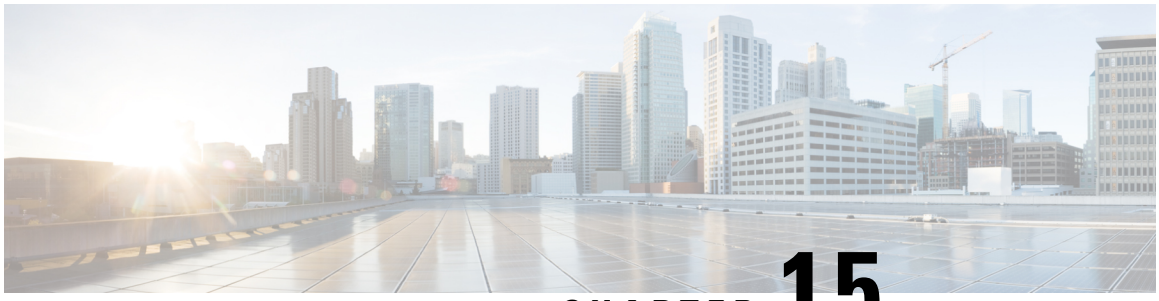
Feature Information for Policer Enhancement Multiple Actions

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

For more information about the platform support and Cisco software image support, use the Cisco Feature Navigator. To access the Cisco Feature Navigator, go to www.cisco.com/go/cfn. You do not need an account on Cisco.com to use this site.

Table 17: Feature Information for QoS for dVTI

Feature Name	Releases	Feature Information
Policer Enhancement Multiple Actions	Cisco IOS XE Release 2.1	Policer Enhancement Multiple Actions specifies multiple conform, exceed, and violate actions for marked packets.



CHAPTER 15

Control Plane Policing

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

Finding Feature Information

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

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

Restrictions for Control Plane Policing

Output Rate-Limiting Support

Output rate-limiting is performed in silent (packet discard) mode. Silent mode enables a router to silently discard packets using policy maps applied to output control plane traffic with the **service-policy output** command. For more information, see the "Output Rate-Limiting and Silent Mode Operation" section.

MQC Restrictions

The Control Plane Policing feature requires the Modular QoS CLI (MQC) to configure packet classification, packet marking, and traffic policing. All restrictions that apply when you use the MQC to configure traffic policing also apply when you configure control plane policing. Only two MQC commands are supported in policy maps—**police** and **set**.

Match Criteria Support and Restrictions

The following classification (match) criteria are supported:

- Standard and extended IP access control lists (ACLs).
- In class-map configuration mode, match criteria specified by the following commands:
  - **match dscp**
  - **match ip dscp**
  - **match ip precedence**
  - **match precedence**
  - **match protocol arp**
  - **match protocol ipv6**
  - **match protocol pppoe**

Note The **match protocol pppoe** command matches all PPPoE data packets that are sent to the control plane.

- **match protocol pppoe-discovery**

Note The **match protocol pppoe-discovery** command matches all PPPoE control packets that are sent to the control plane.

- **match qos-group**

Note The **match input-interface** command is not supported.

Note Features that require Network-Based Application Recognition (NBAR) classification may not work well at the control plane level.

Information About Control Plane Policing

Benefits of Control Plane Policing

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

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

Control Plane Terms to Understand

On the Cisco ASR 1000 Series Router, the following terms are used for the Control Plane Policing feature:

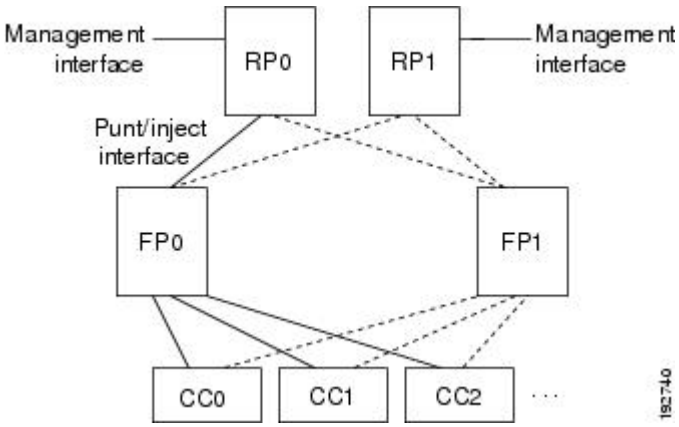
- Control plane—A collection of processes that run at the process level on the Route Processor (RP). These processes collectively provide high-level control for most Cisco IOS XE functions. The traffic sent to or sent by the control plane is called control traffic.
- Forwarding plane—A device that is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

Control Plane Policing Overview

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

These QoS rules are applied only after the packet has been determined to have the control plane as its destination or when a packet exits from the control plane. 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/SYN packets that are destined for the control plane to a maximum rate of 1 megabit per second.

Figure 4: Abstract Illustration of a Cisco ASR 1000 Series Router with Dual RPs and Dual Forwarding Panes



The figure above provides an abstract illustration of a Cisco ASR 1000 Series Router with dual RPs and dual forwarding planes. Only one RP and one forwarding plane are active at any time. The other RP and forwarding plane are in stand-by mode and do not receive traffic from the carrier card (CC). Packets destined to the control plane come in through the carrier card and then go through the active forwarding plane before being punted to the active RP. When an input QoS policy map is configured on the control plane, the active forwarding plane performs the QoS action (for example, a transmit, drop, or set action) before punting packets to the active RP in order to achieve the best protection of the control plane in the active RP.

On the other hand, packets exiting the control plane are injected to the active forwarding plane, and then go out through the carrier card. When an output QoS policy map is configured on the control plane, the active forwarding plane performs the QoS action after receiving the injected packets from the RP. This process saves the valuable CPU resource in the RP.

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

In high-availability (HA) mode, when an RP switchover happens, the active forwarding plane forwards traffic to the new active RP along the new punt/inject interface. The active forwarding plane continues to perform the CoPP function before punting traffic to the new active RP. When a forwarding plane switchover happens, the new active forwarding plane receives traffic from the carrier card and performs the CoPP function before punting traffic to the active RP.

Note The Cisco ASR 1000 Series Router handles some traditional control traffic in the forwarding plane directly to reduce the load on the control plane. One example is the IP Internet Control Message Protocol (ICMP) echo-request packet sent to this router. When a Cisco ASR1000 Series Router receives such packets, the packets are handled directly in the forwarding plane without being punted to the RP. In order to be consistent with other Cisco routers and to provide the same capability to control such packets using CoPP, the Cisco ASR 1000 series router extends the CoPP function on such packets, even though the packets are not punted to the RP. Customers can still use the CoPP function to rate-limit or to mark such packets.

Output Rate-Limiting and Silent Mode Operation

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

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

How to Use Control Plane Policing

Defining Control Plane Services

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

Note

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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **control-plane**
4. **service-policy** {**input** | **output** *policy-map-name*}
5. **end**

DETAILED STEPS

	Command or Action	Purpose
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.

	Command or Action	Purpose
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. • **output**—Applies the specified service policy to packets transmitted from the control plane and enables the device to silently discard packets. • *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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show policy-map control-plane** [**all**] [**input** [**class** *class-name*] | **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. • **output**—(Optional) Displays statistics for the attached output policy.

	Command or Action	Purpose
		• **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. This policy map polices traffic that matches the class map TEST, while allowing all other traffic (that matches the class map "class-default") to go through as is.

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

Control Plane
Service-policy input:TEST
Class-map:TEST (match-all)
      20 packets, 11280 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match:access-group 101
      police:
        8000 bps, 1500 limit, 1500 extended limit
        conformed 15 packets, 6210 bytes; action:transmit
        exceeded 5 packets, 5070 bytes; action:drop
        violated 0 packets, 0 bytes; action:drop
        conformed 0 bps, exceed 0 bps, violate 0 bps
Class-map:class-default (match-any)
      105325 packets, 11415151 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match:any
```

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

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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **access-list** *access-list-number* **permit** *protocol* {**any | host** {*address* | *name*}} {**any | host** {*address* | *name*}}
4. **access-list** *access-list-number* **permit** *protocol* {**tcd | udp**} {**any | host** {*source-addr* | *name*}} **eq** *port number* {**any | host** {*source-addr* | *name*}} **eq** *port number*
5. **class-map** *class-map-name*
6. **match access-group** *access-list-index*
7. **exit**
8. **policy-map** *policy-map-name*

9. **class** *class-map-name*
10. **police rate** *units* **pps**
11. **conform-action** *action*
12. **exit**
13. **exit**
14. **control plane** [**host | transit | cef-exception**]
15. **service-policy** {**input** | **output**} *policy-map-name*
16. **exit**
17. **exit**
18. **show control-plane** {**aggregate** | **cef-exception** | **counters** | **features** | **host** | **transit**}

DETAILED STEPS

	Command or Action	Purpose
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* {**any**	**host** {*address*	*name*}} {**any**	**host** {*address*	*name*}} **Example:** `Device(config)# access-list 140 permit 46 any any`	Configures an access list for filtering frames by protocol type.
Step 4	**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:** `Device(config)# access-list 141 permit udp any eq 1699 any eq 1698`	Configures an access list for filtering frames by UDP protocol and matches only packets with a given port number.
Step 5	**class-map** *class-map-name* **Example:** `Device(config)# class-map match-any MyClassMap`	Creates a class-map and enters QoS class-map configuration mode.
Step 6	**match access-group** *access-list-index* **Example:** `Device(config-cmap)# match access-group 140`	Specifies access groups to apply to an identity policy. The range of valid values is 1-2799.
Step 7	**exit** **Example:** `Device(config-cmap)# exit`	Exits QoS class-map configuration mode and returns to global configuration mode.

	Command or Action	Purpose
Step 8	**policy-map** *policy-map-name* **Example:** `Device(config)# policy-map Policy1`	Specifies a service policy and enters QoS policy-map configuration mode.
Step 9	**class** *class-map-name* **Example:** `Device(config-pmap-)# class MyClassMap`	Enters QoS policy-map class configuration more
Step 10	**police rate** *units* **pps** **Example:** `Device(config-pmap-c)# police rate 10 pps`	Polices traffic destined for the control plane at a specified rate.
Step 11	**conform-action** *action* **Example:** `Device(config-pmap-c-police)# conform-action transmit`	(Optional) Specifies the action to take on packets that conform to the police rate limit and enters policy-map class police configuration mode.
Step 12	**exit** **Example:** `Device(config-pmap-c-police)# exit`	Exits policy-map class police configuration mode
Step 13	**exit** **Example:** `Device(config-pmap-)# exit`	Exits policy-map class configuration mode
Step 14	**control plane** [**host** | **transit** | **cef-exception**] **Example:** `Device(config)# control-plane`	Associates or modifies attributes (such as a service policy) that are associated with the control plane of the device and enters control plane configuration mode.
Step 15	**service-policy** {**input** | **output**} *policy-map-name* **Example:** `Device(config-cp)# service-policy input Policy1`	Attaches a policy map to a control plane.
Step 16	**exit** **Example:** `Device(config-cp)# exit`	Exits control plane configuration mode and returns to global configuration mode.
Step 17	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode returns to privileged EXEC mode.
Step 18	**show control-plane** {**aggregate** | **cef-exception** | **counters** | **features** | **host** | **transit**} **Example:** `Device# show control-plane features`	Displays the configured control plane features

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 without constraint while allowing all remaining Telnet packets to be policed at the specified rate.

```
! Allow 10.1.1.1 trusted host traffic.
Device(config)# access-list 140 deny tcp host 10.1.1.1 any eq telnet

! Allow 10.1.1.2 trusted host traffic.
Device(config)# access-list 140 deny tcp host 10.1.1.2 any eq telnet

! Rate-limit all other Telnet traffic.
Device(config)# access-list 140 permit tcp any any eq telnet
! Define class-map "telnet-class."
Device(config)# class-map telnet-class

Device(config-cmap)# match access-group 140
Device(config-cmap)# exit
Device(config)# policy-map control-plane-in
Device(config-pmap)# class telnet-class
Device(config-pmap-c)# police 80000 conform transmit exceed drop
Device(config-pmap-c)# exit
Device(config-pmap)# exit
! Define aggregate control plane service for the active route processor.
Device(config)# control-plane
Device(config-cp)# service-policy input control-plane-in
Device(config-cp)# end
```

Example: Configuring Control Plane Policing on Output ICMP Traffic

The following example shows how to apply a QoS policy for aggregate control plane services to Telnet traffic transmitted from the control plane. Trusted networks with source addresses 10.0.0.0 and 10.0.0.1 receive Internet Control Management Protocol (ICMP) port-unreachable responses without constraint while allowing all remaining ICMP port-unreachable responses to be dropped.

```
! Allow 10.0.0.0 trusted network traffic.
Device(config)# access-list 141 deny icmp 10.0.0.0 0.0.0.255 any port-unreachable

! Allow
10.0.0.1
 trusted network traffic.
Device(config)# access-list 141 deny icmp 10.0.0.1 0.0.0.255 any port-unreachable

! Rate-limit all other ICMP traffic.
Device(config)# access-list 141 permit icmp any any port-unreachable
Device(config)# class-map icmp-class

Device(config-cmap)# match access-group 141
Device(config-cmap)# exit
Device(config)# policy-map control-plane-out
```

```
! Drop all traffic that matches the class "icmp-class."
Device(config-pmap)# class icmp-class
Device(config-pmap-c)# drop
Device(config-pmap-c)# exit
Device(config-pmap)# exit
Device(config)# control-plane
! Define aggregate control plane service for the active route processor.
Device(config-cp)# service-policy output control-plane-out
Device(config-cp)# end
```

Example: Marking Output Control Plane Packets

The following example shows how to apply a QoS policy on the control plane to mark all egress IPv6 echo-request packets with IPv6 precedence 6.

```
! Match all IPv6 Echo Requests
Device(config)# ipv6 access-list coppacl-ipv6-icmp-request
Device(config-ipv6-acl)# permit icmp any any echo-request
Device(config-ipv6-acl)# exit
Device(config)# class-map match-all coppclass-ipv6-icmp-request
Device(config-cmap)# match access-group name coppacl-ipv6-icmp-request
Device(config-cmap)# exit
! Set all egress IPv6 Echo Requests with precedence 6
Device(config)# policy-map copp-policy
Device(config-pmap)# class coppclass-ipv6-icmp-request
Device(config-pmap-c)# set precedence 6
Device(config-pmap-c)# exit
Device(config-pmap)# exit
! Define control plane service for the active route processor.
Device(config)# control-plane
Device(config-cp)# service-policy output copp-policy
Device(config-cp)# end
```

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

The following example shows how to configure control plane policing (CoPP) to police RSVP packets at a specified rate and displays configured CoPP features.

```
Device> enable
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# access-list 140 permit 46 any any
Device(config)# access-list 141 permit adp any eq 1699 any eq 1698
Device(config)# class-map match-any MyClassMap
Device(config-cmap)# match access-group 140
Device(config-cmap)# match access-group 141
Device(config-cmap)# exit
Device(config)# policy-map Policy1
Device(config-pmap)# class MyClassMap
Device(config-pmap-c)# police rate 10 pps
Device(config-pmap-c-police)# conform-action transmit
Device(config-pmap-c-police)# exceed-action drop
Device(config-pmap-c-police)# exit
Device(config-pmap-c)# exit
Device(config-pmap)# exit
Device(config)# control-plane
```

```
Device(config-cp)# service-policy input Policy1
Device(config-cp)#
*Sep 14 08:07:39.898: %CP-5-FEATURE: Control-plane Policing feature enabled on Control plane
 aggregate path
Device(config-cp)#
Device(config-c p)# exit
Device(config)# exit
Device#
*Sep 14 08:09:04.154: %SYS-5-CONFIG_I: Configured from console by console
Device# show control-plane features
Total 1 features configured

Control plane aggregate path features :

-----------------------------------------------------
Control-plane Policing activated Sep 14 2012 08:0

-----------------------------------------------------
```

Information About Per-Interface QoS for PPPoE Punt Traffics on Cisco ASR 1000 Series Routers

Overview of the Per-Interface QoS for PPPoE Punt Traffic Feature

Prior to Cisco IOS XE Release 3.12, PPP over Ethernet (PPPoE) punt traffic policing was performed only on the control plane. However, this policing could not be applied to the input interface. Effective from Cisco IOS XE 3.12S, the Per-Interface QoS for PPPoE Punt Traffic feature applies QoS policing and matching for PPPoE traffic on both the interface and the control plane. This feature polices the PPPoE discovery and PPPoE Link Control Protocol (LCP) packets on the interface of the Point-to-Point Termination and Aggregation (PTA) and the Local Access Concentrator (LAC). Policing the PPPoE discovery and PPPoE LCP packets on the interface has an important role in reducing the load on the control plane. Punt traffic on input interface will go to the control plane.

For QoS policy maps, applying the policer on both the interface and the control plane improves network availability. It also provides the customer with the flexibility required for implementing security and policing.

Enabling QoS Policing and Matching for PPPoE Traffic on the Input Interface

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **platform qos punt-path-matching**
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**platform qos punt-path-matching** **Example:** `Device(config)# platform qos punt-path-matching`	Enables QoS policing and matching for PPPoE traffic on the input interface.
Step 4	**end** **Example:** `Device(config)# end`	(Optional) Returns to privileged EXEC mode.

Disabling QoS Policing and Matching for PPPoE Traffic on the Input Interface

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **no platform qos punt-path-matching**
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**no platform qos punt-path-matching** **Example:** `Device(config)# no platform qos punt-path-matching`	Disables QoS policing and matching for PPPoE traffic on the input interface.

	Command or Action	Purpose
Step 4	**end** **Example:** `Device(config)# end`	(Optional) Returns to privileged EXEC mode.

Example: Configuring PPPoE and PPPoE Discovery Packets on the Input Interface and Control Plane

The following example shows how to configure PPPoE and PPPoE discovery packets on the input interface and control plane:

```
Device#configure terminal
Device(config)#class-map pppoed
Device(config-cmap)#match protocol pppoe-discovery
Device(config-cmap)#class-map pppoe
Device(config-cmap)#match protocol pppoe
Device(config-cmap)#policy-map pppoe-input
Device(config-pmap)#class pppoed

Device(config-pmap-c)#police 10000
Device(config-pmap-c-police)#class pppoe
Device(config-pmap-c)#police 10000
Device(config-pmap-c-police)#int g0/0/0.100
Device(config-subif)#service-p input pppoe-input

Device(config-subif)#end

Device#show platform hardware qfp active feature qos config global

Punt-Path-Matching are: enabled
```

Additional References for Control Plane Policing

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
QoS features overview	“Quality of Service Overview” module
MQC	“Applying QoS Features Using the MQC” module
Security features overview	“Security Overview” module

MIBs

MIB	MIBs Link
CISCO-CLASS-BASED-QOS-MIB	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

Feature Information for Control Plane Policing

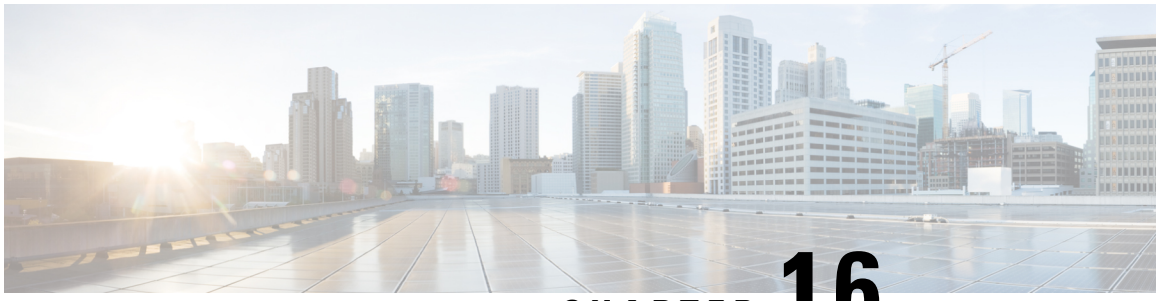
The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train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

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

Table 18: Feature Information for Control Plane Policing

Feature Name	Releases	Feature Information
Control Plane Policing	Cisco IOS XE Release 2.1 Cisco IOS XE Release 2.2	The Control Plane Policing feature allows users to configure a quality of service (QoS) filter that manages the traffic flow of control plane packets to protect the control plane of Cisco IOS routers and switches against reconnaissance and denial-of-service (DoS) attacks. For Cisco IOS XE Release 2.1, this feature was implemented on Cisco ASR 1000 Series Routers. For Cisco IOS XE Release 2.2, this feature was modified to include support for packet marking, output rate-limiting, and additional match criteria. The following commands were introduced or modified: **match protocol pppoe**, **match protocol pppoe-discovery**.

Feature Name	Releases	Feature Information
Per-Interface QoS for PPPoE Punt Traffic on Cisco ASR 1000 Series Routers	Cisco IOS XE Release 3.12	The Per-Interface QoS for PPPoE Punt Traffic on Cisco ASR 1000 Series Routers feature applies QoS policing and matching for PPPoE traffic on both the interface and the control plane. The following command was introduced: **platform qos punt-path-matching**



CHAPTER 16

Management Plane Protection

First Published: February 27, 2006

Last Updated: February 27, 2006

The Management Plane Protection (MPP) feature in Cisco IOS software provides the capability to restrict the interfaces on which network management packets are allowed to enter a device. The MPP feature allows a network operator to designate one or more router interfaces as management interfaces. Device management traffic is permitted to enter a device only through these management interfaces. After MPP is enabled, no interfaces except designated management interfaces will accept network management traffic destined to the device.

Restricting management packets to designated interfaces provides greater control over management of a device, providing more security for that device. Other benefits include improved performance for data packets on nonmanagement interfaces, support for network scalability, need for fewer access control lists (ACLs) to restrict access to a device, and management packet floods on switching and routing interfaces are prevented from reaching the CPU.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. For a list of the releases in which a feature is supported, see Feature Information for Management Plane Protection, on page 170.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn . You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Finding Feature Information

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

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

Feature Information for Management Plane Protection

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

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

Feature Information for Management Plane Protection

Feature Name	Releases	Feature Information
Management Plane Protection	12.4(6)T	Provides the capability to restrict the interfaces on which network management packets are allowed to enter a device.
SMI over Virtual Template	Cisco IOS XE Release 3.16S	Provides the capability to configure management plane protection on a virtual template interface.

Prerequisites for Management Plane Protection

- IP Cisco Express Forwarding must be enabled before a management interface can be configured.

Restrictions for Management Plane Protection

- Out-of-band management interfaces (also called dedicated management interfaces) are not supported. An out-of-band management interface is a dedicated Cisco IOS physical or logical interface that processes management traffic only.
- Loopback and virtual interfaces not associated to physical interfaces are not supported.
- Fallback and standby management interfaces are not supported.
- Hardware-switched and distributed platforms are not supported.

- Secure Copy (SCP) is supported under the Secure Shell (SSH) Protocol and not directly configurable in the command-line interface (CLI).
- Uninformed management stations lose access to the router through nondesignated management interfaces when the Management Plane Protection feature is enabled.
- This feature supports only IPv4 traffic. IPv6 traffic is neither blocked nor denied.

Information About Management Plane Protection

Before you enable the Management Plane Protection feature, you should understand the following concepts:

In-Band Management Interface

An in-band management interface is a Cisco IOS physical or logical interface that processes management as well as data-forwarding packets. Loopback interfaces commonly are used as the primary port for network management packets. External applications communicating with a networking device direct network management requests to the loopback port. An in-band management interface is also called a shared management interface.

Control Plane Protection Overview

A control plane is a collection of processes that run at the process level on a route processor and collectively provide high-level control for most Cisco IOS software functions. All traffic directly or indirectly destined to a router is handled by the control plane.

Control Plane Policing (CoPP) is a Cisco IOS control-plane feature that offers rate limiting of all control-plane traffic. CoPP allows you to configure a quality of service (QoS) filter that manages the traffic flow of control plane packets. This QoS filter helps to protect the control plane of Cisco IOS routers and switches against denial-of-service (DoS) attacks and helps to maintain packet forwarding and protocol states during an attack or during heavy traffic loads.

Control Plane Protection is a framework that encompasses all policing and protection features in the control plane. The Control Plane Protection feature extends the policing functionality of the CoPP feature by allowing finer policing granularity. Control Plane Protection also includes a traffic classifier, which intercepts control-plane traffic and classifies it in control-plane categories. Management Plane Protection operates within the Control Plane Protection infrastructure.

For more information about the Control Plane Policing feature in Cisco IOS software, see the Control Plane Policing module.

For more information about the Control Plane Protection feature in Cisco IOS software, see the Control Plane Protection module .

Management Plane

The management plane is the logical path of all traffic related to the management of a routing platform. One of three planes in a communication architecture that is structured in layers and planes, the management plane performs management functions for a network and coordinates functions among all the planes (management, control, data). The management plane also is used to manage a device through its connection to the network.

Examples of protocols processed in the management plane are Simple Network Management Protocol (SNMP), Telnet, HTTP, Secure HTTP (HTTPS), and SSH. These management protocols are used for monitoring and for CLI access. Restricting access to devices to internal sources (trusted networks) is critical.

Management Plane Protection Feature

The MPP feature in Cisco IOS software provides the capability to restrict the interfaces on which network management packets are allowed to enter a device. The MPP feature allows a network operator to designate one or more router interfaces as management interfaces. Device management traffic is permitted to enter a device through these management interfaces. After MPP is enabled, no interfaces except designated management interfaces will accept network management traffic destined to the device. Restricting management packets to designated interfaces provides greater control over management of a device.

The MPP feature is disabled by default. When you enable the feature, you must designate one or more interfaces as management interfaces and configure the management protocols that will be allowed on those interfaces. The feature does not provide a default management interface. Using a single CLI command, you can configure, modify, or delete a management interface.When you configure a management interface, no interfaces except that management interface will accept network management packets destined to the device. When the last configured interface is deleted, the feature turns itself off.

Following are the management protocols that the MPP feature supports. These management protocols are also the only protocols affected when MPP is enabled.

- Blocks Extensible Exchange Protocol (BEEP)
- FTP
- HTTP
- HTTPS
- SSH, v1 and v2
- SNMP, all versions
- Telnet
- TFTP

Cisco IOS features enabled on management interfaces remain available when the MPP feature is enabled. Nonmanagement packets such as routing and Address Resolution Protocol (ARP) messages for in-band management interfaces are not affected.

This feature generates a syslog for the following events:

- When the feature is enabled or disabled
- When a management interface fails.

For example, a failure will occur when the management interface cannot successfully receive or process packets destined for the control plane for reasons other than resource exhaustion.

Benefits of the Management Plane Protection Feature

Implementing the MPP feature provides the following benefits:

- Greater access control for managing a device than allowing management protocols on all interfaces
- Improved performance for data packets on nonmanagement interfaces
- Support for network scalability
- Simplifies the task of using per-interface ACLs to restrict management access to the device
- Fewer ACLs needed to restrict access to the device

- Management packet floods on switching and routing interfaces are prevented from reaching the CPU

How to Configure a Device for Management Plane Protection

This section contains the following task:

Configuring a Device for Management Plane Protection

Perform this task to configure a device that you have just added to your network or a device already operating in your network. This task shows how to configure MPP where SSH and SNMP are allowed to access the router only through the FastEthernet 0/0 interface.

Before you begin

- IP Cisco Express Forwarding must be enabled before a management interface can be configured.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **control-plane host**
4. **management-interface** *interface* **allow** *protocols*
5. **Ctrl z**
6. **show management-interface** [*interface* | **protocol** *protocol-name*]

DETAILED STEPS

	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	**control-plane host** **Example:** `Router(config)# control-plane host`	Enters control-plane host configuration mode.

	Command or Action	Purpose
Step 4	**management-interface** *interface* **allow** *protocols* **Example:** `Router(config-cp-host)# management-interface FastEthernet 0/0 allow ssh snmp`	Configures an interface to be a management interface, which will accept management protocols, and specifies which management protocols are allowed. • *interface*—Name of the interface that you are designating as a management interface. **Note** Effective with Cisco IOS XE Release 3.16S, you can configure a virtual template interface. • *protocols*—Management protocols you want to allow on the designated management interface. • BEEP • FTP • HTTP • HTTPS • SSH, v1 and v2 • SNMP, all versions • Telnet • TFTP
Step 5	**Ctrl z** **Example:** `Router(config-cp-host)# Ctrl z`	Returns to privileged EXEC mode.
Step 6	**show management-interface** [*interface* | **protocol** *protocol-name*] **Example:** `Router# show management-interface FastEthernet 0/0`	Displays information about the management interface such as type of interface, protocols enabled on the interface, and number of packets dropped and processed. *interface*—(Optional) Interface for which you want to view information. **protocol**—(Optional) Indicates that a protocol is specified. *protocol-name*—(Optional) Protocol for which you want to view information

Examples

The configuration in this example shows MPP configured to allow SSH and SNMP to access the router only through the FastEthernet 0/0 interface. This configuration results in all protocols in the remaining subset of supported management protocols to be dropped on all interfaces unless explicitly permitted. BEEP, FTP, HTTP, HTTPS, Telnet, and TFTP will not be permitted to access the router through any interfaces, including FastEthernet 0/0. Additionally, SNMP and SSH will be dropped on all interfaces except FastEthernet 0/0, where it is explicitly allowed.

To allow other supported management protocols to access the router, you must explicitly allow these protocols by adding them to the protocol list for the FastEthernet 0/0 interface or enabling additional management interfaces and protocols.

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# control-plane host
Router(config-cp-host)# management-interface FastEthernet 0/0 allow ssh snmp
Router(config-cp-host)#
.Aug  2 15:25:32.846: %CP-5-FEATURE: Management-Interface feature enabled on Control plane
 host path
Router(config-cp-host)#
```

The following is output from the **show management-interface** command issued after configuring MPP in the previous example. The **show management-interface** command is useful for verifying your configuration.

```
Router# show management-interface
Management interface FastEthernet0/0
        Protocol        Packets processed
             ssh                0
            snmp                0
Router#
```

Configuration Examples for Management Plane Protection

This section provides the following configuration example:

Configuring Management Plane Protection on Gigabit Ethernet Interfaces: Example

The following example shows how to configure MPP where only SSH, SNMP, and HTTP are allowed to access the router through the Gigabit Ethernet 0/3 interface and only HTTP is allowed to access the router through the Gigabit Ethernet 0/2 interface.

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# control-plane host
Router(config-cp-host)# management-interface GigabitEthernet 0/3 allow http ssh snmp

Router(config-cp-host)#
.Aug  2 17:00:24.511: %CP-5-FEATURE: Management-Interface feature enabled on Control plane
 host path
Router(config-cp-host)# management-interface GigabitEthernet 0/2 allow http
Router(config-cp-host)#
```

The following is output from the **show management-interface** command issued after configuring MPP in the previous example. The **show management-interface** command is useful for verifying your configuration.

```
Router# show management-interface

Management interface GigabitEthernet0/2
        Protocol        Packets processed
            http                0
Management interface GigabitEthernet0/3
        Protocol        Packets processed
            http                0
             ssh                0
            snmp                0
```

Additional References for Management Plane Protection

The following sections provide references related to Management Plane Protection.

Related Documents

Related Topic	Document Title
Network management	Cisco IOS Network Management Configuration Guide
Network security	Cisco IOS Security Configuration Guide
Control Plane Policing	Control Plane Policing module
Control Plane Protection	Control Plane Protection module

RFCs

RFC	Title
RFC 3871	Operational Security Requirements for Large Internet Service Provider (ISP) IP Network Infrastructure

Technical Assistance

Description	Link
The Cisco Technical Support and Documentation website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Feature Information for Management Plane Protection

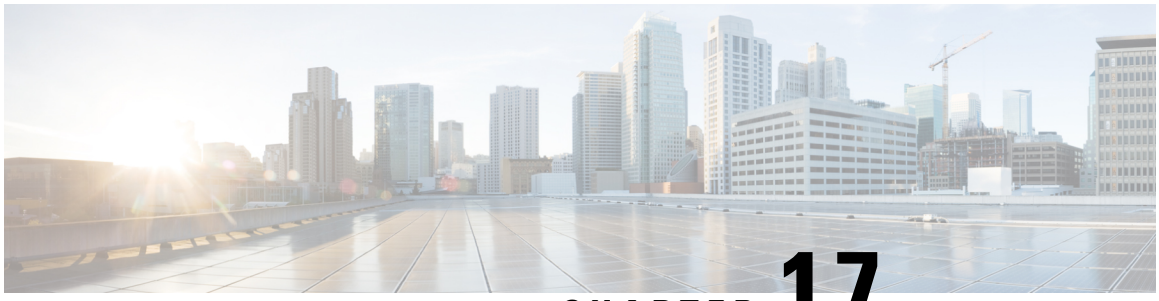
The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train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

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

Feature Information for Management Plane Protection

Feature Name	Releases	Feature Information
Management Plane Protection	12.4(6)T	Provides the capability to restrict the interfaces on which network

Feature Name	Releases	Feature Information
		management packets are allowed to enter a device.
SMI over Virtual Template	Cisco IOS XE Release 3.16S	Provides the capability to configure management plane protection on a virtual template interface.



CHAPTER 17

Class-Based Policing

Class-based policing allows you to control the maximum rate of traffic that is 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.

Finding Feature Information

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

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

Information About Class-Based Policing

Class-Based Policing Functionality

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.

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 that contains the class-based policing configuration to an interface.

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.

Benefits of Class-Based Policing

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.

- 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.
- Use class-based policing to assign packets to a QoS group. The router uses the QoS group to determine how to prioritize packets.

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.

Restrictions for Class-Based Policing

Class-based policing can be configured on an interface or a subinterface, but it is not supported on EtherChannel or tunnel interfaces.

Restrictions for the Cisco ASR 903 Router

- Class-based policing on subinterfaces is not supported.
- Policing is supported for ingress policy maps only.
- Hierarchical policing (policing at both parent level and child level) is not supported.

How to Configure Class-Based Policing

Configuring a Traffic Policing Service Policy

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **class-map** [**match-all** | **match-any**] *class-map-name*
4. **match ip precedence** *precedence-value*
5. **exit**
6. **policy-map** *policy-map-name*
7. **class** {*class-name* | **class-default**}
8. **police** *bps burst-normal burst-max* **conform-action** *action* **exceed-action** *action* **violate-action** *action*
9. **exit**
10. **exit**
11. **interface** *interface-type interface-number*
12. **service-policy** {**input** | **output**} *policy-map-name*
13. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables higher privilege levels, such as privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**class-map** [**match-all**	**match-any**] *class-map-name* **Example:** `Router(config)# class-map match-any MATCH_PREC`	Specifies the name of the class map to be created and enters QoS class map configuration mode. • The class map defines the criteria to use to differentiate the traffic. For example, you can use the class map to differentiate voice traffic from data traffic, based on a series of match criteria defined using the **match** command.

	Command or Action	Purpose
		Note If the **match-all** or **match-any** keyword is not specified, traffic must match all the match criteria to be classified as part of the traffic class.
Step 4	**match ip precedence** *precedence-value* **Example:** `Router(config-cmap)# match ip precedence 0`	Enables packet matching on the basis of the IP precedence values you specify. **Note** You can enter up to four matching criteria, as number abbreviation (0 to 7) or criteria names (critical, flash, and so on), in a single match statement.
Step 5	**exit** **Example:** `Router(config-cmap)# exit`	Returns to global configuration mode.
Step 6	**policy-map** *policy-map-name* **Example:** `Router(config)# policy-map POLICE-SETTING`	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy, and enters QoS policy-map configuration mode.
Step 7	**class** {*class-name* | **class-default**} **Example:** `Router(config-pmap)# class MATCH_PREC`	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, and enters policy-map class configuration mode.
Step 8	**police** *bps burst-normal burst-max* **conform-action** *action* **exceed-action** *action* **violate-action** *action* **Example:** `Router(config-pmap-c)# police 8000 1000 1000 conform-action transmit exceed-action set-qos-transmit 1 violate-action drop`	Configures traffic policing according to burst sizes and any optional actions specified.
Step 9	**exit** **Example:** `Router(config-pmap-c)# exit`	(Optional) Exits policy-map class configuration mode.
Step 10	**exit** **Example:** `Router(config-pmap)# exit`	(Optional) Exits QoS policy-map configuration mode.
Step 11	**interface** *interface-type interface-number* **Example:**	Configures an interface type and enters interface configuration mode.

	Command or Action	Purpose
	`Router(config)# interface GigabitEthernet 0/0/1`	• Enter the interface type and interface number.
Step 12	**service-policy** {**input** | **output**} *policy-map-name* **Example:** `Router(config-if)# service-policy input POLICE-SETTING`	Attaches a policy map to an interface. • Enter either the **input** or **output** keyword and the policy map name.
Step 13	**end** **Example:** `Router(config-if)# end`	(Optional) Exits interface configuration mode and returns to privileged EXEC mode.

Monitoring and Maintaining Traffic Policing

SUMMARY STEPS

1. **enable**
2. **show policy-map**
3. **show policy-map** *policy-map-name*
4. **show policy-map interface**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show policy-map** **Example:** `Router# show policy-map`	Displays all configured policy maps.
Step 3	**show policy-map** *policy-map-name* **Example:** `Router# show policy-map pmap`	Displays the user-specified policy map.
Step 4	**show policy-map interface** **Example:** `Router# show policy-map interface`	Verifies that the Class-Based Policing feature is configured on your interface. If the feature is configured on your interface. • The command output displays policing statistics.

Verifying Class-Based Traffic Policing

Use the **show policy-map interface** 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.

SUMMARY STEPS

1. **enable**
2. **show policy-map interface**
3. **show policy-map interface** *type interface*
4. **show policy-map interface** *type interface* **service instance** *service-instance number*
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show policy-map interface** **Example:** `Router# show policy-map interface`	Verifies that the Class-Based Policing feature is configured on your interface. If the feature is configured on your interface. • The command output displays policing statistics.
Step 3	**show policy-map interface** *type interface* **Example:** `Router# show policy-map interface GigabitEthernet 0/0/1`	Displays traffic statistics for policies applied to a specific interface.
Step 4	**show policy-map interface** *type interface* **service instance** *service-instance number* **Example:** `Router# show policy-map interface GigabitEthernet 0/0/1 service instance 1`	Displays the policy map information for a given service instance under an interface.
Step 5	**exit** **Example:** `Router# exit`	(Optional) Exits privileged EXEC mode.

Example: Verifying Class-Based Traffic Policing

```
Router# show policy-map interface
  FastEthernet1/1/1
  service-policy output: x
    class-map: a (match-all)
      0 packets, 0 bytes
      5 minute rate 0 bps
      match: ip precedence 0
      police:
        1000000 bps, 10000 limit, 10000 extended limit
        conformed 0 packets, 0 bytes; action: transmit
        exceeded 0 packets, 0 bytes; action: drop
        conformed 0 bps, exceed 0 bps, violate 0 bps
```

Troubleshooting Tips

Check the interface type. Verify that class-based policing is supported on your interface. .

Configuration Examples for Class-Based Policing

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 the interface.

```
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 FastEthernet interface 1/1/1 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 is greater than the length of the packet (for example, B), then the packet conforms and B bytes should be removed from the bucket. 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 is less than the length of the packet, but the number of bytes in the exceed bucket is greater than the length of the packet (for example, B), the packet exceeds and B bytes are removed from the bucket.
- 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 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.

Verifying Class-Based Traffic Policing

Use the **show policy-map interface** 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:

```
Router# show policy-map interface
  FastEthernet1/1/1
  service-policy output: x
    class-map: a (match-all)
      0 packets, 0 bytes
      5 minute rate 0 bps
      match: ip precedence 0
      police:
        1000000 bps, 10000 limit, 10000 extended limit
        conformed 0 packets, 0 bytes; action: transmit
        exceeded 0 packets, 0 bytes; action: drop
        conformed 0 bps, exceed 0 bps, violate 0 bps
```

Use the **show policy-map interface** *type nummber* command to view the traffic statistics for policies applied to that specific interface:

```
Router# show policy-map interface gigabitethernet 0/0/1
 GigabitEthernet0/0/1

  Service-policy input: TUNNEL_MARKING

    Class-map: MATCH_PREC (match-any)
      72417 packets, 25418367 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: ip precedence 0
      QoS Set
        ip precedence tunnel 3
          Marker statistics: Disabled

    Class-map: MATCH_DSCP (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: ip dscp default (0)
      QoS Set
        ip dscp tunnel 3
          Marker statistics: Disabled

    Class-map: class-default (match-any)
      346462 packets, 28014400 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: any

  Service-policy output: POLICE-SETTING

    Class-map: MATCH_PREC (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: ip precedence 0
      police:
          cir 8000 bps, bc 1000 bytes, be 1000 bytes
        conformed 0 packets, 0 bytes; actions:
          transmit
        exceeded 0 packets, 0 bytes; actions:
          set-qos-transmit 1
        violated 0 packets, 0 bytes; actions:
          drop
        conformed 0000 bps, exceed 0000 bps, violate 0000 bps

    Class-map: class-default (match-any)
      31 packets, 2019 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: any
```

Use the **show policy-map interface service instance** command to view the traffic statistics for policy applied to the specific service instance in that specific interface:

```
Router# show policy-map interface gig0/0/1 service instance 10
 GigabitEthernet0/0/1: EFP 10

       Service-policy input: ac1

 Class-map: ac1 (match-all)
   0 packets, 0 bytes
   5 minute offered rate 0000 bps, drop rate 0000 bps
   Match: access-group 1
   police:
       cir 50000000 bps, bc 1562500 bytes
     conformed 0 packets, 0 bytes; actions:
       transmit
```

```
    exceeded 0 packets, 0 bytes; actions:
      drop
    conformed 0000 bps, exceeded 0000 bps

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

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"
Modular Quality of Service Command-Line Interface (MQC)	"Applying QoS Features Using the MQC" module

Standards

Standard	Title
None	--

MIBs

MIB	MIBs Link
Class-Based Quality of Service MIB • CISCO-CLASS-BASED-QOS-MIB • CISCO-CLASS-BASED-QOS-CAPABILITY-MIB	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
RFC 2697	*A Single Rate Three Color Marker*

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

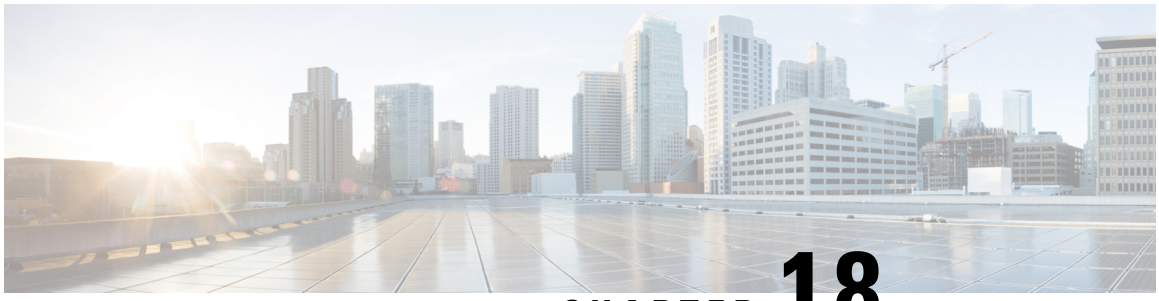
Feature Information for Class-Based Policing

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

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

Table 19: Feature Information for Class-Based Policing

Feature Name	Releases	Feature Information
Class-Based Policing	Cisco IOS XE Release 2.1 Cisco IOS XE Release 3.5S Cisco IOS XE Release 3.16	This feature was introduced on Cisco ASR 1000 Series Routers. In Cisco IOS XE Release 3.5S, support was added for the Cisco ASR 903 Router. In Cisco IOS XE Release 3.16, support was added for the Cisco ASR 900 RSP3 Module. The following command was introduced or modified: **police**.



CHAPTER 18

QoS Percentage-Based Policing

The QoS Percentage-Based Policing feature allows you to configure traffic policing and traffic shaping on the basis of a percentage of bandwidth available on the interface. This feature also allows you to specify the committed burst (bc) size and the excess burst (be) size (used for configuring traffic policing) in milliseconds (ms). Configuring traffic policing in this manner enables you to use the same policy map for multiple interfaces with differing amounts of bandwidth.

Finding Feature Information

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

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

Information About QoS Percentage-Based Policing

Benefits for QoS Percentage-Based Policing

This feature provides the ability to configure traffic policing on the basis of a percentage of bandwidth available on an interface, and it allows you to specify burst sizes in milliseconds. Configuring traffic policing in this manner enables you to use the same policy map for multiple interfaces with differing amounts of bandwidth. That is, you do not have to recalculate the bandwidth for each interface or configure a different policy map for each type of interface.

Configuration of Class and Policy Maps for QoS Percentage-Based Policing

To configure the QoS: Percentage-Based Policing feature, you must define a traffic class, configure a policy map, and then attach that policy map to the appropriate interface.

The MQC is a command-line interface that allows you to define traffic classes, create and configure traffic policies (policy maps), and then attach these traffic policies to interfaces.

In the MQC, the **class-map** command is used to define a traffic class (which is then associated with a traffic policy). The purpose of a traffic class is to classify traffic.

The MQC consists of the following three processes:

- Defining a traffic class with the **class-map** command.
- Creating a traffic policy by associating the traffic class with one or more QoS features (using the **policy-map** command).
- Attaching the traffic policy to the interface with the **service-policy** command.

A traffic class contains three major elements: a name, a series of match commands, and, if more than one **match** command exists in the traffic class, an instruction on how to evaluate these **match** commands (that is, match-all or match-any). The traffic class is named in the **class-map** command line; for example, if you enter the **class-map cisco** command while configuring the traffic class in the CLI, the traffic class would be named "cisco".

The **match** commands are used to specify various criteria for classifying packets. Packets are checked to determine whether they match the criteria specified in the **match** commands. If a packet matches the specified criteria, that packet is considered a member of the class and is forwarded according to the QoS specifications set in the traffic policy. Packets that fail to meet any of the matching criteria are classified as members of the default traffic class.

Traffic Regulation Mechanisms and Bandwidth Percentages

quality of service (QoS) offers two kinds of traffic regulation mechanisms--traffic policing and traffic shaping. A traffic policer typically drops traffic that violates a specific rate. A traffic shaper typically delays excess traffic using a buffer to hold packets and shapes the flow when the data rate to a queue is higher than expected.

Traffic shaping and traffic policing can work in tandem and can be configured in a class map. Class maps organize data packets into specific categories ("classes") that can, in turn, receive a user-defined QoS treatment when used in policy maps (sometimes referred to as "service policies").

Before this feature, traffic policing and traffic shaping were configured on the basis of a user-specified amount of bandwidth available on the interface. Policy maps were then configured on the basis of that specific amount of bandwidth, meaning that separate policy maps were required for each interface.

This feature provides the ability to configure traffic policing and traffic shaping on the basis of a *percentage* of bandwidth available on the interface. Configuring traffic policing and traffic shaping in this manner enables customers to use the same policy map for multiple interfaces with differing amounts of bandwidth.

Configuring traffic policing and shaping on the basis of a percentage of bandwidth is accomplished by using the **police** (percent) and **shape** (percent) commands.

Burst Size in Milliseconds Option

The purpose of the burst parameters (bc and be) is to drop packets gradually and to avoid tail drop. Setting sufficiently high burst values helps to ensure good throughput.

This feature allows you the option of specifying the committed burst (bc) size and the extended burst (be) as milliseconds (ms) of the class bandwidth when you configure traffic policing. The number of milliseconds is used to calculate the number of bytes that will be used by the QoS: Percentage-Based Policing feature.

Specifying these burst sizes in milliseconds is accomplished by using the **bc** and **be** keywords (and their associated arguments) of the **police** (percent) and **shape** (percent) commands.

How to Configure QoS Percentage-Based Policing

Configuring a Class and Policy Map for Percentage-Based Policing

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map** *policy-name*
4. **class** {*class-name* **class-default**}
5. **police cir percent** *percentage* [*burst-in-ms*] [**bc** *conform-burst-in-msec* **ms**] [**be** *peak-burst-in-msec* **ms**] [**pir percent** *percent*]
6. **exit**

DETAILED STEPS

	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-name* **Example:** `Router(config)# policy-map policy1`	Specifies the name of the policy map to be created. Enters policy-map configuration mode. • Enter the policy map name.

	Command or Action	Purpose
Step 4	**class** {*class-name* **class-default**} **Example:** `Router(config-pmap)# class class1`	Specifies the class so that you can configure or modify its policy. Enters policy-map class configuration mode. • Enter the class name or specify the default class (class-default).
Step 5	**police cir percent** *percentage* [*burst-in-ms*] [**bc** *conform-burst-in-msec* **ms**] [**be** *peak-burst-in-msec* **ms**] [**pir percent** *percent*] **Example:** `Router(config-pmap-c)# police cir percent 20 bc 300 ms be 400 ms pir percent 40`	Configures traffic policing on the basis of the specified bandwidth percentage and optional burst sizes. Enters policy-map class police configuration mode. • Enter the bandwidth percentage and optional burst sizes.
Step 6	**exit** **Example:** `Router(config-pmap-c-police)# exit`	Exits policy-map class police configuration mode.

Attaching the Policy Map to an Interface for Percentage-Based Policing

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **pvc** [*name*] *vpi* / *vci* [**ilmi** | **qsaal** | **smds**]
5. **service-policy** {**input**| **output**} *policy-map-name*
6. **end**

DETAILED STEPS

	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	**interface** *type number* **Example:**	Configures an interface (or subinterface) type and enters interface configuration mode.

	Command or Action	Purpose
	`Router(config)#` `interface serial4/0/0`	• Enter the interface type number. **Note** Depending on the needs of your network, you may need to attach the policy map to a subinterface, an ATM PVC, a Frame Relay DLCI, or other type of interface.
Step 4	**pvc** [*name*] *vpi* / *vci* [**ilmi** | **qsaal** | **smds**] **Example:** `Router(config-if)# pvc cisco 0/16 ilmi`	(Optional) Creates or assigns a name to an ATM PVC and specifies the encapsulation type on an ATM PVC. Enters ATM VC configuration mode. **Note** This step is required only if you are attaching the policy map to an ATM PVC. If you are not attaching the policy map to an ATM PVC, skip this step and proceed with Step 5.

Step 5	**service-policy** {**input**| **output**} *policy-map-name*
	Example:
	`Router(config-if)#`
	`service-policy input policy1`
	Example:
		Specifies the name of the policy map to be attached to the input or output direction of the interface.
		Note Policy maps can be configured on ingress or egress routers. They can also be attached in the input or output direction of an interface. The direction (input or output) and the router (ingress or egress) to which the policy map should be attached varies according your network configuration. When using the **service-policy** command to attach the policy map to an interface, be sure to choose the router and the interface direction that are appropriate for your network configuration.
		• Enter the policy map name.

Step 6	**end** **Example:** `Router(config-if)# end`	(Optional) Exits interface configuration mode.

Verifying the Percentage-Based Policing Configuration

SUMMARY STEPS

1. **enable**
2. **show class-map** [*class-map-name*]
3. **show policy-map interface** *interface-name*
4. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show class-map** [*class-map-name*] **Example:** `Router# show class-map class1`	Displays all information about a class map, including the match criterion. • Enter class map name.

Step 3	**show policy-map interface** *interface-name*
	Example:
	`Router#`
	`show policy-map interface serial4/0/0`
		Displays the packet statistics of all classes that are configured for all service policies either on the specified interface or subinterface or on a specific PVC on the interface.
		• Enter the interface name.

Step 4	**exit** **Example:** `Router# exit`	(Optional) Exits privileged EXEC mode.

Troubleshooting Tips for Percentage-Based Policing

The commands in the Verifying the Percentage-Based Policing Configuration, on page 195 section allow you to verify that you achieved the intended configuration and that the feature is functioning correctly. If, after using the **show** commands listed above, you find that the configuration is not correct or the feature is not functioning as expected, perform these operations:

If the configuration is not the one you intended, complete the following procedures:

1. Use the **show running-config** command and analyze the output of the command.
2. If the policy map does not appear in the output of the **show running-config** command, enable the **logging console** command.
3. Attach the policy map to the interface again.

If the packets are not being matched correctly (for example, the packet counters are not incrementing correctly), complete the following procedures:

1. Run the **show policy-map**command and analyze the output of the command.
2. Run the **show running-config** command and analyze the output of the command.
3. Use the **show policy-map interface** command to verify that the policy map is attached to the interface and that the committed information rate (CIR) has been calculated on the basis of the percentage of the interface bandwidth.

Configuration Examples for QoS Percentage-Based Policing

Example Specifying Traffic Policing on the Basis of a Bandwidth Percentage

The following example configures traffic policing using a CIR and a peak information rate (PIR) on the basis of a percentage of bandwidth. In this example, a CIR of 20 percent and a PIR of 40 percent have been specified. Additionally, an optional bc value and be value (300 ms and 400 ms, respectively) have been specified.

```
Router> enable
Router# configure terminal
Router(config)# policy-map policy1
Router(config-pmap)# class class1
Router(config-pmap-c)# police cir percent 20 bc 300 ms be 400 ms pir percent 40

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

After the policy map and class maps are configured, the policy map is attached to interface as shown in the following example.

```
Router> enable
Router# configure terminal
Router(config-if)#

interface serial4/0/0
Router(config-if)#

service-policy input policy1
Router(config-if)# end
```

Example Verifying the Percentage-Based Policing Configuration

This section contains sample output from the **show policy-map interface** command and the **show policy-map** command. The output from these commands can be used to verify and monitor the feature configuration on your network.

The following is sample output from the **show policy-map** command. This sample output displays the contents of a policy map called "policy1." In policy 1, traffic policing on the basis of a CIR of 20 percent has been configured, and the bc and be have been specified in milliseconds. As part of the traffic policing configuration, optional conform, exceed, and violate actions have been specified.

```
Router# show policy-map policy1
  Policy Map policy1
    Class class1
     police cir percent 20 bc 300 ms pir percent 40 be 400 ms
       conform-action transmit
       exceed-action drop
       violate-action drop
```

The following is sample output from the **show policy-map interface** command. This sample displays the statistics for the serial 2/0 interface on which traffic policing has been enabled. The committed burst (bc) and excess burst (be) are specified in milliseconds (ms).

```
Router# show policy-map interface serial2/0
```

```
Serial2/0/0
 Service-policy output: policy1 (1050)
   Class-map: class1 (match-all) (1051/1)
     0 packets, 0 bytes
     5 minute offered rate 0 bps, drop rate 0 bps
     Match: ip precedence 0  (1052)
     police:
         cir 20 % bc 300 ms
         cir 409500 bps, bc 15360 bytes
         pir 40 % be 400 ms
         pir 819000 bps, be 40960 bytes
       conformed 0 packets, 0 bytes; actions:
         transmit
       exceeded 0 packets, 0 bytes; actions:
         drop
       violated 0 packets, 0 bytes; actions:
         drop
       conformed 0 bps, exceed 0 bps, violate 0 bps
   Class-map: class-default (match-any) (1054/0)
     0 packets, 0 bytes
     5 minute offered rate 0 bps, drop rate 0 bps
     Match: any  (1055)
       0 packets, 0 bytes
       5 minute rate 0 bps
```

In this example, the CIR and PIR are displayed in bps, and both the committed burst (bc) and excess burst (be) are displayed in bytes.

The CIR, PIR bc, and be are calculated on the basis of the formulas described below.

Formula for Calculating the CIR

When calculating the CIR, the following formula is used:

CIR percentage specified (as shown in the output of the **show policy-map**command) * bandwidth (BW) of the interface (as shown in the output of the **show interfaces** command) = total bits per second

On serial interface 2/0, the bandwidth (BW) is 2048 kbps. To see the bandwidth of the interface, use the **show interfaces** command. A sample is shown below:

```
Router# show interfaces serial2/0/0
Serial2/0/0 is administratively down, line protocol is down
  Hardware is M4T
  MTU 1500 bytes, BW 2048 Kbit, DLY 20000 usec, rely 255/255, load 1/255
```

The following values are used for calculating the CI:

20 % * 2048 kbps = 409600 bps

Formula for Calculating the PIR

When calculating the PIR, the following formula is used:

PIR percentage specified (as shown in the output of the **show policy-map**command) * bandwidth (BW) of the interface (as shown in the output of the **show interfaces** command) = total bits per second

On serial interface 2/0/0, the bandwidth (BW) is 2048 kbps. To see the bandwidth of the interface, use the **show interfaces** command. A sample is shown below:

```
Router# show interfaces serial2/0
Serial2/0/0 is administratively down, line protocol is down
```

```
Hardware is M4T
MTU 1500 bytes, BW 2048 Kbit, DLY 20000 usec, rely 255/255, load 1/255
```

The following values are used for calculating the PIR:

40 % * 2048 kbps = 819200 bps

Note Discrepancies between this total and the total shown in the output of the **show policy-map interface** command can be attributed to a rounding calculation or to differences associated with the specific interface configuration.

Formula for Calculating the Committed Burst (bc)

When calculating the bc, the following formula is used:

The bc in milliseconds (as shown in the **show policy-map** command) * the CIR in bits per seconds = total number bytes

The following values are used for calculating the bc:

(300 ms * 409600 bps) / 8 = 15360 bytes

Formula for Calculating the Excess Burst (be)

When calculating the bc and the be, the following formula is used:

The be in milliseconds (as shown in the **show policy-map** command) * the PIR in bits per seconds = total number bytes

The following values are used for calculating the be:

400 ms * 819200 bps = 40960 bytes

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 QoS Command-Line Interface (CLI) (MQC), including information about attaching policy maps	"Applying QoS Features Using the MQC" module
Traffic shaping and traffic policing	"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, Software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 2697	*A Single Rate Three Color Marker*
RFC 2698	*A Two Rate Three Color Marker*

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

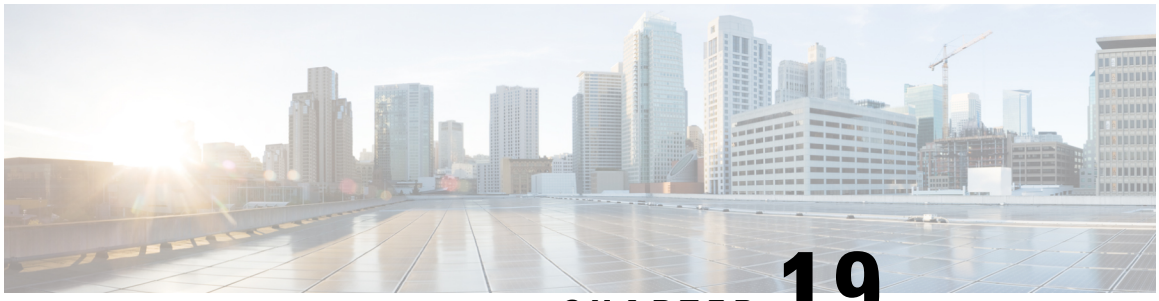
Feature Information for QoS Percentage-Based Policing

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

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

Table 20: Feature Information for QoS: Percentage-Based Policing

Feature Name	Releases	Feature Information
QoS: Percentage-Based Policing	Cisco IOS XE Release 2.1	The QoS: Percentage-Based Policing feature allows you to configure traffic policing and traffic shaping on the basis of a percentage of bandwidth available on the interface. This feature also allows you to specify the committed burst (bc) size and the excess burst (be) size (used for configuring traffic policing) in milliseconds (ms). Configuring traffic policing in this manner enables you to use the same policy map for multiple interfaces with differing amounts of bandwidth. This feature was introduced on Cisco ASR 1000 Series Routers. The following commands were introduced or modified: **police (percent)**, **shape (percent)**, **show policy-map**, **show policy-map interface**.



CHAPTER 19

Two-Rate Policer

This module describes the Two-Rate Policer feature and explains how to configure it.

History for the Two-Rate Policer Feature

Release	Modification
Cisco IOS XE Release 2.1	This feature was implemented on Cisco ASR 1000 Series Routers.

Finding Support Information for Cisco IOS XE Software Images

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

Finding Feature Information

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

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

Feature Overview

When configured, an ATM switch at the network side of a user-to-network (UNI) interface polices the flow of cells in the forward (into the network) direction of a virtual connection. These traffic policing mechanisms are known as usage parameter control (UPC). With UPC, the switch determines whether received cells comply with the negotiated traffic management values and takes one of the following actions on violating cells:

- Pass the cell without changing the cell loss priority (CLP) bit in the cell header.
- Tag the cell with a CLP bit value of 1.
- Drop (discard) the cell.

The SVC/SoftPVC feature enables you to specify which traffic to police, based on service category, on switched virtual circuits (SVCs) or terminating VCs on the destination end of a soft VC.

Benefits

Bandwidth Management Through Rate Limiting

Traffic policing allows you to control the maximum rate of traffic transmitted or received on an interface. Traffic policing is often configured on interfaces at the edge of a network to limit traffic into or out of the network. In most Traffic 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 traffic 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 traffic 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 Traffic Policing feature. If you want to mark traffic but do not want to use Traffic Policing, see the "Marking Network Traffic" module.

Packet Prioritization for Frame Relay Frames

The Traffic 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 Traffic 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 for Two-Rate Policing

The following restrictions apply to the Two-Rate Policer:

- Two-rate policing can be configured on an interface, a subinterface, a Frame Relay data-link connection identifier (DLCI), and an ATM permanent virtual circuit (PVC).
- Two-rate policing is not supported on EtherChannel or tunnel interfaces.

Prerequisites for Two-Rate Traffic Policing

To configure the Two-Rate Policer, a traffic class and a service policy must be created, and the service policy must be attached to a specified interface.

Configuration Tasks

See the following sections for configuration tasks for the Two-Rate Policer feature.

Configuring the Two-Rate Policer

Command	Purpose
Router(config-pmap-c)# **police cir** *cir* [**bc***conform-burst*] **pir** *pir* [**be***peak-burst*] [**conform-action** *action* [**exceed-action** *action* [**violate-action** *action*]]]	Specifies that both the CIR and the PIR are to be used for two-rate traffic policing, and specifies multiple actions applied to packets marked as conforming to, exceeding, or violating a specific rate. Use one line per action that you want to specify. Enters policy-map class police configuration mode. The **bc** and **be** keywords and their associated arguments (*conform-burst* and *peak-burst* , respectively) are optional.

Although not required for configuring the Two-Rate Policer, the command syntax of the **police** command also allows you to specify the action to be taken on a packet when you enable an optional *action* argument. The resulting action corresponding to the keyword choices are listed in Table 1 .

Table 21: police Command Action Keywords

Keyword	Resulting Action
drop	Drops the packet.
set-clp-transmit	Sets the ATM CLP bit from 0 to 1 on the ATM cell and sends the packet with the ATM CLP bit set to 1.
set-dscp-transmit *new-dscp*	Sets the IP DSCP value and sends the packet with the new IP DSCP value setting.
set-frde-transmit	Sets the Frame Relay DE bit from 0 to 1 on the Frame Relay frame and sends the packet with the DE bit set to 1.
set-mpls-exp-transmit	Sets the MPLS experimental bits from 0 to 7 and sends the packet with the new MPLS experimental bit value setting.
set-prec-transmit *new-prec*	Sets the IP precedence and sends the packet with the new IP precedence value setting.
set-qos-transmit *new-qos*	Sets the QoS group value and sends the packet with the new QoS group value setting.
transmit	Sends the packet with no alteration.

Verifying the Two-Rate Policer Configuration

Command	Purpose
`Router#` **`show policy-map interface`**	Displays statistics and configurations of all input and output policies attached to an interface.

Troubleshooting Tips

Monitoring and Maintaining the Two-Rate Policer

Command	Purpose
`Router#` **`show policy-map`**	Displays all configured policy maps.
`Router#` **`show policy-map`** *`policy-map-name`*	Displays the user-specified policy map.

Command	Purpose
Router# **show policy-map interface**	Displays statistics and configurations of all input and output policies that are attached to an interface.

Configuration Examples

Example Limiting the Traffic Using a Policer Class

In this example, the Two-Rate Policer is configured on a class to limit traffic to an average committed rate of 500 kbps and a peak rate of 1 Mbps.

```
Router(config)# class-map police
Router(config-cmap)# match access-group 101
Router(config-cmap)# policy-map policy1
Router(config-pmap)# class police
Router(config-pmap-c)# police cir 500000 bc 10000 pir 1000000 be 10000 conform-action
 transmit exceed-action set-prec-transmit 2 violate-action drop
Router(config)# interface serial3/0/0
Router(config-if)# service-policy output policy1
Router(config-if)# end
Router# show policy-map policy1
 Policy Map policy1
  Class police
   police cir 500000 conform-burst 10000 pir 1000000 peak-burst 10000 conform-action transmit
 exceed-action set-prec-transmit 2 violate-action drop
```

Traffic marked as conforming to the average committed rate (500 kbps) will be sent as is. Traffic marked as exceeding 500 kbps, but not exceeding 1 Mbps, will be marked with IP Precedence 2 and then sent. All traffic exceeding 1 Mbps will be dropped. The burst parameters are set to 10,000 bytes.

In the following example, 1.25 Mbps of traffic is sent ("offered") to a *policer* class.

```
Router# show policy-map interface serial3/0/0
 Serial3/0/0
  Service-policy output: policy1
   Class-map: police (match all)
    148803 packets, 36605538 bytes
    30 second offered rate 1249000 bps, drop rate 249000 bps
    Match: access-group 101
    police:
     cir 500000 bps, conform-burst 10000, pir 1000000, peak-burst 100000
     conformed 59538 packets, 14646348 bytes; action: transmit
     exceeded 59538 packets, 14646348 bytes; action: set-prec-transmit 2
     violated 29731 packets, 7313826 bytes; action: drop
     conformed 499000 bps, exceed 500000 bps violate 249000 bps
   Class-map: class-default (match-any)
    19 packets, 1990 bytes
    30 seconds offered rate 0 bps, drop rate 0 bps
    Match: any
```

The Two-Rate Policer marks 500 kbps of traffic as conforming, 500 kbps of traffic as exceeding, and 250 kbps of traffic as violating the specified rate. Packets marked as conforming will be sent as is, and packets

marked as exceeding will be marked with IP Precedence 2 and then sent. Packets marked as violating the specified rate are dropped.

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*
Token bucket mechanisms	"Policing and Shaping Overview" module
MQC	"Applying QoS Features Using the MQC" module
QoS features such traffic marking, and traffic policing	• "Marking Network Traffic" module • "Traffic Policing" module

Standards

Standard	Title
None	--

MIBs

MIB	MIBs Link
• CISCO-CLASS-BASED-QOS-MIB • CISCO-CLASS-BASED-QOS-CAPABILITY-MIB	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
RFC 2698	*A Two Rate Three Color Marker*

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

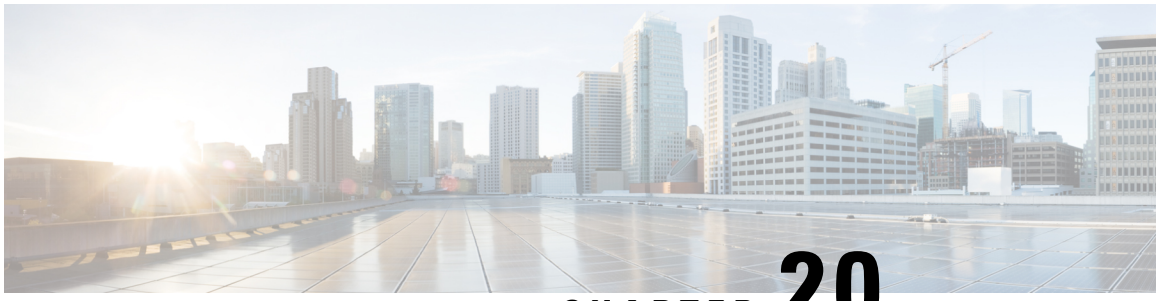
Feature Information for Two-Rate Policer

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

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

Table 22: Feature Information for Two-Rate Policer

Feature Name	Releases	Feature Information
Two-Rate Policer	12.2(4)T 12.2(4)T3 12.0(26)S 12.2(28)SB 12.2(33)SRA 12.2(33)SXH Cisco IOS XE Release 2.1 Cisco IOS XE 3.1.0 SG	This feature was introduced. Support for the Cisco 7500 series routers was added. This feature was integrated into Cisco IOS Release 12.0(26)S for the Cisco 7200 and 7500 series routers. This feature was integrated into Cisco IOS Release 12.2(28)SB. This feature was integrated into Cisco IOS Release 12.2(33)SRA. This feature was integrated into Cisco IOS Release 12.2(33)SXH. This feature was implemented on Cisco ASR 1000 Series Routers. This feature was integrated into Cisco IOS XE 3.1.0 SG.



CHAPTER 20

Punt Policing and Monitoring

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

Finding Feature Information

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

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

Information About Punt Policing and Monitoring

Overview of Punt Policing and Monitoring

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

Punt policing frees the RP from having to process noncritical traffic. Traffic is placed in queues based on various criteria, and you can configure the maximum punt rate for each queue which allows you to configure the system so that packets are less likely to be dropped from queues that contain critical traffic.

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.

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.

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:**	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Device# configure terminal	Enters global configuration mode.
Step 3	**platform qos-policer queue** *queue-id cir* **Example:** Device(config)# platform punt-police queue 20 9000 10000	Enables punt policing on a queue, and specifies the maximum punt rate on a per-queue basis.
Step 4	**end** **Example:** Device(config)# end	(Optional) Returns to privileged EXEC mode.

Configuring Punt Policing on an Interface

Note At an interface level, punt control can be enabled or disabled by the **no punt-control enable** command. You can configure the rate, however, by default, it uses the global configuration if the rate is not configured.

Perform this task to enable or disable punt control on an interface:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **platform punt-interface rate***rate*
4. **punt-control enable** *rate*
5. **end**

DETAILED STEPS

	Command or Action	Purpose
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	**platform punt-interface rate***rate* **Example:** Device(config)# platform punt-interface rate 10	Sets the global punt-interface policer rate.
Step 4	**punt-control enable** *rate* **Example:** Device(config)# interface Port-channel 1.2 Device(config-if)# punt-control enable	Punt control is enabled at an interface level.
Step 5	**end** **Example:**	(Optional) Returns to privileged EXEC mode.

How to Configure Punt Policing and Monitoring

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
```

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
```

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

```
*Jun 6 08:25:35.893: %IOSXE-5-PLATFORM: F0: cpp_cp: QFP:0.0
Thread:046 TS:00000000400859588264 %PUNT_INJECT-5-DROP_PUNT_INTF:
punt interface policer drop packet from GigabitEthernet2/3/1.726
```

Configuration Examples for Punt Policing and Monitoring

Example: Configuring Punt Policing

The following example shows how to enable punt-policing:

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

Additional References

Related Documents

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

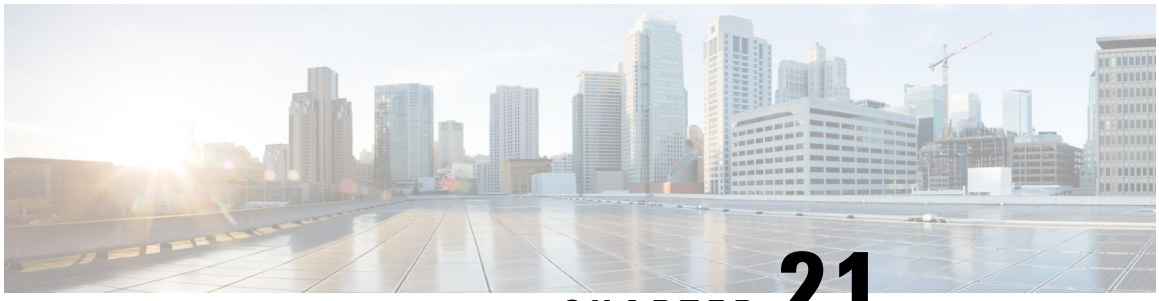
Feature Information for Punt Policing and Monitoring

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

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

Table 23: Feature Information for Punt Policing and Monitoring

Feature Name	Releases	Feature Information
Punt Policing and Monitoring	Cisco IOS XE Release 3.5S	The Punt Policing and Monitoring feature allows you to specify a maximum punt rate on a per-queue basis. For Cisco IOS XE Release 3.5S, this feature was implemented on Cisco ASR 903 Router. The following command was introduced: **platform punt-police queue**



CHAPTER 21

Port-Shaper and LLQ in the Presence of EFPs

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

Finding Feature Information

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

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

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

- If you configure a class-based policy on the port, then you cannot configure service-policies on Ethernet Flow Points (EFPs).
- Attaching a service policy to the BDI is not supported.
- ACL based shaping policy-map cannot be applied to the EFP and/or egress interface.
- Usage of bandwidth remaining percentage (BRP) in the absence of priority class, allocates the available bandwidth in an iterative way. For example, the bandwidth is allocated for the first BRP class as per the percentage of share configured in the respective class-map and the remaining bandwidth is iteratively allocated to all other BRP classes until the bandwidth is exhausted.
- You must remove bandwidth statement from the child policy before it is removed from the child policy.

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.

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

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:

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:

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:

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.

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

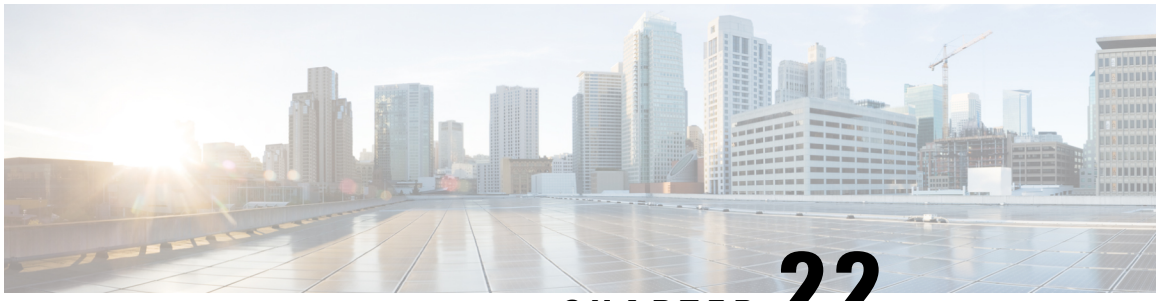
Feature Information for Port-Shaper and LLQ in the Presence of EFPs

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

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

Table 24: Feature Information for Port-Shaper and LLQ in the Presence of EFPs

Feature Name	Releases	Feature Information
Port-Shaper and LLQ in the Presence of EFPs	Cisco IOS Release XE 3.6S	The Port-Shaper and LLQ in the Presence of EFPs feature provides support for LLQ and traffic prioritization across all EFPs on a port. In Cisco IOS XE Release 3.6S, support was added for the Cisco ASR 903 router.



CHAPTER 22

Adaptive QoS over DMVPN

Adaptive QoS over Dynamic Multipoint VPN (DMVPN) ensures effective bandwidth management using dynamic shapers based on available bandwidth. This feature enables various QoS features to adapt to non service-level agreement (SLA) based environments where bandwidth is variable and fluctuate with time.

Finding Feature Information

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

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

Prerequisites for Adaptive QoS over DMVPN

Adaptive QoS over DMVPN can be enabled either on hub or spoke or both. To enable feature at a spoke side, the spoke must support basic egress per-SA QoS policy.

Internet Protocol Security (IPSec) is required and must be configured before Adaptive QoS is enabled on the DMVPN tunnel.

Restrictions for Adaptive QoS over DMVPN

The Adaptive QoS over DMVPN feature configuration is:

- Supported only on DMVPN tunnels
- Allowed only on egress direction
- Allowed only in parent most policy that has class-default only
- Not supported on Point-to-Point tunnels
- Adaptive QOS is not supported on Cisco IWAN 2.1

Information About Adaptive QoS over DMVPN

Overview of Adaptive QoS over DMVPN

Enterprise networks are increasingly using the Internet as form of WAN transport, therefore QoS models needs to be revisited. QoS works effectively when deployed in an service-level agreement (SLA) environment today, like Multiprotocol Label Switching (MPLS) . The available bandwidth on the internet at a given point of time can vary, and can be often much lesser than the actual bandwidth offered by the service provider. In cases of non SLA environments, QoS has limitations - mainly because it cannot predict changing bandwidth on the link.

Cisco Intelligent WAN (IWAN) recommends using Dynamic Multipoint VPN (DMVPN) over Internet to connect branches to the data center or headquarters, and QoS to be deployed in such environments of fluctuating bandwidth. Currently, the shapers that are applied as part of the egress QoS policy are static in value - they are configured based on the service provider bandwidth offering, they do not change with time and hence do not reflect the actual available Internet bandwidth. In many instances where Internet available bandwidth becomes much lesser than the offered bandwidth, the shapers become irrelevant as they do not adapt to the varying bandwidth. Due to the static value of the shapers, application traffic gets dropped indiscriminately at the Internet core, nullifying the very need to have configured a QoS policy to protect critical traffic.

DMVPN provides the ability to do QoS per-tunnel, which means a QoS policy can be applied at the hub towards a specific spoke, to ensure a high bandwidth hub does not overrun a low capacity spoke. However, these QoS policies still work with static shapers per spoke. If the bandwidth towards a particular spoke fluctuates, the shapers towards the spokes do not adapt. Also, it is not possible today to configure a QoS policy for the traffic from the spoke towards the hub, which is very common in many retail-like environments.

The Adaptive QoS over DMVPN feature provides the following benefits:

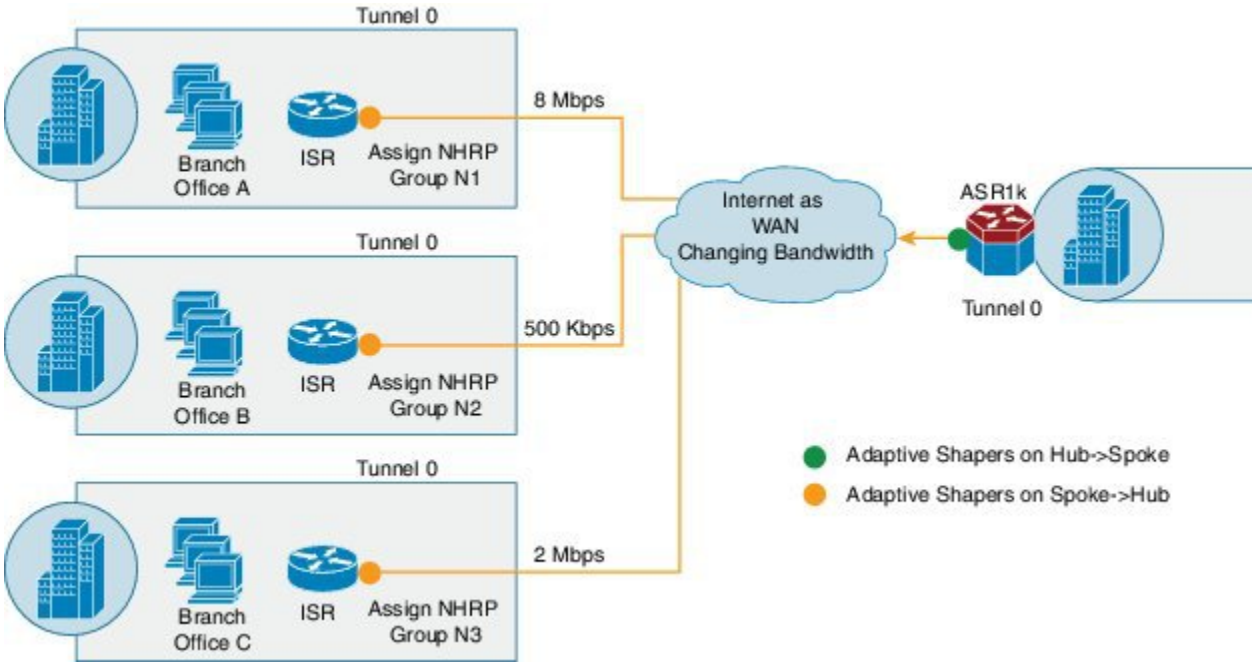
- Adjusts the shaper parameters based on the actual available Internet bandwidth in both directions that is periodically computed.
- Allows to configure a QoS policy on the spoke towards the hub.
- Ensures better control of application performance at the enterprise edge even in changing bandwidth scenarios over the Internet.
- Allows aggregate tunnel shape adaptation to provide effective bandwidth between spoke and hub.

Adaptive QoS for Per-Tunnel QoS over DMVPN

Per-tunnel QoS over DMVPN can be configured on the hub towards the spoke today using Next Hop Resolution Protocol (NHRP) groups. The QoS policies contain static shapers. With Adaptive QoS, the framework of per tunnel QoS configuration remains the same, but the shaper can be an adaptive one as shown in the following

figure. These shapers would adapt automatically based on the changing Internet bandwidth that is periodically computed using an algorithm.

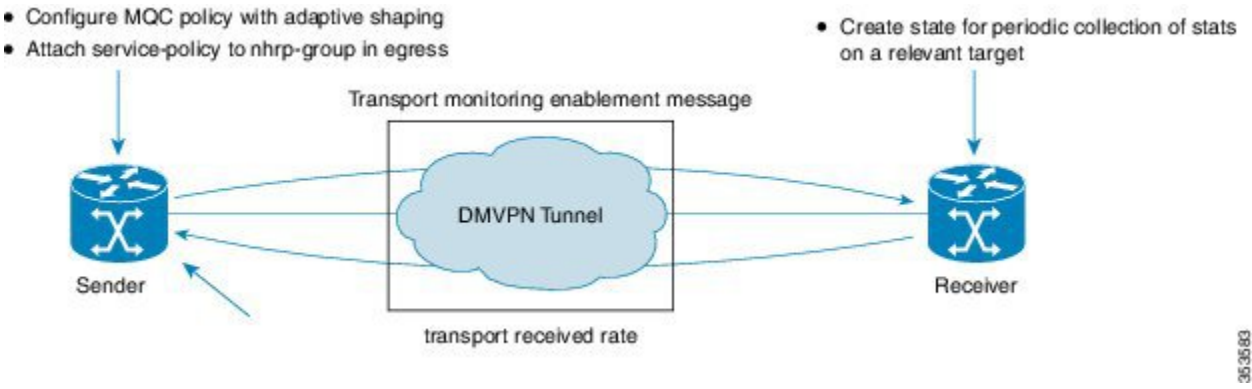
Figure 5: Adaptive QoS for Per-Tunnel QoS over DMVPN



Workflow of Adaptive QoS

The Adaptive QoS over DMVPN feature adapts shaping rate at the Sender based on the available bandwidth between specific Sender and Receiver (two end-points of a DMVPN tunnel).

Figure 6: Workflow of Adaptive QoS



At the Sender:

- Configure MQC Policy with Adaptive shaping
- Attach service-policy to nhrp-group in Egress

At the Receiver:

Create state for periodic collection of stats on a relevant target

How to Configure Adaptive QoS over DMVPN

Note Configure the Per-Tunnel QoS for DMVPN before configuring the Adaptive QoS over DMVPN feature, as Adaptive QoS over DMVPN feature is an enhancement to the Per-Tunnel QoS for DMVPN feature.

Note For details on configuring the Per-Tunnel QoS for DMVPN feature, refer to Per-Tunnel QoS for DMVPN .

Configuring Adaptive QoS for DMVPN

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map** *parent-policy-name*
4. **class class-default**
5. **shape adaptive** { **upper-bound** *bps* |**percent** *percentage* }[**lower-bound** *bps*| **percent** *percentage*]
6. **end**
7. **configure terminal**
8. **interface tunnel** *tunnel-id*
9. **nhrp map group** *group-name* **service-policy output** *parent-policy-name*
10. **end**

DETAILED STEPS

	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** *parent-policy-name* **Example:** `Router(config)# policy-map example`	Creates or modifies a child policy map and enters policy-map configuration mode. • Enter the name of the child policy map.

	Command or Action	Purpose
Step 4	**class class-default** **Example:** `Router(config-pmap)# class class-default`	This step associates the traffic class with the traffic policy. Configures the default class map and enters policy-map class configuration mode.
Step 5	**shape adaptive** { **upper-bound** *bps* |**percent** *percentage* }[**lower-bound** *bps*| **percent** *percentage*] **Example:** `Router(config-pmap-c)# shape adaptive upper-bound 20000`	Creates a specific adaptive shaper that has upper bound on the rate and optionally lower bound on the rate. **Note** When such a template is attached to a target, adaptive shaping is enabled for that instance. Shaping rate adapts to a new rate, that is a function of parameters, including peer's received rate.
Step 6	**end** **Example:** `Router(config-pmap-c)# end`	Returns to privileged EXEC mode.
Step 7	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 8	**interface tunnel** *tunnel-id* **Example:** `Router(config)# interface tunnel 0`	Configures an interface type and enters interface configuration mode. • Enter the interface type and interface number.
Step 9	**nhrp map group** *group-name* **service-policy output** *parent-policy-name* **Example:** `Router(config-if)# nhrp map group 1 service-policy output example`	Adds the NHRP group to the QoS policy map on the hub.
Step 10	**end** **Example:** `Router(config-if)# end`	Returns to privileged EXEC mode.

Verifying the Adaptive QoS over DMVPN

SUMMARY STEPS

1. **enable**
2. **show dmvpn**

3. **show policy-map** [*policy-map-name*]
4. **show policy-map multipoint**
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables higher privilege levels, such as privileged EXEC mode. • Enter your password if prompted.
Step 2	**show dmvpn** **Example:** `Router# show dmvpn`	Displays detailed DMVPN information for each session, including the Next Hop Server (NHS) and NHS status, crypto session information, and socket details. Also displays the NHRP group received from the spoke and the QoS policy applied to the spoke tunnel.
Step 3	**show policy-map** [*policy-map-name*] **Example:** `Router# show policy-map example`	Displays the configuration of all classes for a specified policy map or of all classes for all existing policy maps.
Step 4	**show policy-map multipoint** **Example:** `Router# show policy-map tunnel 0`	(Optional) Displays the statistics and the configurations of the input and output policies that are attached to an interface.
Step 5	**exit** **Example:** `Router(config-if)# exit`	(Optional) Returns to user EXEC mode.

Troubleshooting the Adaptive QoS over DMVPN

SUMMARY STEPS

1. **enable**
2. **debug qos peer mon detail**
3. **debug qos peer rate detail**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables higher privilege levels, such as privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**debug qos peer mon detail** **Example:** `Router# debug qos peer mon detail`	Displays debug messages for Adaptive QoS over DMVPN.
Step 3	**debug qos peer rate detail** **Example:** `Router# debug qos peer rate detail`	Displays debug messages for Adaptive QoS over DMVPN.

Configuration Examples for Configuring Adaptive QoS over DMVPN

Example Configuring Adaptive QoS over DMVPN

The following example shows how to configure Adaptive QoS over DMVPN:

```
Router(config)# policy-map example
Router(config-pmap)# class class-default
Router(config-pmap-c)# shape adaptive upper-bound 20000
Router(config-pmap-c)# end
Router# configure terminal
Router(config)# interface tunnel 0
Router(config-if)# nhrp map group 1 service-policy output example
Router(config-if)# end
```

Example Verifying Adaptive QoS over DMVPN

The **show policy-map** and **show policy-map interface** commands can be used to confirm that the Adaptive QoS over DMVPN feature is enabled at an interface.

The following is a sample output of the **show dmvpn** command:

```
Router# show dmvpn


Interface: Tunnel1, IPv4 NHRP Details
Type: Hub, NHRP Peers:1,

# Ent  Peer NBMA Addr   Peer Tunnel Add   State UpDn Tm    Attrb
 ----- ------------- -----------------     ----- -------   -----
  1    10.1.1.1          10.10.1.2        UP    00:18:37   D


Interface: Tunnel2, IPv4 NHRP Details
Type: Hub, NHRP Peers:1,
```

```
# Ent Peer NBMA Addr   Peer Tunnel Add   State  UpDn Tm  Attrb
----- ---------------  --------------    ------  -------  -------

  1  10.2.1.1          10.10.2.2        UP     00:22:09  D


Interface: Tunnel3, IPv4 NHRP Details
Type: Hub, NHRP Peers:1,

# Ent Peer NBMA Addr   Peer Tunnel Add   State  UpDn Tm  Attrb
----- --------------   ---------------   ------ -------   ----
   1  10.3.1.1         10.10.3.2         UP     00:22:04   D


Interface: Tunnel4, IPv4 NHRP Details
Type: Hub, NHRP Peers:1,

# Ent Peer NBMA Addr   Peer Tunnel Add   State UpDn Tm  Attrb
----- --------------   ----------------  -----  ------  ----
  1    10.3.1.1        10.10.3.2         UP   00:22:01   D
```

The following is a sample output of the **show policy-map** command:

```
Router# show policy-map


Policy Map test
    Class class-default
      Adaptive Rate Traffic Shaping
      cir upper-bound 2120000 (bps) cir lower-bound 1120000 (bps)
```

The following is a sample output of the **show policy-map multipoint** command:

```
Router# show policy-map multipoint

 Service-policy output: test

  Class-map: class-default (match-any)
   0 packets, 0 bytes
   5 minute offered rate 0000 bps, drop rate 0000 bps
   Match: any
   Queueing
   queue limit 64 packets
   (queue depth/total drops/no-buffer drops)0/0/0
   (pkts output/bytes output) 0/0
   shape (adaptive) cir 2120000,bc 8480, be 8480
   lower bound cir 2120000
   target shape rate 2120000
```

Note One of the important parameters displayed as an output of the **show policy-map multipoint** command is **target shape rate**. The Adaptive QoS over DMVPN feature dynamically changes the value of the **target shape rate** to adapt to the available bandwidth.

Example for Troubleshooting Adaptive QoS over DMVPN

The **debug qos peer mon detail** and **debug qos peer rate detail** commands can be used to display any errors for the Adaptive QoS over DMVPN feature.

The following is a sample output of the **debug qos peer mon detail** command:

```
Router# debug qos peer mon detail

QoS peer remote monitoring debugging is on

Router#

*May 22 21:25:28.006 UTC: [SEND]Processing entry with address :
50.1.1.2,vrfid : 0 sending rate(delta bytes) : 1514
*May 22 21:25:28.006 UTC: [SEND]Processing entry with address :
50.1.1.3,vrfid : 0 sending rate(delta bytes) : 1598
*May 22 21:25:28.201 UTC: [RCV]Received message for interface Tunnel1
address 50.1.1.2 vrf 0
*May 22 21:25:28.201 UTC:
fdiff : 20517, sdiff : 19661, cur_dif : 3318, cum_diff : 20907

*May 22 21:25:28.201 UTC: qos_rate_status_update -- 392
*May 22 21:25:28.201 UTC: Last count : 128650
```

The following is a sample output of the **debug qos peer rate detail** command:

```
Router# debug qos peer rate detail


 *May 22 21:34:32.456 UTC: [RCV]Received message for interface Tunnel1
address 50.1.1.3 vrf 0
 *May 22 21:34:32.456 UTC: Enter qos_process_remote_rate_message:
 *May 22 21:34:32.456 UTC: Message for tun with o_ip : 50.1.1.3 tun t_ip
 : 13.1.1.1
 *May 22 21:34:32.456 UTC: [RCV]<DELTA>Message remote rate value is
116730f_cum_diff: 140155, s_cum_diff: 135612
 HoldTh: 5000, CurTh: 11250
 Gonna Go Up f_cum_diff: 140155, s_cum_diff: 135612
 Yes increasing
 Suggested rate: 120000

 *May 22 21:34:32.456 UTC: rx_bytes = 116730, tx_bytes = 125282, Suggested
 rate = 120000
```

```
*May 22 21:34:32.456 UTC: Exiting : 1
```

Additional References

The following sections provide references related to the Control Plane Logging feature.

Related Documents

Related Topic	Document Title
NHRP MIB	Dynamic Multipoint VPN Configuration Guide
QoS commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	Cisco IOS Quality of Service Solutions Command Reference
QoS feature overview	Quality of Service Overview module
Per-Tunnel QoS for DMVPN	Dynamic Multipoint VPN Configuration Guide

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
CISCO-CLASS-BASED-QOS-MIB CISCO-NHRP-MIB	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

RFCs

RFC	Title
None	—

Technical Assistance

Description	Link
The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Feature Information for Adaptive QoS over DMVPN

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

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

Table 25: Feature Information for Adaptive QoS over DMVPN

Feature Name	Releases	Feature Information
Adaptive QoS over DMVPN	Cisco IOS XE 3.14S	Adaptive QoS over Dynamic Multipoint VPN (DMVPN) ensures effective bandwidth management using dynamic shapers based on available bandwidth. This feature enables various QoS features to adapt to non service-level agreement (SLA) based environments where bandwidth is variable and fluctuate with time. The following commands were introduced or modified: **shape adaptive**, **show policy-map**, and **show policy-map interface**.