



QoS: Policing and Shaping Configuration Guide, Cisco IOS Release 12.4

Americas Headquarters

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

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

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

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

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

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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

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

© 2011 Cisco Systems, Inc. All rights reserved.



CONTENTS

Policing and Shaping Overview	1
Finding Feature Information	1
What Is a Token Bucket	2
Policing with CAR	3
How CAR Works	3
Matching Criteria	3
Rate Limits	4
What Rate Limits Define	4
Extended Burst Value	4
How Extended Burst Capability Works	5
Recommended Burst Values	5
Actual and Compounded Debt Example	5
Conform and Exceed Actions	6
Multiple Rate Policies	6
Restrictions of CAR and VIP-Distributed CAR	7
Traffic Policing	7
Benefits of Traffic Policing	8
Restrictions for Traffic Policing	8
Prerequisites for Traffic Policing	9
Traffic Shaping to Regulate Packet Flow	9
Configuring Traffic Policing	11
Finding Feature Information	11
Feature Overview	11
Benefits	12
Restrictions	13
Supported Platforms	13
Supported Standards MIBs and RFCs	14
Prerequisites	14
Configuration Tasks	14

Configuring Traffic Policing	15
Troubleshooting Tips	15
Monitoring and Maintaining Traffic Policing	15
Configuration Examples	15
Example Configuring a Service Policy that Includes Traffic Policing	16
Two-Rate Policer	17
Finding Feature Information	17
Prerequisites for Two-Rate Policer	17
Restrictions for Two-Rate Policer	18
Information About Two-Rate Policer	18
Benefits	19
How to Use the Two-Rate Policer	20
Configuring the Two-Rate Policer	20
Verifying the Two-Rate Policer Configuration	21
Troubleshooting Tips	21
Monitoring and Maintaining the Two-Rate Policer	21
Configuration Examples	21
Example Limiting the Traffic Using a Policer Class	21
Additional References	22
Feature Information for Two-Rate Policer	23
Policer Enhancement - Multiple Actions	25
Finding Feature Information	25
Feature Overview	25
Benefits	26
Restrictions	26
Related Features and Technologies	26
Related Documents	26
Supported Platforms	27
Supported Standards MIBs and RFCs	27
Prerequisites	28
Configuration Tasks	28
Configuring Multiple Policer Actions	28
Verifying the Multiple Policer Actions Configuration	28
Troubleshooting Tips	29
Monitoring and Maintaining the Multiple Policer Actions	29

Configuration Examples	29
Example Multiple Actions in a Two-Rate Policer	29
Example Verifying the Multiple Policer Actions	30
Percentage-Based Policing and Shaping	31
Finding Feature Information	31
Feature Overview	31
Benefits	32
Restrictions	32
Related Features and Technologies	32
Related Documents	32
Supported Standards MIBs and RFCs	33
Prerequisites	33
Configuration Tasks	34
Configuring Policing and Shaping Based on Bandwidth Percentage	34
Attaching the Policy Map to an Interface or a VC	35
Verifying the Policing and Shaping Bandwidth Percentage Setting	35
Troubleshooting Tips	35
Configuration Examples	35
Example Specifying Traffic Policing Based on a Bandwidth Percentage	35
Example Specifying Traffic Shaping Based on a Bandwidth Percentage	36
Example Verifying That CEF Is Enabled	36
Modular QoS CLI Three-Level Hierarchical Policer	39
Finding Feature Information	39
Restrictions for the Modular QoS CLI Three-Level Hierarchical Policer	40
Information About the Modular QoS CLI Three-Level Hierarchical Policer	41
Modular Quality of Service Command-Line Interface	41
Packet Flow in the Modular QoS CLI Three-Level Hierarchical Policer	42
Other Traffic Policing-Related Features	42
How to Configure the Modular QoS CLI Three-Level Hierarchical Policer	43
Configuring Traffic Policing	43
Attaching the Policy Map to an Interface	44
What to Do Next	46
Verifying the Configuration	46
Troubleshooting Tips	47
Configuration Examples for the Modular QoS CLI Three-Level Hierarchical Policer	48

Example Configuring the Modular QoS CLI Three-Level Hierarchical Policer	48
Additional References	50
ATM Policing by Service Category for SVC and SoftPVC	53
Finding Feature Information	53
Feature Overview	53
Benefits	54
Related Features and Technologies	54
Related Documents	54
Supported Platforms	54
Supported Standards MIBs and RFCs	54
Configuration Tasks	55
Configuring ATM Policing by Service Category for SVC and SoftPVC	55
Verifying ATM Policing by Service Category for SVC and SoftPVC	55
Troubleshooting Tips	56
Monitoring and Maintaining ATM Policing by Service Category for SVC and SoftPVC	57
Example Monitoring and Maintaining ATM Policing by Service Category for SVC and SoftPVC	57
Configuration Examples	58
Example Non-UBR Traffic Policing	58
Modular QoS CLI Unconditional Packet Discard	59
Finding Feature Information	59
Feature Overview	59
Benefits	60
Restrictions	60
Related Features and Technologies	60
Related Documents	60
Supported Standards MIBs and RFCs	60
Configuration Tasks	61
Configuring the Class Map	61
Creating a Policy Map	62
Attaching the Policy Map to an Interface or a VC	63
Verifying the Discard Action Configuration in the Traffic Class	64
Configuration Examples	64
Example Configuring the Discard Action Configuration in a Traffic Class	64
Example Verifying the Discard Action Configuration in the Policy Map	64
Control Plane Policing	67

Finding Feature Information	67
Prerequisites for Control Plane Policing	67
Restrictions for Control Plane Policing	67
Information About Control Plane Policing	69
Benefits of Control Plane Policing	69
Terms to Understand	70
Control Plane Security and Packet QoS Overview	71
Aggregate Control Plane Services	72
Distributed Control Plane Services	73
Usage of Distributed CP Services	74
Output Rate-Limiting and Silent Mode Operation	75
How to Use Control Plane Policing	75
Defining Aggregate Control Plane Services	75
Defining Distributed Control Plane Services	77
Verifying Aggregate Control Plane Services	78
Verifying Distributed Control Plane Services	79
Configuration Examples for Control Plane Policing	81
Example Configuring Control Plane Policing on Input Telnet Traffic	81
Example Configuring Control Plane Policing on Output ICMP Traffic	81
Additional References	82
Feature Information for Control Plane Policing	83



Policing and Shaping Overview

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

The rate-limiting features of committed access rate (CAR) and the Traffic Policing feature provide the functionality for policing traffic. The features of Generic Traffic Shaping (GTS), Class-Based Traffic Shaping, Distributed Traffic Shaping (DTS), and Frame Relay Traffic Shaping (FRTS) provide the functionality for shaping traffic.

You can deploy these features 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. (For example, the CAR rate-limiting 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, GTS and Class-Based Shaping use a weighted fair queue to delay packets in order to shape the flow, and DTS and FRTS use either a priority queue, a custom queue, or a FIFO queue for the same, depending on how you configure it.)

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

- [Finding Feature Information, page 1](#)
- [What Is a Token Bucket, page 2](#)
- [Policing with CAR, page 3](#)
- [Traffic Policing, page 7](#)
- [Traffic Shaping to Regulate Packet Flow, page 9](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see 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 document.

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.

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:

$$\text{mean rate} = \text{burst size} / \text{time interval}$$

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:

$$(\text{token bucket capacity in bits} / \text{time interval in seconds}) + \text{established rate in bps} = \text{maximum flow speed in bps}$$

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.

Policing with CAR

Committed access rate (CAR) embodies a rate-limiting feature for policing traffic, in addition to its packet classification feature discussed in the "Classification Overview" module. The rate-limiting feature of CAR manages the access bandwidth policy for a network by ensuring that traffic falling within specified rate parameters is sent, while dropping packets that exceed the acceptable amount of traffic or sending them with a different priority. The exceed action for CAR is to drop or mark down packets.

The rate-limiting function of CAR does the following:

- Allows you to control the maximum rate of traffic sent or received on an interface.
- Gives you the ability to define Layer 3 aggregate or granular incoming or outgoing (ingress or egress) bandwidth rate limits and to specify traffic handling policies when the traffic either conforms to or exceeds the specified rate limits.

Aggregate bandwidth rate limits match all of the packets on an interface or subinterface. Granular bandwidth rate limits match a particular type of traffic based on precedence, MAC address, or other parameters.

CAR is often configured on interfaces at the edge of a network to limit traffic into or out of the network.

- [How CAR Works, page 3](#)
- [Restrictions of CAR and VIP-Distributed CAR, page 7](#)

How CAR Works

CAR examines traffic received on an interface or a subset of that traffic selected by access list criteria. It then compares the rate of the traffic to a configured token bucket and takes action based on the result. For example, CAR will drop the packet or rewrite the IP precedence by resetting the type of service (ToS) bits. You can configure CAR to send, drop, or set precedence.

CAR utilizes a token bucket measurement. Tokens are inserted into the bucket at the committed rate. The depth of the bucket is the burst size. Traffic arriving at the bucket when sufficient tokens are available is said to conform, and the corresponding number of tokens are removed from the bucket. If a sufficient number of tokens are not available, then the traffic is said to exceed.

- [Matching Criteria, page 3](#)
- [Rate Limits, page 4](#)
- [Conform and Exceed Actions, page 6](#)
- [Multiple Rate Policies, page 6](#)

Matching Criteria

Traffic matching entails identification of traffic of interest for rate limiting, precedence setting, or both. Rate policies can be associated with one of the following qualities:

- Incoming interface
- All IP traffic
- IP precedence (defined by a rate-limit access list)
- MAC address (defined by a rate-limit access list)
- Multiprotocol Label Switching (MPLS) experimental (EXP) value (defined by a rate-limit access list)
- IP access list (standard and extended)

CAR provides configurable actions, such as send, drop, or set precedence when traffic conforms to or exceeds the rate limit.

**Note**

Matching to IP access lists is more processor intensive than matching based on other criteria.

Rate Limits

CAR propagates bursts. It does no smoothing or shaping of traffic, and therefore does no buffering and adds no delay. CAR is highly optimized to run on high-speed links--DS3, for example--in distributed mode on Versatile Interface Processors (VIPs) on the Cisco 7500 series.

CAR rate limits may be implemented either on input or output interfaces or subinterfaces including Frame Relay and ATM subinterfaces.

- [What Rate Limits Define, page 4](#)
- [Extended Burst Value, page 4](#)
- [How Extended Burst Capability Works, page 5](#)
- [Recommended Burst Values, page 5](#)
- [Actual and Compounded Debt Example, page 5](#)

What Rate Limits Define

Rate limits define which packets conform to or exceed the defined rate based on the following three parameters:

- Average rate. The average rate determines the long-term average transmission rate. Traffic that falls under this rate will always conform.
- Normal burst size. The normal burst size determines how large traffic bursts can be before some traffic exceeds the rate limit.
- Excess Burst size. The Excess Burst (Be) size determines how large traffic bursts can be before all traffic exceeds the rate limit. Traffic that falls between the normal burst size and the Excess Burst size exceeds the rate limit with a probability that increases as the burst size increases.

The maximum number of tokens that a bucket can contain is determined by the normal burst size configured for the token bucket.

When the CAR rate limit is applied to a packet, CAR removes from the bucket tokens that are equivalent in number to the byte size of the packet. If a packet arrives and the byte size of the packet is greater than the number of tokens available in the standard token bucket, extended burst capability is engaged if it is configured.

Extended Burst Value

Extended burst is configured by setting the extended burst value greater than the normal burst value. Setting the extended burst value equal to the normal burst value excludes the extended burst capability. If extended burst is not configured, given the example scenario, the exceed action of CAR takes effect because a sufficient number of tokens are not available.

When extended burst is configured and this scenario occurs, the flow is allowed to borrow the needed tokens to allow the packet to be sent. This capability exists so as to avoid tail-drop behavior, and, instead, engage behavior like that of Random Early Detection (RED).

How Extended Burst Capability Works

Here is how the extended burst capability works. If a packet arrives and needs to borrow n number of tokens because the token bucket contains fewer tokens than its packet size requires, then CAR compares the following two values:

- Extended burst parameter value.
- Compounded debt. Compounded debt is computed as the sum over all ai :
 - a indicates the actual debt value of the flow after packet i is sent. Actual debt is simply a count of how many tokens the flow has currently borrowed.
 - i indicates the i th packet that attempts to borrow tokens since the last time a packet was dropped.

If the compounded debt is greater than the extended burst value, the exceed action of CAR takes effect. After a packet is dropped, the compounded debt is effectively set to 0. CAR will compute a new compounded debt value equal to the actual debt for the next packet that needs to borrow tokens.

If the actual debt is greater than the extended limit, all packets will be dropped until the actual debt is reduced through accumulation of tokens in the token bucket.

Dropped packets do not count against any rate or burst limit. That is, when a packet is dropped, no tokens are removed from the token bucket.



Note

Though it is true the entire compounded debt is forgiven when a packet is dropped, the actual debt is not forgiven, and the next packet to arrive to insufficient tokens is immediately assigned a new compounded debt value equal to the current actual debt. In this way, actual debt can continue to grow until it is so large that no compounding is needed to cause a packet to be dropped. In effect, at this time, the compounded debt is not really forgiven. This scenario would lead to excessive drops on streams that continually exceed normal burst. (See the example in the following section, "[Actual and Compounded Debt Example](#), page 5.")

Testing of TCP traffic suggests that the chosen normal and extended burst values should be on the order of several seconds worth of traffic at the configured average rate. That is, if the average rate is 10 Mbps, then a normal burst size of 10 to 20 Mb and an Excess Burst size of 20 to 40 Mb would be appropriate.

Recommended Burst Values

Cisco recommends the following values for the normal and extended burst parameters:

```
normal burst = configured rate * (1 byte)/(8 bits) * 1.5 seconds
extended burst = 2 * normal burst
```

With the listed choices for parameters, extensive test results have shown CAR to achieve the configured rate. If the burst values are too low, then the achieved rate is often much lower than the configured rate.

Actual and Compounded Debt Example

This example shows how the compounded debt is forgiven, but the actual debt accumulates.

For this example, assume the following parameters:

- Token rate is 1 data unit per time unit
- Normal burst size is 2 data units
- Extended burst size is 4 data units
- 2 data units arrive per time unit

After 2 time units, the stream has used up its normal burst and must begin borrowing one data unit per time unit, beginning at time unit 3:

Time	DU arrivals	Actual Debt	Compounded Debt
1	2	0	0
2	2	0	0
3	2	1	1
4	2	2	3
5	2	3 (temporary)	6 (temporary)

At this time a packet is dropped because the new compounded debt (6) would exceed the extended burst limit (4). When the packet is dropped, the compounded debt effectively becomes 0, and the actual debt is 2. (The values 3 and 6 were only temporary and do not remain valid in the case where a packet is dropped.) The final values for time unit 5 follow. The stream begins borrowing again at time unit 6.

Time	DU arrivals	Actual Debt	Compounded Debt
5	2	2	0
6	2	3	3
7	2	4 (temporary)	7 (temporary)

At time unit 6, another packet is dropped and the debt values are adjusted accordingly.

Time	DU arrivals	Actual Debt	Compounded Debt
7	2	3	0

Conform and Exceed Actions

CAR utilizes a token bucket, thus CAR can pass temporary bursts that exceed the rate limit as long as tokens are available.

Once a packet has been classified as conforming to or exceeding a particular rate limit, the router performs one of the following actions on the packet:

- Transmit--The packet is sent.
- Drop--The packet is discarded.
- Set precedence and transmit--The IP Precedence (ToS) bits in the packet header are rewritten. The packet is then sent. You can use this action to either color (set precedence) or recolor (modify existing packet precedence) the packet.
- Continue--The packet is evaluated using the next rate policy in a chain of rate limits. If there is not another rate policy, the packet is sent.
- Set precedence and continue--Set the IP Precedence bits to a specified value and then evaluate the next rate policy in the chain of rate limits.

For VIP-based platforms, two more actions are possible:

- Set QoS group and transmit--The packet is assigned to a QoS group and sent.
- Set QoS group and continue--The packet is assigned to a QoS group and then evaluated using the next rate policy. If there is not another rate policy, the packet is sent.

Multiple Rate Policies

A single CAR rate policy includes information about the rate limit, conform actions, and exceed actions. Each interface can have multiple CAR rate policies corresponding to different types of traffic. For example, low priority traffic may be limited to a lower rate than high priority traffic. When there are multiple rate

policies, the router examines each policy in the order entered until the packet matches. If no match is found, the default action is to send.

Rate policies can be independent: each rate policy deals with a different type of traffic. Alternatively, rate policies can be cascading: a packet may be compared to multiple different rate policies in succession.

Cascading of rate policies allows a series of rate limits to be applied to packets to specify more granular policies (for example, you could rate limit total traffic on an access link to a specified subrate bandwidth and then rate limit World Wide Web traffic on the same link to a given proportion of the subrate limit) or to match packets against an ordered sequence of policies until an applicable rate limit is encountered (for example, rate limiting several MAC addresses with different bandwidth allocations at an exchange point). You can configure up to a 100 rate policies on a subinterface.

Restrictions of CAR and VIP-Distributed CAR

CAR and VIP-distributed CAR can only be used with IP traffic. Non-IP traffic is not rate limited.

CAR or VIP-distributed CAR can be configured on an interface or subinterface. However, CAR and VIP-distributed CAR are not supported on the following interfaces:

- Fast EtherChannel
- Tunnel
- PRI
- Any interface that does not support Cisco Express Forwarding (CEF)

CAR is only supported on ATM subinterfaces with the following encapsulations: aal5snap, aal5mux, and aal5nlpid.



Note

CAR provides rate limiting and does not guarantee bandwidth. CAR should be used with other QoS features, such as distributed weighted fair queueing (DWFQ), if premium bandwidth assurances are required.

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).

The Traffic Policing feature 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 configured) and is useful in managing network bandwidth in cases where 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 entering the interface with Traffic Policing configured is placed into 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 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.

The Traffic Policing feature supports the following MIBs:

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

This feature also supports RFC 2697, *A Single Rate Three Color Marker*.

For information on how to configure the Traffic Policing feature, see the "Configuring Traffic Policing" module.

- [Benefits of Traffic Policing, page 8](#)
- [Restrictions for Traffic Policing, page 8](#)
- [Prerequisites for Traffic Policing, page 9](#)

Benefits of Traffic Policing

Bandwidth Management Through Rate Limiting

Traffic policing allows you to control the maximum rate of traffic sent 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. Traffic that falls within the rate parameters is sent, whereas traffic that exceeds the parameters is dropped or sent with a different priority.

Packet Marking Through IP Precedence, QoS Group, and DSCP Value Setting

Packet marking allows you to partition your network into multiple priority levels or classes of service (CoS), as follows:

- Use traffic policing to set the IP precedence or differentiated services code point (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 DWRED 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.

Restrictions for Traffic Policing

The following restrictions apply to the Traffic Policing feature:

- On a Cisco 7500 series router, traffic policing can monitor CEF switching paths only. In order to use the Traffic Policing feature, CEF must be configured on both the interface receiving the packet and the interface sending the packet.
- On a Cisco 7500 series router, traffic policing cannot be applied to packets that originated from or are destined to a router.
- Traffic policing can be configured on an interface or a subinterface.
- Traffic policing is not supported on the following interfaces:
 - Fast EtherChannel
 - Tunnel
 - PRI

- Any interface on a Cisco 7500 series router that does not support CEF

Prerequisites for Traffic Policing

On a Cisco 7500 series router, CEF must be configured on the interface before traffic policing can be used.

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 leaving an interface. This way, you can match the flow of the traffic to the speed of the interface receiving the packet.

Cisco provides three mechanisms for regulating or shaping traffic: Class-Based Traffic Shaping, Generic Traffic Shaping (GTS), and Frame Relay Traffic Shaping (FRTS).

For more information about traffic shaping, see the "Regulating Packet Flow Using Traffic Shaping" module.

For information on configuring Frame Relay and FRTS, see the "Configuring Frame Relay" module and the "MQC-Based Frame Relay Traffic Shaping" module, respectively.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

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



Configuring Traffic Policing

This feature module describes the Traffic Policing feature. Traffic policing allows you to control the maximum rate of traffic transmitted or received on an interface.

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS 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, page 11](#)
- [Feature Overview, page 11](#)
- [Supported Platforms, page 13](#)
- [Supported Standards MIBs and RFCs, page 14](#)
- [Prerequisites, page 14](#)
- [Configuration Tasks, page 14](#)
- [Monitoring and Maintaining Traffic Policing, page 15](#)
- [Configuration Examples, page 15](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see 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 document.

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

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.

The Traffic Policing feature is applied when you attach a traffic policy contain the Traffic Policing configuration to an interface. A traffic policy is configured using the Modular Quality of Service (QoS) Command-Line Interface (CLI) (MQC).

The table below lists the feature history.

Table 1 **Feature History**

Cisco IOS Release	Enhancement
12.1(5)T	This command was introduced for Cisco IOS Release 12.1 T. A new Traffic Policing algorithm was introduced. The violate-action option became available. This feature became available on Cisco 2600, 3600, 4500, 7200, and 7500 series routers.
12.2(2)T	The set-clp-transmit option for the <i>action</i> argument was added to the police command. The set-frde-transmit option for the <i>action</i> argument was added to the police command. However, the set-frde-transmit option is not supported for Any Transport over Multiprotocol Label Switching (MPLS) (AToM) traffic in this release. The set-mpls-exp-transmit option for the <i>action</i> argument was added to the police command.
Cisco IOS	For information about feature support in Cisco IOS software, use Cisco Feature Navigator.

- [Benefits, page 12](#)
- [Restrictions, page 13](#)

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

- On a Cisco 7500 series router, traffic policing can monitor Cisco Express Forwarding (CEF) switching paths only. In order to use the Traffic Policing feature, Cisco Express Forwarding must be configured on both the interface receiving the packet and the interface sending the packet.
- On a Cisco 7500 series router, traffic policing cannot be applied to packets that originated from or are destined to a router.
- Traffic policing can be configured on an interface or a subinterface.
- Traffic policing is not supported on the following interfaces:
 - Fast EtherChannel
 - Tunnel



Note

Traffic policing is supported on tunnels that are using the Cisco generic routing encapsulation (GRE) tunneling protocol.

- ◦ PRI
- ◦ Any interface on a Cisco 7500 series router that does not support Cisco Express Forwarding

Supported Platforms



Note

Cisco IOS Release 12.2(2)T or later does not run on Cisco 2500 series routers.

- Cisco 2500 series
- Cisco 2600 series
- Cisco 3640 routers
- Cisco 4500 series
- Cisco 7000 series with RSP7000
- Cisco 7100 series
- Cisco 7200 series
- Cisco 7500 series

**Note**

To use the **set-clp-transmit** action available with this feature, the Enhanced ATM Port Adapter (PA-A3) is required. Therefore, the **set-clp-transmit** action is not supported on any platform that does not support the PA-A3 adapter (such as the Cisco 2600 series router, the Cisco 3640 router, and the 4500 series router). For more information, see the documentation for your specific router.

Supported Standards MIBs and RFCs

Standards

No new or modified standards are supported by this feature.

MIBs

Class-Based Quality of Service MIB

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

For descriptions of supported MIBs and how to use MIBs, see the Cisco MIB web site on CCO at <http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>.

RFCs

- RFC 2697, *A Single Rate Three Color Marker*

Prerequisites

On a Cisco 7500 series router, Cisco Express Forwarding (CEF) must be configured on the interface before traffic policing can be used.

Configuration Tasks

- [Configuring Traffic Policing, page 15](#)
- [Troubleshooting Tips, page 15](#)

Configuring Traffic Policing

Command	Purpose
Router(config-pmap-c)# police <i>bps burst-normal burst-max conform-action action exceed-action action violate-action action</i>	<p>Specifies a maximum bandwidth usage by a traffic class.</p> <p>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.</p>

Troubleshooting Tips

- Check the interface type. Verify that your interface is not mentioned in the nonsupported interface description in the [Restrictions, page 13](#) section of this module.
- For input traffic policing on a Cisco 7500 series router, verify that CEF is configured on the interface where traffic policing is configured.
- For output traffic policing on a Cisco 7500 series router, ensure that the incoming traffic is CEF-switched. Traffic policing cannot be used on the switching path unless CEF switching is enabled.

Monitoring and Maintaining Traffic Policing

Command	Purpose
Router# show policy-map	Displays all configured policy maps.
Router# show policy-map <i>policy-map-name</i>	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 Configuring a Service Policy that Includes Traffic Policing, page 16](#)

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 example, traffic policing is configured with the average rate at 8000 bits per second, the normal burst size at 1500 bytes, and the excess burst size at 4000 bytes. Packets coming into Fast Ethernet interface 0/0 are evaluated by the token bucket algorithm to analyze whether packets conform, exceed, or violate the parameters. Packets that conform are transmitted, packets that exceed are assigned a QoS group value of 4 and are transmitted, 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 1500 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 fastethernet 0/0
Router(config-if)# service-policy input police
```

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

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



Two-Rate Policer

This document describes the Two-Rate Policer feature and how to configure it. Two-Rate Policer allows you to manage traffic rates through an interface; it is especially helpful in managing network bandwidth where large packets are in the same traffic stream.

- [Finding Feature Information, page 17](#)
- [Prerequisites for Two-Rate Policer, page 17](#)
- [Restrictions for Two-Rate Policer, page 18](#)
- [Information About Two-Rate Policer, page 18](#)
- [How to Use the Two-Rate Policer, page 20](#)
- [Configuration Examples, page 21](#)
- [Additional References, page 22](#)
- [Feature Information for Two-Rate Policer, page 23](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see 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 document.

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 Two-Rate Policer

Supported Platforms

- Cisco 2600 series
- Cisco 3620
- Cisco 3640
- Cisco 7100 series
- Cisco 7200 series
- Cisco 7500 series (VIP-based platform only)

**Note**

The **set-clp-transmit** action available with Two-Rate Policer, the Enhanced ATM Port Adapter (PA-A3) is required. The **set-clp-transmit** action is not supported on any platform that does not support the PA-A3 adapter (such as the Cisco 2600 series router, the Cisco 3620 router, and the 3640 router). For more information, see the documentation for your specific router.

- On a Cisco 7500 series router, Cisco Express Forwarding or Distributed Cisco Express Forwarding must be configured on the interface before you can use 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. These tasks are performed using the Modular quality of service (QoS) Command-Line Interface (CLI) (MQC). For information on the MQC, see the "Applying QoS Features Using the MQC" module.

Restrictions for Two-Rate Policer

The following restrictions apply to the Two-Rate Policer feature:

- On a Cisco 7500 series router, traffic policing can monitor Cisco Express Forwarding or Distributed Cisco Express Forwarding switching paths only. Cisco Express Forwarding or Distributed Cisco Express Forwarding must be configured on both the interface receiving the packet and the interface sending the packet.
- On a Cisco 7500 series router, traffic policing cannot be applied to packets that originated from or are destined to a router.
- 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 the following interfaces:
 - Fast EtherChannel
 - PRI
 - Any interface on a Cisco 7500 series router that does not support Cisco Express Forwarding or Distributed Cisco Express Forwarding

Information About Two-Rate Policer

Networks police traffic by limiting the input or output transmission rate of a class of traffic based on user-defined criteria. Policing traffic 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).

The Two-Rate Policer 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 IP precedence value, IP differentiated services code point (DSCP) value, Multiprotocol Label Switching (MPLS) experimental value, Quality of Service (QoS) group, ATM Cell Loss Priority (CLP) bit, and the Frame Relay Discard Eligibility (DE) bit.

With the Two-Rate Policer, you can enforce traffic policing according to two separate rates--committed information rate (CIR) and peak information rate (PIR). You can specify the use of these two rates, along with their corresponding values, by using two keywords, **cir** and **pir**, of the **police** command.

The Two-Rate Policer 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 the interface (depending on the location of the interface on which the Two-Rate Policer is configured) and is useful in managing network bandwidth in cases where 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 coming into the interface with the Two-Rate Policer configured is assigned one of these categories. Within these three categories, users can decide packet treatments. For instance, packets that conform can be configured to be sent, packets that exceed can be configured to be sent with a decreased priority, and packets that violate can be configured to be dropped.

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

**Note**

Two-Rate Policer enables you to use Differentiated Services (DiffServ) Assured Forwarding (AF) Per-Hop Behavior (PHB) traffic conditioning. For more information about DiffServ, see the "Implementing DiffServ for End-to-End Quality of Service Overview" module.

**Note**

Starting with Cisco IOS Release 12.1(5)T, you can police traffic by using the Traffic Policing feature (sometimes referred to as the single-rate policer). The Two-Rate Policer (available with Cisco IOS Release 12.2(4)T) is in addition to the Traffic Policing feature, and it provides additional functionality. For more information about the Traffic Policing feature, see the "Traffic Policing" module.

- [Benefits, page 19](#)

Benefits

Bandwidth Management Through Rate Limiting

Two-Rate Policer provides improved bandwidth management through rate limiting. Before this feature was available, you could police traffic with the single-rate Traffic Policing feature. The Traffic Policing feature provided a certain amount of bandwidth management by allowing you to set the peak burst size (be). The Two-Rate Policer supports a higher level of bandwidth management and supports a sustained excess rate. With the Two-Rate Policer, you can enforce traffic policing according to two separate rates--CIR and PIR--specified in bits per second (bps).

Packet Marking Through IP Precedence, DSCP Value, MPLS Experimental Value, and the QoS Group Setting

In addition to rate-limiting, the Two-Rate Policer allows you to independently mark the packet according to whether the packet conforms, exceeds, or violates a specified rate. Packet marking also allows you to partition your network into multiple priority levels or CoSs.

- Use the Two-Rate Policer to set the IP precedence value, the IP DSCP value, or the MPLS experimental value for packets that enter the network. Then networking devices within your network can use this setting to determine how the traffic should be treated. For example, the Weighted Random

Early Detection (WRED) feature uses the IP precedence value to determine the probability that a packet will be dropped.

- Use the Two-Rate Policer to assign packets to a QoS group. The router uses the QoS group to determine how to prioritize packets within the router.

If you want to mark traffic but do not want to use the Two-Rate Policer, see the "Marking Network Traffic" module.

Packet Marking for Frame Relay Frames

The Two-Rate Policer 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 that have the DE bit set to 1 are discarded before frames that have the DE bit set to 0.

Packet Marking for ATM Cells

The Two-Rate Policer 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 that have the ATM CLP bit set to 1 are discarded before cells that have the ATM CLP bit set to 0.

How to Use the Two-Rate Policer

- [Configuring the Two-Rate Policer, page 20](#)
- [Verifying the Two-Rate Policer Configuration, page 21](#)
- [Troubleshooting Tips, page 21](#)
- [Monitoring and Maintaining the Two-Rate Policer, page 21](#)

Configuring the Two-Rate Policer

Command	Purpose
<pre>Router(config-pmap-c)# police cir cir [bc conform-burst] pir pir [be peak-burst</pre>	<p>Specifies that both the CIR and the PIR are to be used for two-rate traffic policing. The bc and be keywords and their associated arguments (<i>conform-burst</i> and <i>peak-burst</i>, respectively) are optional.</p> <p>Specifies the action taken on a packet when you enable an optional action argument.</p> <p>Note The Two-Rate Policer works by using a token bucket mechanism. There are currently two types of token bucket algorithms: a single token bucket algorithm (available through the Traffic Policing feature) and a two token bucket algorithm (available through the Two-Rate Policer).</p>

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

- Check the interface type. Verify that your interface is not listed as a nonsupported interface in the [Restrictions for Two-Rate Policer, page 18](#) section of this module.
- 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 Two-Rate Policer

Command	Purpose
Router# show policy-map	Displays all configured policy maps.
Router# show policy-map <i>policy-map-name</i>	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 Limiting the Traffic Using a Policer Class, page 21](#)

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 10
1
```

```

Router(config-cmap)# policy-map
  policyl
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
Router(config-if)# service-policy
  output policyl
Router(config-if)# end
Router# show
  policy-map policyl
  Policy Map policyl
    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.

```

Router# show
  policy-map interface serial3/0
  Serial3/0
    Service-policy output: policyl
    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

```

Additional References

The following sections provide references related to the Two-Rate Policer feature.

Related Documents

Related Topic	Document Title
MQC	<ul style="list-style-type: none"> "Applying QoS Features Using the MQC" module
QoS features such as class-based weighted fair queueing (CBWFQ), traffic marking, and traffic policing	<ul style="list-style-type: none"> "Configuring Weighted Fair Queueing" module "Marking Network Traffic" module "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
<ul style="list-style-type: none"> CISCO-CLASS-BASED-QOS-MIB CISCO-CLASS-BASED-QOS-CAPABILITY-MIB 	<p>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:</p> <p>http://www.cisco.com/go/mibs</p>

RFCs

RFC	Title
RFC 2698	<i>A Two Rate Three Color Marker</i>

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<p>http://www.cisco.com/cisco/web/support/index.html</p>

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 2 **Feature Information for Two-Rate Policer**

Feature Name	Releases	Feature Information
Two-Rate Policer	12.2(4)T	This feature was introduced.
	12.2(4)T3	Support for the Cisco 7500 series routers was added.
	12.0(26)S	This feature was integrated into Cisco IOS Release 12.0(26)S for the Cisco 7200 and 7500 series routers.
	12.2(28)SB	This feature was integrated into Cisco IOS Release 12.2(28)SB.
	12.2(33)SRA	This feature was integrated into Cisco IOS Release 12.2(33)SRA.
	12.2(33)SXH	This feature was integrated into Cisco IOS Release 12.2(33)SXH.
	Cisco IOS XE 3.1.0 SG	This feature was integrated into Cisco IOS XE 3.1.0 SG.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

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



Policer Enhancement - Multiple Actions

Feature History

Release	Modification
12.2(8)T	This feature was introduced.

This document describes the Policer Enhancement -- Multiple Actions feature in Cisco IOS Release 12.2(8)T. It includes the following sections:

- [Finding Feature Information, page 25](#)
- [Feature Overview, page 25](#)
- [Supported Platforms, page 27](#)
- [Supported Standards MIBs and RFCs, page 27](#)
- [Prerequisites, page 28](#)
- [Configuration Tasks, page 28](#)
- [Monitoring and Maintaining the Multiple Policer Actions, page 29](#)
- [Configuration Examples, page 29](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see 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 document.

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 Traffic Policing feature (a 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.

- [Benefits, page 26](#)
- [Restrictions, page 26](#)
- [Related Features and Technologies, page 26](#)
- [Related Documents, page 26](#)

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

- On a Cisco 7500 series router, traffic policing can monitor Cisco Express Forwarding (CEF) or distributed CEF (dCEF) switching paths only. To use the Two-Rate Policer, CEF or dCEF must be configured on both the interface receiving the packet and the interface sending the packet.
- On a Cisco 7500 series router, traffic policing cannot be applied to packets that originated from or are destined to a router.
- Multiple policer actions can be configured on an interface, a subinterface, a Frame Relay data-link connection identifier (DLCI), and an ATM permanent virtual circuit (PVC) only.
- When using this feature, you can specify a maximum of four actions at one time.
- Multiple policer actions are not supported on the following interfaces:
 - Fast EtherChannel
 - PRI
 - Any interface on a Cisco 7500 series router that does not support CEF or dCEF

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
- Cisco IOS Quality of Service Solutions Command Reference.
- RFC 2697, *A Single Rate Three Color Marker*
- RFC 2698, *A Two Rate Three Color Marker*

Supported Platforms

- Cisco 1700 series
- Cisco 2600 series
- Cisco 3620
- Cisco 3640
- Cisco 3660
- Cisco 7100 series
- Cisco 7200 series
- Cisco 7500 series (VIP-based platform only)
- Cisco MC3810

**Note**

To use the *set-clp-transmit* action available with this feature, the Enhanced ATM Port Adapter (PA-A3) is required. Therefore, the *set-clp-transmit* action is not supported on any platform that does not support the PA-A3 adapter (such as the Cisco 2600 series router and the Cisco 3640 router). For more information, refer to the documentation for your specific router.

Supported Standards MIBs and RFCs

Standards

No new or modified standards are supported by this feature.

MIBs

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

To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL:

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

RFCs

- RFC 2697, *A Single Rate Three Color Marker*
- RFC 2698, *A Two Rate Three Color Marker*

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, page 28](#)
- [Verifying the Multiple Policer Actions Configuration, page 28](#)
- [Troubleshooting Tips, page 29](#)

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 <i>policy-map-name</i>	Creates a policy map. Enters policy-map configuration mode.
Step 2	Router(config-pmap)# class <i>class-default</i>	Specifies the default traffic class for a service policy. Enters policy-map class configuration mode.
Step 3	Router(config-pmap-c)# police { cir <i>cir</i> } [bc <i>conform-burst</i>] { pir <i>pir</i> } [be <i>peak-burst</i>] [conform-action <i>action</i> [exceed-action <i>action</i> [violate-action <i>action</i>]]]	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 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 in the "Restrictions" section of this document.
- For input traffic policing on a Cisco 7500 series router, verify that CEF or dCEF 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 CEF-switched or dCEF-switched. Traffic policing cannot be used on the switching path unless CEF or dCEF 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 <i>policy-map-name</i>	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, page 29](#)
- [Example Verifying the Multiple Policer Actions, page 30](#)

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
```

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

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



Percentage-Based Policing and Shaping

Feature History

Release	Modification
12.2(13)T	This feature was introduced.

Supported Platforms

For platforms supported in Cisco IOS Release 12.2(13)T, consult Cisco Feature Navigator.

This document describes the Percentage-Based Policing and Shaping feature in Cisco IOS Release 12.2(13)T. It includes the following sections:

- [Finding Feature Information, page 31](#)
- [Feature Overview, page 31](#)
- [Supported Standards MIBs and RFCs, page 33](#)
- [Prerequisites, page 33](#)
- [Configuration Tasks, page 34](#)
- [Configuration Examples, page 35](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see 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 document.

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

Cisco IOS 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 based on 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.

This feature also provides the option of specifying burst sizes in milliseconds (ms) when configuring traffic policing and shaping based on a percentage of bandwidth.

- [Benefits, page 32](#)
- [Restrictions, page 32](#)
- [Related Features and Technologies, page 32](#)
- [Related Documents, page 32](#)

Benefits

Increased Flexibility

This feature provides the ability to configure traffic policing and traffic shaping based on a *percentage* of bandwidth available on an 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.

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 QoS command-line interface (CLI) (Modular QoS CLI)
- Class-based weighted fair queueing (CBWFQ)
- Class-based packet marking
- Cisco Express Forwarding (CEF) and Distributed CEF (dCEF)
- Traffic policing
- Two-rate policing
- Traffic shaping

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

None

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/TTDIT/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

- RFC 2697, *A Single Rate Three Color Marker*
- RFC 2698, *A Two Rate Three Color Marker*

Prerequisites

On a Cisco 7500 series router, Distributed Cisco Express Forwarding (dCEF) must be configured on the interface before you can use the Percentage-Based Policing and Shaping feature.

Configuration Tasks

- [Configuring Policing and Shaping Based on Bandwidth Percentage](#), page 34
- [Attaching the Policy Map to an Interface or a VC](#), page 35
- [Verifying the Policing and Shaping Bandwidth Percentage Setting](#), page 35
- [Troubleshooting Tips](#), page 35

Configuring Policing and Shaping Based on Bandwidth Percentage

SUMMARY STEPS

1. Router (config)# **policy-map***policy-name*
2. Router(config-pmap)# **class-map***class-map-name*
3. Router(config-pmap-c)# **police cir percent** *percent*[**bc***conform-burst-in-msec*] [**pir percent** *percent*] [**be***peak-burst-in-msec*]
4. Router(config-pmap-c)# **shape {average | peak} percent***percent* [*bc*] [*be*]
5. Router (config-pmap-c)# **service-policy***policy-map-name*
6. Router(config-pmap-c)# **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router (config)# policy-map <i>policy-name</i>	Specifies the name of the policy map to be created. Enters policy-map configuration mode.
Step 2	Router(config-pmap)# class-map <i>class-map-name</i>	Specifies the name of the class map to be created. Enters policy-map class configuration mode.
Step 3	Router(config-pmap-c)# police cir percent <i>percent</i> [bc <i>conform-burst-in-msec</i>] [pir percent <i>percent</i>] [be <i>peak-burst-in-msec</i>]	Configures traffic policing.
Step 4	Router(config-pmap-c)# shape {average peak} percent <i>percent</i> [<i>bc</i>] [<i>be</i>]	Configures traffic shaping using either an average or peak traffic shaping rate based on a percentage of available bandwidth.
Step 5	Router (config-pmap-c)# service-policy <i>policy-map-name</i>	Specifies the name of a policy map to be used as a child policy map for this class.
Step 6	Router(config-pmap-c)# exit	Exits policy-map class configuration mode.

Attaching the Policy Map to an Interface or a VC

Command	Purpose
<pre>Router(config-if)# service-policy output policy-map-name</pre>	<p>Specifies the name of the policy map to be attached to the input direction of an interface or VC.</p> <p>The policy map evaluates all traffic entering that interface or VC.</p>
<pre>Router(config-if-atm-vc)# sevice-policy output policy-map-name</pre>	<p>Note Traffic shaping is supported on service policies attached to output interfaces or output VCs only.</p>

Verifying the Policing and Shaping Bandwidth Percentage Setting

Command	Purpose
<pre>Router# show class-map</pre>	<p>Displays all information about a class map, including the match criterion.</p>
<pre>Router# show policy-map</pre>	<p>Displays all configured policy maps.</p>
<pre>Router# show policy-map interface interface-name</pre>	<p>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 permanent virtual circuit (PVC) on the interface.</p>

Troubleshooting Tips

- For input traffic policing on a Cisco 7500 series router, verify that dCEF is enabled 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 dCEF-switched. Traffic policing cannot be used on the switching path unless dCEF switching is enabled.

Configuration Examples

- [Example Specifying Traffic Policing Based on a Bandwidth Percentage, page 35](#)
- [Example Specifying Traffic Shaping Based on a Bandwidth Percentage, page 36](#)
- [Example Verifying That CEF Is Enabled, page 36](#)

Example Specifying Traffic Policing Based on a Bandwidth Percentage

The following example configures traffic policing using a committed information rate (CIR) and a peak information rate (PIR) based on 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 (config)#  
  policy-map policy1  
  
Router(config-pmap)# class-map class1  
  
Router(config-pmap-c)# police cir percent 20 bc 300 ms pir percent 40 be 400 ms  
  
Router (config-pmap-c)# service-policy child-policy1  
  
Router(config-pmap-c)# exit  
  
Router(config-pmap-c)# interface serial 3/1  
  
Router(config-if)#  
  service-policy output policy1
```

The purpose of the burst parameters (bc and be values) is to drop packets gradually, as is done with Weighted Random Early Detection (WRED), and to avoid tail drop. Setting sufficiently high burst values helps to ensure good throughput.

Example Specifying Traffic Shaping Based on a Bandwidth Percentage

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

```
Router (config)#  
  policy-map policy1  
  
Router(config-pmap)# class-map class1  
  
Router(config-pmap-c)# shape average percent 25 300 ms 400 ms  
  
Router (config-pmap-c)# service-policy child-policy1  
  
Router(config-pmap-c)# exit  
  
Router(config-pmap-c)# interface serial 3/1  
  
Router(config-if)#  
  service-policy output policy1
```

The purpose of the bc and be values is to drop packets gradually, as is done with WRED, and to avoid tail drop. Setting sufficiently high burst values helps to ensure good throughput.

Example Verifying That CEF Is Enabled

On a Cisco 7500 series router, dCEF must be configured on the interface before you can use the Percentage-Based Policing and Shaping feature. The **show ip cef summary** command can be used to

confirm that dCEF is enabled and is being used for IP switching. In rare instances, this command displays "IP Distributed CEF without switching" in the command output. This indicates that dCEF is disabled. The following sample output of the **show ip cef summary** command indicates that dCEF is disabled:

```
Router# show ip cef summary

IP Distributed CEF with switching (Table Version 36), flags=0x0
 18 routes, 0 reresolve, 0 unresolved (0 old, 0 new), peak 3
 18 leaves, 19 nodes, 22136 bytes, 45 inserts, 27 invalidations
 0 load sharing elements, 0 bytes, 0 references
 universal per-destination load sharing algorithm, id 680E93E2
 3(0) CEF resets, 1 revisions of existing leaves
 Resolution Timer:Exponential (currently 1s, peak 1s)
 0 in-place/0 aborted modifications
 refcounts: 5136 leaf, 5120 node
```

When you configure a feature that requires special handling or is not yet supported in the dCEF switching paths, packets are forwarded to the next switching layer for handling. In this instance, the output of the **show cef interface** command displays "Packets switched to this interface on line card are dropped to next slow path" as shown in the following sample output.

```
Router# show cef interface Serial 10/0/0:28

Serial10/0/0:28 is up (if_number 38)
 Internet address is 90.0.0.1/8
 ICMP redirects are never sent
 Per packet loadbalancing is disabled
 Inbound access list is not set
 Interface is marked as point to point interface
 Packets switched to this interface on linecard are dropped to next slow path
Hardware idb is Serial10/0/0:28
 Fast switching type 4, interface type 20
 IP Distributed CEF switching enabled
 Fast flags 0x0. ifindex 37(37)
 Slot 10 Slot unit 0 VC 28
 Hardware transmit queue ptr 0x48001AE0 (0x48001AE0)
 Transmit limit accumulator 0x48000102 (0x48000102)
 IP MTU 1500
```

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

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



Modular QoS CLI Three-Level Hierarchical Policer

The Modular QoS CLI (MQC) Three-Level Hierarchical Policer extends the traffic policing functionality by allowing you to configure traffic policing at three levels of policy map hierarchies; a primary level, a secondary level, and a tertiary level. Traffic policing may be configured at any or all of these levels, depending on the needs of your network. Configuring traffic policing in a three-level hierarchical structure provides a high degree of granularity for traffic policing.

Feature Specifications for the Modular QoS CLI (MQC) Three-Level Hierarchical Policer

Feature History

Release	Modification
12.2(13)T	This feature was introduced.

Supported Platforms

For platforms supported in Cisco IOS Release 12.2(13)T, consult Cisco Feature Navigator.

- [Finding Feature Information, page 39](#)
- [Restrictions for the Modular QoS CLI Three-Level Hierarchical Policer, page 40](#)
- [Information About the Modular QoS CLI Three-Level Hierarchical Policer, page 41](#)
- [How to Configure the Modular QoS CLI Three-Level Hierarchical Policer, page 43](#)
- [Configuration Examples for the Modular QoS CLI Three-Level Hierarchical Policer, page 48](#)
- [Additional References, page 50](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see 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 document.

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 the Modular QoS CLI Three-Level Hierarchical Policer

If traffic policing is configured at both the top level and secondary levels, note the following caveats:

- When traffic policing is configured at both the primary and secondary levels, the traffic policer at the secondary level acts only on packets sent by the policer at the top level.

However, the packet classification for the policy map at the secondary level occurs before the primary level policer has acted on the classes. When this situation occurs, the class counters for the policy map at the secondary level may not be equal to the number of packets acted upon by the second level policer.

The following output of the **show policy-map interface** command helps to illustrate this point. In this sample output two policy maps (called "primary_level," and "secondary_level," respectively) have been configured. The primary_level policy map contains a class map called "c1," and the secondary_level policy map contains a class map called "c3".

```
> > > show policy interface serial5/0.1
> > > Serial5/0.1
> > >
> > > Service-policy output: primary_level
> > >
> > > Class-map: c1 (match-all)
> > > 24038 packets, 3004750 bytes
> > > 30 second offered rate 0 bps, drop rate 0 bps
> > > Match: any
> > > police:
> > >   cir 300000 bps, bc 9375 bytes
> > >   conformed 18105 packets, 2263125 bytes; actions:
> > >     transmit
> > >   exceeded 5933 packets, 741625 bytes; actions: (*)
> > >     drop
> > >   conformed 0 bps, exceed 0 bps
> > >
> > > Service-policy : secondary_level
> > >
> > > Class-map: c3 (match-all)
> > > 24038 packets, 3004750 bytes
> > >
> > > 30 second offered rate 0 bps, drop rate 0 bps
> > > Match: any
> > > police: (<= Indicates traffic policing has been configured)
> > >   cir 200000 bps, bc 3000 bytes
> > >   pir 250000 bps, be 3000 bytes
> > >   conformed 12047 packets, 1505875 bytes; actions: (**)
> > >     set-frde-transmit
> > >   exceeded 3004 packets, 375500 bytes; actions: (**)
> > >     set-frde-transmit
> > >   violated 3054 packets, 381750 bytes; actions: (**)
> > >     set-frde-transmit
> > >   conformed 0 bps, exceed 0 bps, violate 0 bps
> > >
> > > 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
```

Note the following about this example:

- - The class counter for the class map called "c3" shows 24038 packets (italicized in the example).
 - Traffic policing has been configured in the policy map, and the traffic policing feature for class map "c3" shows a total of 18105 packets -- 12047 conformed packets, plus 3004 exceeded

packets, plus 3054 violated packets (indicated by the double asterisks (***) in the example). This total is because 5933 packets have already been dropped in class map "c1" (indicated by the "*" in the example).

- Therefore, only 18105 packets (24038 packets minus 5933 packets) are acted upon by the traffic policing feature configured in the second_level policy map.
- In this implementation of the Modular QoS CLI (MQC) Three-Level Hierarchical Policer, traffic policing at the primary level does not guarantee fairness in sharing bandwidth among the child classes. If packets from two different classes arrive at the same rate and then go through a traffic policer, the output rates of the two classes could be different because this feature acts as an aggregate policer.

In other words, it is possible that the primary-level policer could drop packets in one class in favor of the other class. This situation would happen because the primary-level policer had enough tokens when the packets for one class arrived, but there were not enough tokens left for the other class. This pattern could continue indefinitely, based on the arrival pattern of the packets.

Information About the Modular QoS CLI Three-Level Hierarchical Policer

- [Modular Quality of Service Command-Line Interface, page 41](#)
- [Packet Flow in the Modular QoS CLI Three-Level Hierarchical Policer, page 42](#)
- [Other Traffic Policing-Related Features, page 42](#)

Modular Quality of Service Command-Line Interface

The MQC is a command-line interface (CLI) structure that allows you to create traffic policies and attach these 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 Modular quality of service (QoS) CLI structure 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.

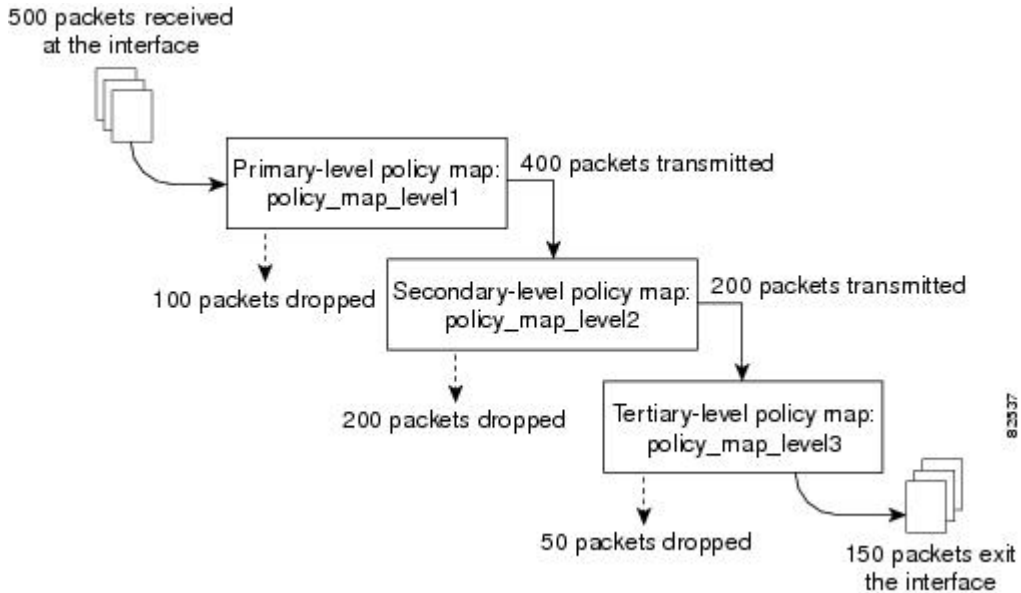
A traffic class contains three major elements: a name, a series of **match** commands, and, if more than one **match** command exists in the traffic class, an instruction on how to evaluate these **match** commands. The traffic class is named in the **class-map** command line; that is, if you enter the **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.

Packet Flow in the Modular QoS CLI Three-Level Hierarchical Policer

The figure below illustrates the flow of packets among policy maps configured for traffic policing at each level in the hierarchy.

Figure 1 Packet Flow Among Policy Maps



In the figure above, three policy maps are configured: `policy_map_level1` (the primary-level policy map), `policy_map_level2` (the secondary-level policy map), and `policy_map_level3` (the tertiary-level policy map). Traffic policing is configured in each policy map, and each policy map is attached to a service policy and to an interface.

In this simplified illustration, 500 packets arrive at the interface at which the policy map called "policy_map_level1" is attached. Because of the way traffic policing is configured in this policy map, 100 packets are dropped and 400 packets are transmitted.

The traffic policer at the secondary-level policy map (`policy_map_level2`) then evaluates the packets and treats them as determined by the way traffic policing is configured at this level. Of the 400 packets received, 200 are dropped and 200 are transmitted.

The traffic policer at the tertiary-level policy map (`policy_map_level3`), in turn, evaluates the 200 packets it has now received and applies the appropriate treatment as determined by the way the traffic policing is configured at this level.

Other Traffic Policing-Related Features

The Cisco IOS traffic policing software features allow you to control the maximum rate of traffic sent 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. Traffic that falls within the rate parameters is sent, whereas traffic that exceeds or violates the parameters is dropped or sent with a different priority.

The Cisco IOS software currently includes the following traffic policing features:

- Traffic Policing (a single-rate policer)

- Two-Rate Policer
- Policer Enhancements -- Multiple Actions
- Percentage-Based Policing and Shaping

Previously, these features could be configured at two levels of a policy map hierarchy; the top level and one secondary level. With the Modular QoS CLI (MQC) Three-Level Hierarchical Policer, these traffic policing-related features can be configured in three levels of a policy map hierarchy.

The tasks for configuring each of these traffic policing-related features is essentially the same. That is, you use the MQC to create a policy map. Then you use the **police** command to configure traffic policing for a specific class within that policy map. The policy map is then attached to an interface.

Traffic policing can be configured to specify multiple marking actions for the traffic being policed, or to use a percentage of available bandwidth when policing traffic.

How to Configure the Modular QoS CLI Three-Level Hierarchical Policer

- [Configuring Traffic Policing, page 43](#)
- [Attaching the Policy Map to an Interface, page 44](#)
- [Verifying the Configuration, page 46](#)

Configuring Traffic Policing

Traffic policing can be configured at any level of the policy map hierarchy, that is, at the primary level, secondary level, or the tertiary level.

Before configuring traffic policing, you must use the MQC to create a policy map.

SUMMARY STEPS

1. **enable**
2. **configure** {terminal | memory | network}
3. **policy-map** *policy-name*
4. **class-map** *class-map-name*
5. **police** *bps burst-normal burst-max conform-action action exceed-action action violate-action action*
6. **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.

Command or Action	Purpose
Step 2 <code>configure { terminal memory network }</code> Example: <pre>Router# configure terminal</pre>	Enters global configuration mode.
Step 3 <code>policy-map policy-name</code> Example: <pre>Router(config)# policy-map policyl</pre>	Specifies the name of the policy map created earlier and enters policy-map configuration mode. <ul style="list-style-type: none"> • See the Configuring Traffic Policing, page 43. • Enter policy map name.
Step 4 <code>class-map class-map-name</code> Example: <pre>Router(config-pmap)# class-map class1</pre>	Specifies the name of the class map created when the policy map was created earlier and enters policy-map class configuration mode. <ul style="list-style-type: none"> • See the Configuring Traffic Policing, page 43. • Enter the class map name.
Step 5 <code>police bps burst-normal burst-max conform-action action exceed-action action violate-action action</code> Example: <pre>Router(config-pmap-c)# police 8000 1000 1000 conform-action transmit exceed-action drop violate-action drop</pre>	Configures traffic policing according to burst sizes and any optional actions specified.
Step 6 <code>exit</code> Example: <pre>Router(config-pmap-c)# exit</pre>	(Optional) Exits the policy-map class configuration mode.

Attaching the Policy Map to an Interface

After the policy map has been created and traffic policing has been configured, the policy map must be attached to an interface. Policy maps can be attached to either the input or output direction of the interface.

Depending on the needs of your network, you may need to attach the policy map to a subinterface, an ATM permanent virtual circuit (PVC), a Frame Relay data-link connection identifier (DLCI), or other type of interface.

SUMMARY STEPS

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

DETAILED STEPS

Command or Action	Purpose
<p>Step 1 enable</p> <p>Example:</p> <pre>Router> enable</pre>	<p>Enables higher privilege levels, such as privileged EXEC mode.</p> <ul style="list-style-type: none"> • Enter your password if prompted.
<p>Step 2 configure { terminal memory network }</p> <p>Example:</p> <pre>Router# configure terminal</pre>	<p>Enters global configuration mode.</p>
<p>Step 3 interface <i>type number</i></p> <p>Example:</p> <p>Example:</p> <pre>Router(config-if)# interface s4/0</pre>	<p>Configures an interface (or subinterface) type and enters interface configuration mode.</p> <ul style="list-style-type: none"> • Enter the interface type number.
<p>Step 4 pvc [<i>name</i>] <i>vpi / vci</i> [ilmi qsaal smds]</p> <p>Example:</p> <pre>Router(config-if)# pvc cisco 0/16 ilmi</pre>	<p>(Optional) Creates or assigns a name to an ATM PVC and specifies the encapsulation type on an ATM PVC. Enters ATM virtual circuit (VC) configuration mode (config-if-atm-vc).</p> <p>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 Attaching the Policy Map to an Interface, page 44.</p>

Command or Action	Purpose
<p>Step 5 <code>service-policy {input output} policy-map-name</code></p> <p>Example:</p> <pre>Router(config-if)# service-policy input policy1</pre> <p>Example:</p>	<p>Specifies the name of the policy map to be attached to the input <i>or</i> output direction of the interface.</p> <p>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.</p> <ul style="list-style-type: none"> • Enter the policy map name.
<p>Step 6 <code>exit</code></p> <p>Example:</p> <pre>Router(config-if)# exit</pre>	<p>(Optional) Exits interface configuration mode.</p>

- [What to Do Next, page 46](#)

What to Do Next

If you want to configure traffic policing at another level in the policy map hierarchy, repeat the steps in the [Configuring Traffic Policing, page 43](#) section and the [Attaching the Policy Map to an Interface, page 44](#) section.

Verifying the Configuration

This task allows you to verify that you created the configuration you intended and that the feature is functioning correctly.

SUMMARY STEPS

1. **enable**
2. Do one of the following:
 - `show policy-map`
 - `show policy-map interface interface-name`
3. **exit**

DETAILED STEPS

Command or Action	Purpose
<p>Step 1 <code>enable</code></p> <p>Example:</p> <pre>Router> enable</pre>	<p>Enables higher privilege levels, such as privileged EXEC mode.</p> <ul style="list-style-type: none"> Enter your password if prompted.
<p>Step 2 Do one of the following:</p> <ul style="list-style-type: none"> <code>show policy-map</code> <code>show policy-map interface <i>interface-name</i></code> <p>Example:</p> <pre>Router# show policy-map</pre> <p>Example:</p> <pre>Router# show policy-map interface s4/0</pre>	<p>Displays all configured policy maps.</p> <p>or</p> <p>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.</p> <ul style="list-style-type: none"> Enter the interface name.
<p>Step 3 <code>exit</code></p> <p>Example:</p> <pre>Router(config-if)# exit</pre>	<p>(Optional) Exits interface configuration mode.</p>

- [Troubleshooting Tips, page 47](#)

Troubleshooting Tips

The commands in the [Verifying the Configuration, page 46](#) 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, the configuration is not correct or the feature is not functioning as expected, do the following:

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

- Use the **show running-config** command and analyze the output of the command.
- If the policy map does not appear in the output of the **show running-config** command, enable the **logging console** command.
- 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:

- Use the **show policy-map** command and analyze the output of the command.
- Use the **show running-config** command and analyze the output of the command.
- Run the **show policy-map interface** command and analyze the output of the command. Review the the following:
 - If a policy map applies queueing, and the packets are matching the correct class, but you see unexpected results, compare the number of packets to the number of packets matched.
 - If the interface is congested, and you are only seeing a small number of packets matched, check the tuning of the 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 show output of the command.

Configuration Examples for the Modular QoS CLI Three-Level Hierarchical Policer

- [Example Configuring the Modular QoS CLI Three-Level Hierarchical Policer, page 48](#)

Example Configuring the Modular QoS CLI Three-Level Hierarchical Policer

In the following example, the Modular QoS CLI (MQC) Three-Level Hierarchical Policer has been configured for three classes within three separate policy maps. The three classes, called "c1," "c2," and "c3," respectively, have been configured using the match criteria specified as follows:

```
class-map c1
  match any
class-map c2
  match ip precedence 1 2 3
class-map c3
  match ip precedence 2
```

Next, the classes are configured in three separate policy maps, called "p_all" (the primary-level policy map), "pmatch_123" (the secondary-level policy map), and "pmatch_2" (the tertiary-level policy map), as shown below.

```
policy p_all
  class c1
    police 100000
    service-policy pmatch_123
policy pmatch_123
  class c2
    police 20000
    service-policy pmatch_2
policy pmatch_2
  class c3
    police 8000
```

The primary goal of this configuration is to limit all traffic to 100 kbps. Within this, the secondary goal is make sure that packets with precedence values of 1, 2, or 3 do not exceed 20 kbps and that packets with precedence value of 2 never exceed 8 kbps.

To verify that the classes have been configured correctly and to confirm the results of the traffic policing configuration in the policy maps, the **show policy-map** command and the **show policy-map interface** command can be used, as shown in the following sections.

The following sample output of the **show policy-map** command verifies the configuration of the classes in the policy maps:

```
Router# show policy map
  Policy Map p_all
    Class c1
      police cir 100000 bc 3000
        conform-action transmit
        exceed-action drop
        service-policy pmatch_123
  Policy Map pmatch_123
    Class c2
      police cir 20000 bc 1500
        conform-action transmit
        exceed-action drop
        service-policy pmatch_2
  Policy Map pmatch_2
    Class c3
      police cir 8000 bc 1500
        conform-action transmit
        exceed-action drop
```

The following sample output of the **show policy-map interface** command confirms the results of this configuration on the attached interface:

```
Router# show policy-map interface Ethernet3/1
Ethernet3/1
  Service-policy output:p_all
    Class-map:c1 (match-all)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match:any
      police:
        cir 100000 bps, bc 3000 bytes
        conformed 0 packets, 0 bytes; actions:
          transmit
        exceeded 0 packets, 0 bytes; actions:
          drop
        conformed 0 bps, exceed 0 bps,
      Service-policy :pmatch_123
      Class-map:c2 (match-all)
        0 packets, 0 bytes
        5 minute offered rate 0 bps, drop rate 0 bps
        Match:ip precedence 1 2 3
        police:
          cir 20000 bps, bc 1500 bytes
          conformed 0 packets, 0 bytes; actions:
            transmit
          exceeded 0 packets, 0 bytes; actions:
            drop
          conformed 0 bps, exceed 0 bps,
      Service-policy :pmatch_2
      Class-map:c3 (match-all)
        0 packets, 0 bytes
        5 minute offered rate 0 bps, drop rate 0 bps
        Match:ip precedence 2
        police:
          cir 8000 bps, bc 1500 bytes
          conformed 0 packets, 0 bytes; actions:
            transmit
          exceeded 0 packets, 0 bytes; actions:
            drop
          conformed 0 bps, exceed 0 bps,
      Class-map:class-default (match-any)
        0 packets, 0 bytes
        5 minute offered rate 0 bps, drop rate 0 bps
```

```

Match:any
Class-map:class-default (match-any)
  0 packets, 0 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
Match:any
Class-map:class-default (match-any)
  0 packets, 0 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
Match:any

```

Additional References

The following sections provide additional references related to the Modular QoS CLI (MQC) Three-Level Hierarchical Policer:

Related Documents

Related Topic	Document Title
QoS commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	<i>Cisco IOS Quality of Service Solutions Command Reference</i>
Additional information about configuring traffic policing	"Policing and Shaping Overview" module
Modular Quality of Service (QoS) Command-Line Interface (CLI) (MQC)	"Applying QoS Features Using the MQC" module
Two-rate traffic policing	"Two-Rate Policer" module
Traffic policing using multiple policer actions	"Policer Enhancements--Multiple Actions" module
Percentage-based traffic policing and shaping	"Percentage-Based Policing and Shaping" module
Frame Relay configurations	"Configuring Frame Relay" module
Frame Relay commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	<i>Cisco IOS Wide-Area Networking Command Reference</i>

Standards

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

MIBs

MIBs	MIBs Link
<ul style="list-style-type: none"> • CISCO-CLASS-BASED-QOS-CAPABILITY-MIB • CISCO-CLASS-BASED-QOS-MIB 	<p>To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL:</p> <p>http://www.cisco.com/public/sw-center/netmgmt/cntk/mibs.shtml</p>

RFCs

RFCs	Title
RFC 2697	<i>A Single Rate Three Color Marker</i>
RFC 2698	<i>A Two Rate Three Color Marker</i>

Technical Assistance

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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

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



ATM Policing by Service Category for SVC and SoftPVC

Feature History

Release	Modification
12.2(4)B	This feature was introduced on the Cisco 6400 NSP.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

This module describes the ATM Policing by Service Category for SVC/SoftPVC feature in Cisco IOS Release 12.2(13)T and includes the following sections:

- [Finding Feature Information, page 53](#)
- [Feature Overview, page 53](#)
- [Supported Platforms, page 54](#)
- [Supported Standards MIBs and RFCs, page 54](#)
- [Configuration Tasks, page 55](#)
- [Monitoring and Maintaining ATM Policing by Service Category for SVC and SoftPVC, page 57](#)
- [Configuration Examples, page 58](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see 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 document.

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, page 54](#)
- [Related Features and Technologies, page 54](#)
- [Related Documents, page 54](#)

Benefits

This feature enables you to select which and how traffic is affected by UPC. For example, you can configure your switch to pass all UBR traffic, but tag all other traffic types.

Related Features and Technologies

- Intelligent early packet discard (EPD)
- Intelligent partial (tail) packet discard

Related Documents

- [ATM Switch Router Software Configuration Guide](#)
- [ATM and Layer 3 Switch Router Command Reference](#)
- [Guide to ATM Technology](#)
- [ATM Forum UNI 3.1 Specification](#)

Supported Platforms

This feature is supported on the node switch processor (NSP) of the Cisco 6400 carrier-class broadband aggregator.

Supported Standards MIBs and RFCs

Standards

None

MIBs

CISCO-ATM-IF-MIB.my--New objects were created for per-service category SVC UPC intent.

To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL:

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

RFCs

None

Configuration Tasks

- [Configuring ATM Policing by Service Category for SVC and SoftPVC](#), page 55
- [Verifying ATM Policing by Service Category for SVC and SoftPVC](#), page 55
- [Troubleshooting Tips](#), page 56

Configuring ATM Policing by Service Category for SVC and SoftPVC

SUMMARY STEPS

1. Switch(config)# **interface atm***slot/subslot/port*
2. Switch(config-if)# **atm svc-upc-intent** [{**abr** | **cbr** | **vbr-rt** | **vbr-nrt** | **ubr**}] {**tag** | **pass** | **drop**}

DETAILED STEPS

	Command or Action	Purpose
Step 1	Switch(config)# interface atm <i>slot/subslot/port</i>	Selects the ATM interface.
Step 2	Switch(config-if)# atm svc-upc-intent [{ abr cbr vbr-rt vbr-nrt ubr }] { tag pass drop }	Specifies the UPC mode. If no service category is specified, then the UPC mode configuration is applied to all traffic types.
	Example:	
	Example:	
	(Repeat this step for each service category and UPC mode combination.)	

Verifying ATM Policing by Service Category for SVC and SoftPVC

SUMMARY STEPS

1. Enter the **show atm vc** or **show atm vp** EXEC command to display the UPC mode for a particular VC or VP.
2. Enter the **show atm interface** EXEC command. If the UPC mode is not the same for all service categories, the "Svc Upc Intent" field displays "by sc."

DETAILED STEPS

Step 1 Enter the **show atm vc** or **show atm vp EXEC** command to display the UPC mode for a particular VC or VP.

Example:

```
Switch# show atm vc int atm 0/0/1 2 120
Interface:ATM0/0/1, Type:oc3suni
VPI = 2 VCI = 120
Status:DOWN
Time-since-last-status-change:1wld
Connection-type:PVC
Cast-type:point-to-multipoint-leaf
Packet-discard-option:disabled
Usage-Parameter-Control (UPC):pass

Wrr weight:2
Number of OAM-configured connections:0
OAM-configuration:disabled
OAM-states: Not-applicable
Cross-connect-interface:ATM0/0/1, Type:oc3suni
...
```

Step 2 Enter the **show atm interface EXEC** command. If the UPC mode is not the same for all service categories, the "Svc Upc Intent" field displays "by sc."

Example:

```
Switch# show atm interface atm 8/0/1
Interface:      ATM8/0/1      Port-type:      oc3suni
IF Status:     UP              Admin Status:  up
Auto-config:   enabled           AutoCfgState:  completed
IF-Side:       Network         IF-type:        NNI
Uni-type:      not applicable  Uni-version:   not applicable
Max-VPI-bits:  8              Max-VCI-bits:  14
Max-VP:        255           Max-VC:         16383
ConfMaxSvpcVpi:255      CurrMaxSvpcVpi:255
ConfMaxSvccVpi:255      CurrMaxSvccVpi:255
ConfMinSvccVci:35       CurrMinSvccVci:35
Svc Upc Intent:by sc
                Signalling:  Enabled
ATM Address for Soft VC:47.0091.8100.0000.0002.b9ae.9301.4000.0c84.0010.00
Configured virtual links:
  PVCLs SoftVCLs  SVCLs  TVCLs  PVPLs SoftVPLs  SVPLs Total-Cfgd Inst-Conns
    3      4      0      0      1      0      0      8      7
Logical ports(VP-tunnels): 0
Input cells: 3036674      Output cells: 3036816
5 minute input rate:      0 bits/sec,      0 cells/sec
5 minute output rate:     0 bits/sec,      0 cells/sec
Input AAL5 pkts:1982638, Output AAL5 pkts:1982687, AAL5 crc errors:0
```

Troubleshooting Tips

If a VC is not configured with the appropriate UPC mode, make sure that the VC was set up after the **atm svc-upc-intent** command was configured. Changes to the UPC mode take affect after the VC is torn down and set up again.

Monitoring and Maintaining ATM Policing by Service Category for SVC and SoftPVC

Command	Purpose
Switch# show atm interface	Displays ATM-specific information about an ATM interface.
Switch# show controllers atm slot/subslot/port	Displays information about a physical port device. Includes dropped (or discarded) cells.
Switch# show atm vc [interface atm slot/subslot/port]	Displays the configured UPC action and intelligent packet discard mechanisms, as well as the number of cells discarded due to UPC violations.

- [Example Monitoring and Maintaining ATM Policing by Service Category for SVC and SoftPVC, page 57](#)

Example Monitoring and Maintaining ATM Policing by Service Category for SVC and SoftPVC

```
Switch# show atm vc interface atm 3/0/1.51 51 16

Interface: ATM3/0/1.51, Type: oc3suni
VPI = 51 VCI = 16
Status: DOWN
Time-since-last-status-change: 2w0d
Connection-type: PVC
Cast-type: point-to-point
Packet-discard-option: enabled

Usage-Parameter-Control (UPC): pass

Wrr weight: 32
Number of OAM-configured connections: 0
OAM-configuration: disabled
OAM-states: Not-applicable
Cross-connect-interface: ATM2/0/0, Type: ATM Swi/Proc
Cross-connect-VPI = 0
Cross-connect-VCI = 73
Cross-connect-UPC: pass
Cross-connect OAM-configuration: disabled
Cross-connect OAM-state: Not-applicable
Encapsulation: AAL5ILMI
Threshold Group: 6, Cells queued: 0
Rx cells: 0, Tx cells: 0
Tx Clp0:0, Tx Clp1: 0
Rx Clp0:0, Rx Clp1: 0
Rx Upc Violations:0, Rx cell drops:0

Rx pkts:0, Rx pkt drops:0
Rx connection-traffic-table-index: 6
Rx service-category: UBR (Unspecified Bit Rate)
Rx pcr-clp01: 424
Rx scr-clp01: none
Rx mcr-clp01: none
Rx cdvt: 1024 (from default for interface)
Rx mbs: none
```

```
Tx connection-traffic-table-index: 6
Tx service-category: UBR (Unspecified Bit Rate)
Tx pcr-clp01: 424
Tx scr-clp01: none
Tx mcr-clp01: none
Tx      cdvt: none
Tx      mbs: none
No AAL5 connection registered
```

Configuration Examples

- [Example Non-UBR Traffic Policing, page 58](#)

Example Non-UBR Traffic Policing

In the following example, the UBR traffic on ATM 3/0/0 is passed while all other traffic is policed:

```
Switch(config)# interface atm 3/0/0
Switch(config-if)# atm svc-upc-intent ubr pass
Switch(config-if)# atm svc-upc-intent cbr tag
Switch(config-if)# atm svc-upc-intent vbr-rt tag
Switch(config-if)# atm svc-upc-intent vbr-nrt tag
Switch(config-if)# atm svc-upc-intent abr drop
```

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

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



Modular QoS CLI Unconditional Packet Discard

Feature History

Release	Modification
12.2(13)T	This feature was introduced.

Supported Platforms

For platforms supported in Cisco IOS Release 12.2(13)T, consult Cisco Feature Navigator.

This module describes the Modular QoS CLI (MQC) Unconditional Packet Discard feature in Cisco IOS Release 12.2(13)T. It includes the following sections:

- [Finding Feature Information, page 59](#)
- [Feature Overview, page 59](#)
- [Supported Standards MIBs and RFCs, page 60](#)
- [Configuration Tasks, page 61](#)
- [Configuration Examples, page 64](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see 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 document.

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

The Modular QoS CLI (MQC) Unconditional Packet Discard feature allows customers to classify traffic matching certain criteria and then configure the system to unconditionally discard any packets matching that criteria. The Modular QoS CLI (MQC) Unconditional Packet Discard feature is configured using the Modular Quality of Service Command-Line Interface (MQC) feature. Packets are unconditionally discarded by using the new **drop** command within the MQC.

- [Benefits, page 60](#)
- [Restrictions, page 60](#)
- [Related Features and Technologies, page 60](#)
- [Related Documents, page 60](#)

Benefits

Enhanced System Utilization

This feature allows you to discard (drop), without any further system processing, the packets of a particular class. This function is very useful when you want to discard all the packets for nonessential applications (for instance, Internet browsing applications or unauthorized video applications) and allocate system resources to more essential applications. This feature allows the user to discard those nonessential packets and simultaneously obtain the bit and drop rate statistics for that particular class and the traffic within that class. The statistics are gathered through the CISCO-CLASS-BASED-QOS-MIB.

Restrictions

Packets are unconditionally discarded by configuring the drop action inside a traffic class (inside of a policy map). This drop action is accomplished with the new **drop** command. Note the following restrictions for configuring the drop action within a traffic class:

- The discarding action is the only action that can be configured in a traffic class. That is, no other actions can be configured in the traffic class.
- When a traffic class is configured with the **drop** command, a "child" (nested) policy cannot be configured for this specific traffic class through the **service policy** command.
- The discarding action cannot be configured for the default class known as the class-default class.

Related Features and Technologies

- Modular quality of service command-line interface (MQC)

Related Documents

- "Applying QoS Features Using the MQC" module
- "Classifying Network Traffic" module
- "Marking Network Traffic" module
- Cisco IOS Quality of Service Solutions Command Reference

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

Configuration Tasks

- [Configuring the Class Map, page 61](#)
- [Creating a Policy Map, page 62](#)
- [Attaching the Policy Map to an Interface or a VC, page 63](#)
- [Verifying the Discard Action Configuration in the Traffic Class, page 64](#)

Configuring the Class Map

SUMMARY STEPS

1. Router(config)# **class-map***class-map-name*
2. Router(config-cmap)# **match access-group** {*access-group* | **name***access-group-name* }
3. Router(config-cmap)# **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# class-map <i>class-map-name</i>	Specifies the name of the class map to be created. If match-all or match-any is not specified, traffic must match all the match criteria to be classified as part of the traffic class. Enters class-map configuration mode.

	Command or Action	Purpose
Step 2	Router(config-cmap)# match access-group { <i>access-group</i> <i>name</i> <i>access-group-name</i> }	Specifies that traffic matching the specified access group will be placed in the map class created above. This command provides just an example of the match criterion you can specify. For more information about the additional match criteria available, see the "Applying QoS Features Using the MQC" module.
Step 3	Router(config-cmap)# exit	Exits from the configuration mode.

Creating a Policy Map

SUMMARY STEPS

1. Router (config)# **policy-map***policy-name*
2. Router (config-pmap)# **class***class-name*
3. Router (config-pmap)# **drop**
4. Router(config-cmap)# **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router (config)# policy-map <i>policy-name</i> Example:	Specifies the name of the policy map to be created. Enters policy-map configuration mode.
Step 2	Router (config-pmap)# class <i>class-name</i>	Specifies the name of the traffic class configured earlier in the Configuring the Class Map, page 61 section above. This traffic class is used to classify traffic to the policy map. Enters policy-map class configuration mode.
Step 3	Router (config-pmap)# drop	Discards the packets in the specified traffic class.
Step 4	Router(config-cmap)# exit	Exits policy-map configuration mode.

Attaching the Policy Map to an Interface or a VC

SUMMARY STEPS

1. Router(config)# **interfacetype** *number* [*name-tag*]
2. Router(config-if)# **pvc** [*name*] *vpi/vci* [**ilmi** | **qsaal** | **smds**]
3. Do one of the following:
 - Router(config-if)# **service-policy input***policy-map-name*
 -
 -
 -
4. Router(config-if)# **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# interfacetype <i>number</i> [<i>name-tag</i>] Example:	Configures the interface type and enters interface configuration mode.
Step 2	Router(config-if)# pvc [<i>name</i>] <i>vpi/vci</i> [ilmi qsaal smds]	(Optional) Creates or assigns a name to an ATM permanent virtual circuit (PVC), and specifies the encapsulation type on an ATM PVC. Enters ATM VC configuration mode (config-if-atm-vc). This step is required only if you are attaching the policy map to an ATM PVC.
Step 3	Do one of the following: <ul style="list-style-type: none"> • Router(config-if)# service-policy input<i>policy-map-name</i> • • • Example: Router(config-if-atm-vc)# service-policy output <i>policy-map-name</i> Example:	Specifies the name of the policy map to be attached to the input or output direction of an interface or VC. The policy map evaluates all traffic entering or leaving that interface or VC.

Command or Action	Purpose
Step 4 Router(config-if)# exit	Exits interface configuration mode.

Verifying the Discard Action Configuration in the Traffic Class

Command	Purpose
Router# show policy-map	Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps.
Router# show policy-map interface <i>interface-name</i>	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.

Configuration Examples

- [Example Configuring the Discard Action Configuration in a Traffic Class, page 64](#)
- [Example Verifying the Discard Action Configuration in the Policy Map, page 64](#)

Example Configuring the Discard Action Configuration in a Traffic Class

In the following sample configuration, a traffic class called "class1" has been created and configured for use in a policy-map called "policy1." The policy-map policy1 is attached to an output serial interface 2/0. All packets matching access-group 101 are placed in a class called "c1." Packets belonging to this class are discarded.

```
Router(config)# class-map class1
Router(config-cmap)# match access-group 101
Router(config-cmap)# policy-map policy1
Router(config-pmap)# class c1
Router(config-pmap-c)# drop
Router(config-pmap-c)# interface s2/0
Router(config-if)# service-policy output policy1
Router(config-if)# exit
```

The following sample output of the **show policy-map** command displays the contents of the policy map called "policy1." All the packets belonging to the class called "c1" are discarded.

```
Router# show policy-map policy1
Policy Map policy1
Class c1
drop
```

Example Verifying the Discard Action Configuration in the Policy Map

The following sample output of the **show policy-map interface** command displays the statistics for the Serial2/0 interface, to which a policy map called "policy1" is attached. The discard action has been

specified for all the packets belonging to a class called "c1." In this example, 32000 bps of traffic is sent ("offered") to the class and all of them are dropped. Therefore, the drop rate shows 32000 bps.

```
Router# show policy-map interface
Serial2/0
Service-policy output: policy1
Class-map: c1 (match-all)
  10184 packets, 1056436 bytes
  5 minute offered rate 32000 bps, drop rate 32000 bps
Match: ip precedence 0
drop
```

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

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



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 Cisco IOS 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, page 67](#)
- [Prerequisites for Control Plane Policing, page 67](#)
- [Restrictions for Control Plane Policing, page 67](#)
- [Information About Control Plane Policing, page 69](#)
- [How to Use Control Plane Policing, page 75](#)
- [Configuration Examples for Control Plane Policing, page 81](#)
- [Additional References, page 82](#)
- [Feature Information for Control Plane Policing, page 83](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see 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 document.

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 Control Plane Policing

The Modular Quality of Service (QoS) Command-Line interface (CLI) (MQC) is used to configure the packet classification and policing functionality of the Control Plane Policing feature.

Before configuring Control Plane Policing (CoPP), you should understand the procedures for using the MQC. For information about the MQC, see the "Applying QoS Features Using the MQC" module.

Restrictions for Control Plane Policing

Aggregate and Distributed Control Plane Policing

Aggregate policing is supported in Cisco IOS Release 12.0(29)S, Cisco IOS Release 12.2(18)S, Cisco IOS Release 12.3(4)T, and later releases.

Distributed policing is supported only in Cisco IOS Release 12.0(30)S and later Cisco IOS 12.0S releases.

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](#), page 75.

Output rate-limiting (policing) in silent mode is supported only in:

- Cisco IOS Release 12.2(25)S and later Cisco IOS 12.2S releases
- Cisco IOS Release 12.3(4)T and later Cisco IOS 12.3T releases

Output rate-limiting is not supported for distributed control plane services in Cisco IOS 12.0S releases or in Cisco IOS 12.2SX releases.

Output rate-limiting is not supported on the Cisco 7500 series and Cisco 10720 Internet router.

MQC Restrictions

The Control Plane Policing feature requires the MQC to configure packet classification and policing. All restrictions that apply when you use the MQC to configure policing also apply when you configure control plane policing. Only two MQC actions are supported in policy maps--**police** and **drop**.



Note

On the Cisco 10720 Internet router, only the **police** command, not the **drop** command, is supported in policy maps. In addition, in a QoS service policy that is attached to the Cisco 10720 control plane, the **police** command does not support **set** actions as arguments in **conform-action**, **exceed-action**, and **violate-action** parameters.

Features that require Network-Based Application Recognition (NBAR) classification may not work well at the control plane level. The following classification (match) criteria are supported on all platforms:

- Standard and extended IP access lists (ACLs).
- In class-map configuration mode: **match ip dscp**, **match ip precedence**, and **match protocol arp**, and **match protocol pppoe** commands.



Note

In the Cisco IOS 12.2SX release, the **match protocol arp** command is not supported.

On the Cisco 10720 Internet router, the following MQC commands are also supported in class-map configuration mode: **match input-interface**, **match mpls experimental**, **match protocol ipv6**, and **match qos-group**. When using these commands for control plane policing on the Cisco 10720 Internet router, note the following restrictions:

- Packet classification using match criteria is not supported for packets that cannot be classified in the Cisco 10720 data path, such as unknown Layer 2 encapsulation and IP options.
- The following IPv6 fields are not supported in packet classification for IPv6 QoS on the Cisco 10720 Internet router and are, therefore, not supported for control plane policing:
 - IPv6 source and destination addresses

- Layer 2 class of service (CoS)
- IPv6 routing header flag
- IPv6 undetermined transport flag
- IPv6 flow label
- IP Real-Time transport Protocol (RTP)

**Note**

Packets that are not supported for QoS packet classification on the Cisco 10720 Internet router are not policed in the default traffic class for control plane policing.

CISCO-CLASS-BASED-QOS-MIB Control Plane Support

In Cisco IOS Release 12.3(7)T and later Cisco IOS 12.3T releases, the CISCO-CLASS-BASED-QOS-MIB is extended to manage control plane QoS policies and provide information about the control plane.

Cisco IOS Release 12.2(18)SXD1

In Cisco IOS Release 12.2(18)SXD1 and later releases, Hardware Control Plane Interface for Control Plane Policing has the following restrictions:

- Supported only with Supervisor Engine 720. Not supported with Supervisor Engine 2.
- Does not support CoPP output rate-limiting (policing).
- Does not support the CoPP silent operation mode.
- Cisco IOS Release 12.2(18)SXD1 and later releases automatically install the CoPP service policy on all DFC-equipped switching modules.

For more information about control plane policing in Cisco IOS Release 12.2(18)SXD1 and later releases, see either of these publications:

- For Catalyst 6500 series switches, see the "Configuring Control Plane Policing (CoPP)" module.
- For Cisco 7600 series routers, see the "Configuring Denial of Service Protection" module.

Information About Control Plane Policing

- [Benefits of Control Plane Policing, page 69](#)
- [Terms to Understand, page 70](#)
- [Control Plane Security and Packet QoS Overview, page 71](#)
- [Aggregate Control Plane Services, page 72](#)
- [Distributed Control Plane Services, page 73](#)
- [Usage of Distributed CP Services, page 74](#)
- [Output Rate-Limiting and Silent Mode Operation, page 75](#)

Benefits of Control Plane Policing

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

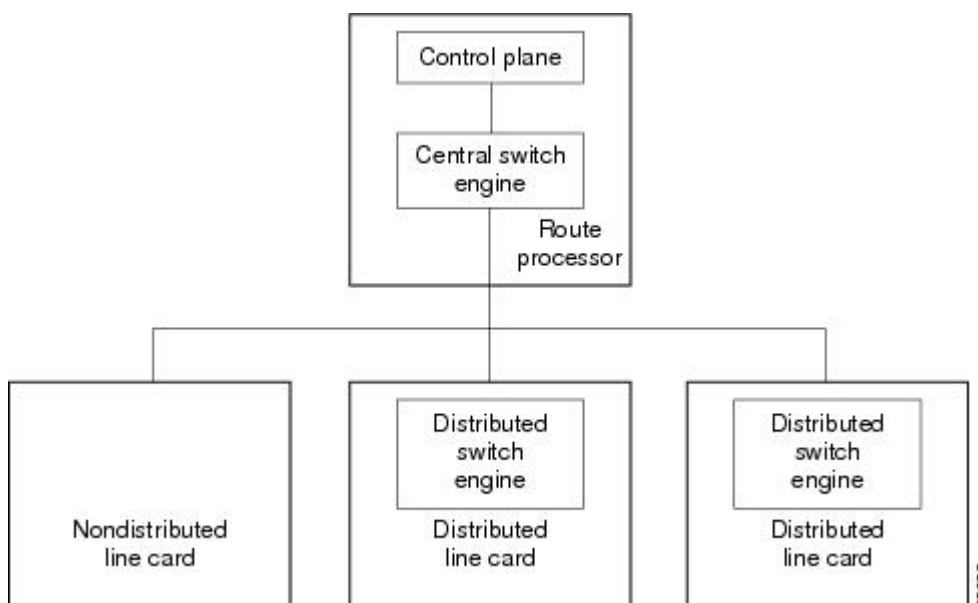
- Protection against DoS attacks at infrastructure routers and switches
- QoS control for packets that are destined to the control plane of Cisco routers or switches

- Ease of configuration for control plane policies
- Better platform reliability and availability

Terms to Understand

Because different platforms can have different architectures, the following set of terms is defined. The figure below illustrates how control plane policing works.

Figure 2 *Layout of Control Plane, Central Switch Engine, Distributed Switch Engines, and Line Cards on a Router*



- Control plane (CP)--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 functions.
- Central switch engine--A device that is responsible for high-speed routing of IP packets. It also typically performs high-speed input and output services for nondistributed interfaces. (See nondistributed line cards.) The central switch engine is used to implement aggregate CP protection for all interfaces on the router.



Note

All IP packets that are destined for the CP should pass through the central switch engine before they are forwarded to the process level.

On the Cisco 10720 Internet router, control plane policing is implemented on Cisco Parallel eXpress Forwarding (PXF) in a Toaster-based architecture. PXF is a hardware-based central switch engine that can filter traffic at a higher rate than the route processor. PXF switches all data traffic separately from the route processor. PXF packet processing occurs at an intermediate step between the nondistributed line cards and the route processor shown in the figure above. In addition to the regular punting, PXF also punts certain types of packets (such as unknown Layer 2 encapsulation and packets with IP options) to the RP for further processing at interrupt level.

**Note**

On the Cisco 10720 Internet router, you can configure enhanced RP protection by using the **ip option drop** command to drop IPv4 packets with IP options that are punted to the RP by PXF. Tunneled IPv4 packets and IPv4 packets with an unsupported encapsulation method are not dropped. For more information, see the "ACL IP Options Selective Drop" module.

- Distributed switch engine--A device that is responsible for high-speed switching of IP packets on distributed line cards without using resources from the central switch engine. It also typically performs input and output services for the line card. Each distributed switch engine is used to implement distributed CP services for all ports on a line card. Input CP services distribute the processing load across multiple line cards and conserve vital central switch engine resources. Distributed CP services are optional; however, they provide a more refined level of service than aggregate services.
- Nondistributed line cards--Line cards that are responsible for receiving packets and occasionally performing input and output services. All packets must be forwarded to the central switch engine for a routing or switching decision. Aggregate CP services provide coverage for nondistributed line cards.

**Note**

Distributed CP services are supported only in Cisco IOS Release 12.0(30)S and later 12.0S releases.

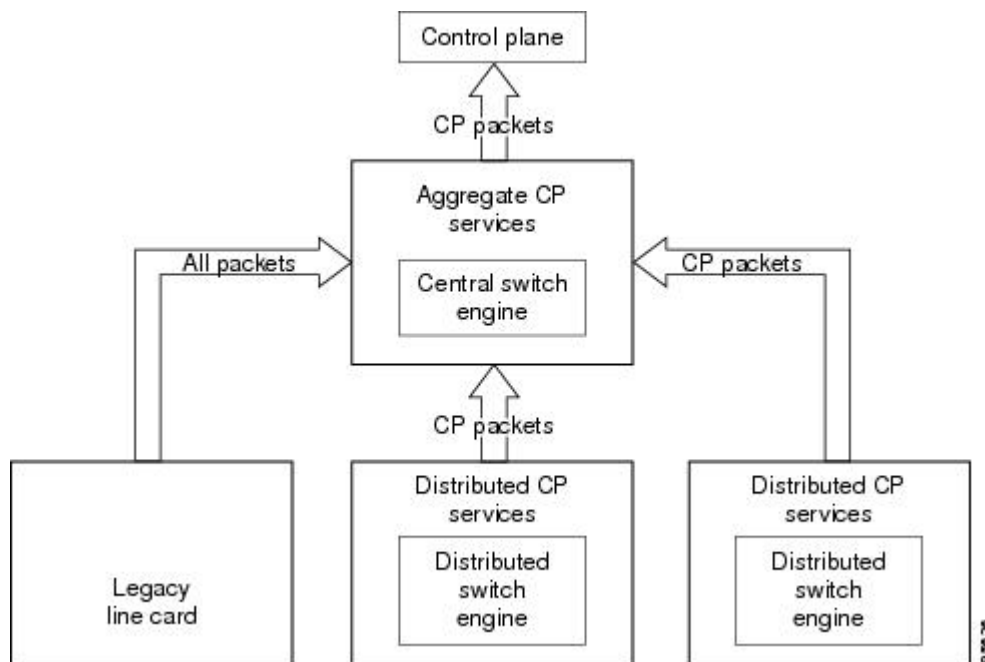
Control Plane Security and Packet QoS Overview

To protect the CP on a router from DoS attacks and to provide packet QoS, the Control Plane Policing feature treats the CP as a separate entity with its own ingress (input) and egress (output) ports, which are like ports on a router and switch. Because the Control Plane Policing feature treats the CP as a separate entity, a set of rules can be established and associated with the ingress and egress ports of the CP.

These rules are applied only after the packet has been determined to have the CP as its destination or when a packet exits the CP. Thereafter, you can configure a service policy 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 CP to a maximum rate of 1 megabit per second.

Input CP services are executed after router input port services have been performed and after a routing decision on the input path has been made. As shown in the figure below, CP security and packet QoS are applied on:

Figure 3 *Input Control Plane Services: Aggregate and Distributed Services*



The following types of Layer 3 packets are forwarded to the control plane and processed by aggregate and distributed control plane policing:

- Routing protocol control packets
- Packets destined for the local IP address of the router
- Packets from management protocols (such as Simple Network Management Protocol [SNMP], Telnet, and secure shell [SSH])



Note

Ensure that Layer 3 control packets have priority over other packet types that are destined for the control plane.

Aggregate Control Plane Services

Aggregate control plane services provide control plane policing for all CP packets that are received from all line-card interfaces on the router.

The central switch engine executes normal input port services and makes routing decisions for an incoming packet: if the packet is destined for the CP, aggregate services are performed. Because CP traffic from all line cards must pass through aggregate CP services, these services manage the cumulative amount of CP traffic that reaches the CP.

Aggregate CP service steps are as follows:

- 1 The line card receives a packet and delivers it to the central switch engine.

**Note**

Before the packet is sent to the central switch engine, additional processing may be necessary for platforms that support hardware-level policing or platform-specific aggregate policing. It is possible that the packet may undergo multiple checks before it undergoes the generic Cisco IOS check.

- 1 The interfaces perform normal (interface-level) input port services and QoS.
- 2 The central switch engine performs Layer 3 switching or makes a routing decision, determining whether or not the packet is destined for the CP.
- 3 The central switch engine performs aggregate CP services for all CP packets.
- 4 On the basis of the results of the aggregate CP services, the central switch engine either drops the packet or delivers the packet to the CP for final processing.

Functionality Highlights of Aggregate CP Services

The following list highlights the functionality of aggregate CP services:

- Aggregate CP services are defined for a single input interface, such as the CP, and represent an aggregate for all ports on a router.
- Modular QoS is used to define CP services. Class maps and policy maps for both DoS protection and packet QoS are defined for a single aggregate CP service policy.
- Modular QoS does not prevent a single bad port from consuming all allocated bandwidth. Class maps that match an interface or subinterface may be able to constrain the contribution of each interface through an interface-specific policy map.

Distributed Control Plane Services

Distributed control plane services provide control plane policing for all CP packets that are received from the interfaces on a line card.

A distributed switch engine executes normal input port services and makes routing decisions for a packet: if the packet is destined for the CP, distributed CP services are performed. Afterwards, CP traffic from each line card is forwarded to the central switch engine where aggregate CP services are applied.

**Note**

Distributed CP services may also forward conditioned packets to the central switch engine. In this case, aggregate CP services are also performed on the conditioned CP traffic.

Distributed CP service steps are as follows:

- 1 A line card receives a packet and delivers it to the distributed switch engine.
- 2 The distributed switch engine performs normal (interface-level) input port services and QoS.
- 3 The distributed switch engine performs Layer 2 or Layer 3 switching or makes a routing decision, determining whether the packet is destined for the CP.
- 4 The distributed switch engine performs distributed CP services for all CP packets.
- 5 On the basis of the results of the distributed CP services, the distributed switch engine either drops the packet or marks the packet and delivers it to the central switch engine for further processing.
- 6 The central switch engine performs aggregate CP services and delivers the packet to the CP for final processing.

Functionality Highlights of Distributed CP Services

The following list highlights the functionality of distributed CP services:

- Distributed CP services are defined for a single input interface, such as the distributed CP, and represent an aggregate for all ports on a line card.
- The MQC is used to define CP services. Class maps and policy maps for both DoS protection and packet QoS are defined for a single distributed CP service policy. Each line card may have a unique CP service policy that applies traffic classifications, QoS policies, and DoS services to packets received from all ports on the line card in an aggregate way.
- The MQC does not prevent one bad port from consuming all allocated bandwidth on a line card. Class maps that match an interface or subinterface may be able to constrain the contribution of each interface through an interface-specific policy map.
- Distributed CP services allow you to limit the number of CP packets forwarded from a line card to the central switch engine. The total number of CP packets received from all line cards on a router may exceed aggregate CP levels.

Usage of Distributed CP Services

The purpose of CP protection and packet QoS is to apply sufficient control to the packets that reach the control plane. To successfully configure this level of CP protection, you must:

- Apply traditional QoS services using the MQC to CP packets.
- Protect the path to the control plane against indiscriminate packet dropping due to resource exhaustion. If packets are not dropped according to user-defined QoS policies, but are dropped due to a resource limitation, the QoS policy is not maintained.

Distributed CP services allow you to configure specific CP services that are enforced at the line-card level and are required for the following reasons:

- While under a DoS attack, line-card resources may be consumed. In this case, you must configure a drop policy to identify important packets. The drop policy ensures that all important packets arrive to the central switch engine for aggregate CP protection and arrive later to the CP. Distributed CP services allow routers to apply the appropriate drop policy when resources are consumed and therefore maintain the desired QoS priorities. If a line card indiscriminately drops packets, the aggregate CP filter becomes ineffective and the QoS priorities are no longer maintained.
- It is not possible to prevent one interface from consuming all aggregate CP resources. A DoS attack on one port may negatively impact CP processing of traffic from other ports. Distributed CP services allow you to limit the amount of important traffic that is forwarded by a line card to the CP. For example, you can configure a layered approach in which the combined rates of all line cards are over-subscribed compared to the aggregate rate. The rate of each individual line card would be below the aggregate rate, but combined together, the rates of all line cards exceed it. This over-subscription model is commonly used for other resource-related functions and helps limit the contribution of CP packets from any one line card.
- Distributed CP services provide for slot-level (line-card) filtering. Customer-facing interfaces may have greater security requirements (with more restrictions or for billing reasons) than network-facing interfaces to backbone devices.
- Because distributed CP protection allows you to configure packet filters on a per-line-card basis, processing cycles on line cards may offload aggregate level processing. You can configure Border Gateway Protocol (BGP) filtering at the distributed level for interfaces that use BGP, allowing the aggregate level to filter packets with the remaining filter requirements. Or you can configure identical filters for distributed and aggregate CP services with a distributed packet marking scheme that informs

the aggregate filter that a packet has already been checked. Distributed CP service processing further reduces aggregate processing and can significantly reduce the load on aggregate CP services.

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 CP is performed in silent mode. In silent mode, a router that is running Cisco IOS 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.

When control plane policing is configured for output traffic, error messages are not generated in the following cases:

- Traffic that is being transmitted to a port to which the router is not listening
- A connection to a legitimate address and port that is rejected because of a malformed request

The silent mode functionality and output policing on CP traffic are supported only in:

- Cisco IOS Release 12.2(25)S and later Cisco IOS 12.2S releases
- Cisco IOS Release 12.3(4)T and later Cisco IOS 12.3T releases

Silent mode and output policing on CP traffic are not supported for distributed control plane services.

How to Use Control Plane Policing

- [Defining Aggregate Control Plane Services, page 75](#)
- [Defining Distributed Control Plane Services, page 77](#)
- [Verifying Aggregate Control Plane Services, page 78](#)
- [Verifying Distributed Control Plane Services, page 79](#)

Defining Aggregate Control Plane Services

To configure aggregate CP services, such as packet rate control and silent packet discard, for the active route processor, complete the following steps.

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.
- Support for output policing is available only in Cisco IOS Release 12.3(4)T and later T-train releases. (Note that 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
<p>Step 1 enable</p> <p>Example:</p> <pre>Router> enable</pre>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> • Enter your password if prompted.
<p>Step 2 configure terminal</p> <p>Example:</p> <pre>Router# configure terminal</pre>	<p>Enters global configuration mode.</p>
<p>Step 3 control-plane</p> <p>Example:</p> <pre>Router(config)# control-plane</pre>	<p>Enters control-plane configuration mode (a prerequisite for Defining Aggregate Control Plane Services, page 75).</p>
<p>Step 4 service-policy {input output <i>policy-map-name</i></p> <p>Example:</p> <pre>Router(config-cp)# service-policy input control-plane-policy</pre>	<p>Attaches a QoS service policy to the control plane. Note the following points:</p> <ul style="list-style-type: none"> • 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 router to silently discard packets. • <i>policy-map-name</i> --Name of a service policy map (created using the policy-map command) to be attached. The name can be a maximum of 40 alphanumeric characters.
<p>Step 5 end</p> <p>Example:</p> <pre>Router(config-cp)# end</pre>	<p>(Optional) Returns to privileged EXEC mode.</p>

Defining Distributed Control Plane Services

To configure distributed CP services, such as packet rate control, for packets that are destined for the CP and sent from the interfaces on a line card, complete the following steps.

Before you enter control-plane configuration mode to attach an existing QoS policy for performing distributed control-plane services, 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.
- Support for output policing is available only in Cisco IOS Release 12.3(4)T and later T-train releases. (Note that output policing does not provide any performance benefits. It simply controls the information that is leaving the device.)
- With Cisco IOS 12.2SX releases, the Supervisor Engine 720 automatically installs the service policy on all DFC-equipped switching modules.

>

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **control-plane** [slot *slot-number*]
4. **service-policy input** *policy-map-name*
5. **end**

DETAILED STEPS

Command or Action	Purpose
Step 1 enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2 configure terminal Example: Router# configure terminal	Enters global configuration mode.

Command or Action	Purpose
<p>Step 3 <code>control-plane [slot slot-number]</code></p> <p>Example:</p> <pre>Router(config)# control-plane slot 3</pre>	<p>Enters control-plane configuration mode, which allows you to optionally attach a QoS policy (used to manage CP traffic) to the specified slot.</p> <ul style="list-style-type: none"> Enter the slot keyword and the slot number, as applicable.
<p>Step 4 <code>service-policy input policy-map-name</code></p> <p>Example:</p> <pre>Router(config-cp)# service-policy input control-plane-policy</pre>	<p>Attaches a QoS policy map to filter and manage CP traffic on a specified line card before the aggregate CP policy is applied. Note the following points:</p> <ul style="list-style-type: none"> input --Applies the specified policy map using the distributed switch engine to CP packets that are received from all interfaces on the line card. policy-map-name --Name of a service policy map (created using the policy-map command) to be attached. The name can be a maximum of 40 alphanumeric characters. <p>Note The service-policy output policy-map-name command is not supported for applying a QoS policy map for distributed control plane services.</p>
<p>Step 5 <code>end</code></p> <p>Example:</p> <pre>Router(config-cp)# end</pre>	<p>(Optional) Returns to privileged EXEC mode.</p>

Verifying Aggregate Control Plane Services

To display information about the service policy attached to the control plane for aggregate CP services, complete the following steps.

SUMMARY STEPS

- `enable`
- `show policy-map control-plane [all] [input [class class-name] | output [class class-name]]`
- `exit`

DETAILED STEPS

Command or Action	Purpose
<p>Step 1 <code>enable</code></p> <p>Example:</p> <pre>Router> enable</pre>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> Enter your password if prompted.

Command or Action	Purpose
<p>Step 2 <code>show policy-map control-plane [all] [input [class <i>class-name</i>] output [class <i>class-name</i>]]</code></p> <p>Example:</p> <pre>Router# show policy-map control-plane all</pre>	<p>Displays information about the control plane. Note the following points:</p> <ul style="list-style-type: none"> • all --(Optional) Service policy information about all QoS policies used in aggregate and distributed CP services. • input --(Optional) Statistics for the attached input policy. • output --(Optional) Statistics for the attached output policy. • class <i>class-name</i> --(Optional) Name of the traffic class whose configuration and statistics are displayed.
<p>Step 3 <code>exit</code></p> <p>Example:</p> <pre>Router(config-cp)# exit</pre>	<p>(Optional) Exits privileged EXEC mode.</p>

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.

```
Router# 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
```

Verifying Distributed Control Plane Services

To display information about the service policy attached to the control plane to perform distributed CP services, complete the following steps.

SUMMARY STEPS

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

DETAILED STEPS

Command or Action	Purpose
<p>Step 1 <code>enable</code></p> <p>Example:</p> <pre>Router> enable</pre>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> Enter your password if prompted.
<p>Step 2 <code>show policy-map control-plane [all][slot slot-number] [input [class class-name] output [class class-name]]</code></p> <p>Example:</p> <pre>Router# show policy-map control-plane slot 2</pre>	<p>Displays information about the service policy used to apply distributed CP services on the router. Note the following points:</p> <ul style="list-style-type: none"> all --(Optional) Service policy information about all QoS policies used in aggregate and distributed CP services. slot slot-number --(Optional) Service policy information about the QoS policy map used to perform distributed CP services on the specified line card. input --(Optional) Statistics for the attached input policy map. output --(Optional) Statistics for the attached output policy map. class class-name --(Optional) Name of the traffic class whose configuration and statistics are displayed.
<p>Step 3 <code>exit</code></p> <p>Example:</p> <pre>Router# exit</pre>	<p>(Optional) Exits privileged EXEC mode.</p>

Examples

The following example shows how to display information about the classes of CP traffic received from all interfaces on the line card in slot 1 to which the policy map TESTII is applied for distributed CP services. This policy map polices traffic that matches the traffic class TESTII, while allowing all other traffic (that matches the class map "class-default") to go through as is.

```
Router# show policy-map control-plane slot 1
Control Plane - slot 1
Service-policy input: TESTII (1048)
Class-map: TESTII (match-all) (1049/4)
  0 packets, 0 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
  Match: protocol arp (1050)
  police:
    cir 8000 bps, bc 4470 bytes, be 4470 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) (1052/0)
  0 packets, 0 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
  Match: any (1053)
```


Configuration Examples for Control Plane Policing

This section contains examples that shows how to configure aggregate control plane services on both an input and an output interface:

- [Example Configuring Control Plane Policing on Input Telnet Traffic, page 81](#)
- [Example Configuring Control Plane Policing on Output ICMP Traffic, page 81](#)

Example Configuring Control Plane Policing on Input Telnet Traffic

The following example shows how to apply a QoS policy for aggregate CP 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.
Router(config)# access-list 140 deny tcp host 10.1.1.1 any eq telnet

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

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

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

Example Configuring Control Plane Policing on Output ICMP Traffic

The following example shows how to apply a QoS policy for aggregate CP 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.
Router(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.
Router(config)# access-list 141 deny icmp 10.0.0.1 0.0.0.255 any port-unreachable

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

```

Router(config-cmap)# match access-group 141
Router(config-cmap)# exit
Router(config)# policy-map control-plane-out
! Drop all traffic that matches the class "icmp-class."
Router(config-pmap)# class icmp-class
Router(config-pmap-c)# drop
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# control-plane
! Define aggregate control plane service for the active route processor.
Router(config-cp)# service-policy output control-plane-out
Router(config-cp)# end

```

Additional References

The following sections provide references related to the Control Plane Policing feature.

Related Documents

Related Topic	Document Title
QoS commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	<i>Cisco IOS Quality of Service Solutions Command Reference</i>
QoS features overview	"Quality of Service Overview" module
MQC	"Applying QoS Features Using the MQC" module
Security features overview	"Control Plane Security Overview" module in the <i>Cisco IOS Security Configuration Guide: Securing the Control Plane</i>
Control plane policing in Cisco IOS Release 12.2(18)SXD1 and later releases	For Catalyst 6500 series switches, see the "Configuring Control Plane Policing (CoPP)" module. For Cisco 7600 series routers, see the "Configuring Denial of Service Protection" module.
Enhanced RP protection	"ACL IP Options Selective Drop" 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
<ul style="list-style-type: none"> CISCO-CLASS-BASED-QOS-MIB <p>Note Supported only in Cisco IOS Release 12.3(7)T.</p>	<p>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</p>

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 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 3 *Feature Information for Control Plane Policing*

Feature Name	Releases	Feature Information
Control Plane Policing	12.2(18)S 12.3(4)T 12.3(7)T 12.0(29)S 12.2(18)SXD1 12.0(30)S 12.2(27)SBC 12.0(32)S 12.3(31)SB2 15.0(1)S	<p>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.</p> <p>For Release 12.2(18)S, this feature was introduced.</p> <p>For Release 12.3(4)T, this feature was integrated into Cisco IOS Release 12.3(4)T, and the output rate-limiting (silent mode operation) feature was added.</p> <p>For Release 12.3(7)T, the CISCO-CLASS-BASED-QOS-MIB was extended to manage control plane QoS policies, and the police rate command was introduced to support traffic policing on the basis of packets per second for control plane traffic.</p> <p>For Release 12.0(29)S, this feature was integrated into Cisco IOS Release 12.0(29)S.</p> <p>For Release 12.2(18)SXD1, this feature was integrated into Cisco IOS Release 12.2(18)SXD1.</p> <p>For Release 12.0(30)S, this feature was modified to include support for distributed control plane services on the Cisco 12000 series Internet router.</p> <p>For Release 12.2(27)SBC, this feature was integrated into Cisco IOS Release 12.2(27)SBC.</p> <p>For Release 12.0(32)S, this feature was modified to include support for aggregate control plane services on the Cisco 10720 Internet router.</p> <p>For Release 12.3(31)SB2, this feature was implemented on the</p>

Feature Name	Releases	Feature Information
		<p>Cisco 10000 series router for the PRE3.</p> <p>For Release 15.0(1)S, this feature was integrated into Cisco IOS Release 15.0(1)S.</p>

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

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

