



Traffic Policing

This feature module describes the Traffic Policing feature. It includes information on the benefits of the feature, supported platforms, related documents, and so forth.

For complete conceptual information, see the “[Policing and Shaping Overview](#)” module.

For a complete description of the Traffic Policing commands mentioned in this module, refer to the *Cisco IOS Quality of Service Solutions Command Reference*. To locate documentation of other commands that appear in this module, use the command reference master index or search online.

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

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.

Contents

This document includes the following sections:

- [Feature Overview](#), page 2
- [Supported Platforms](#), page 4
- [Supported Standards, MIBs, and RFCs](#), page 4
- [Prerequisites](#), page 5
- [Configuration Tasks](#), page 5
- [Monitoring and Maintaining Traffic Policing](#), page 6
- [Configuration Examples](#), page 6
- [Command Reference](#), page 7
- [Glossary](#), page 8



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

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.

Traffic policing allows you to control the maximum rate of traffic transmitted or received on an interface. 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 Command-Line Interface (CLI) (MQC). For information about the MQC, see the [“Applying QoS Features Using the MQC”](#) module.

Table 1 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

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

Related Features and Technologies

- Modular Quality of Service Command-Line Interface
- Class-Based Weighted Fair Queueing (CBWFQ)
- Class-Based Marking

Related Documents

- [“Applying QoS Features Using the MQC”](#) module
- [“Configuring Committed Access Rate”](#) module
- [“Marking Network Traffic”](#) module
- [“Configuring Weighted Fair Queueing”](#) module
- [Cisco IOS Quality of Service Solutions Command Reference](#)

Supported Platforms

- Cisco 2500 series



Note

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

- 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.

For additional information on CEF, see the [“Cisco Express Forwarding Features Roadmap”](#) module.

Configuration Tasks

See the following sections for configuration tasks for the Traffic Policing feature. Each task in the list indicates if the task is optional or required.

- [Configuring Traffic Policing](#) (Required)

Configuring Traffic Policing

To successfully configure the Traffic Policing feature, a traffic class and a traffic policy must be created, and the traffic policy must be attached to a specified interface. These tasks are performed using the MQC. For information about the MQC, see the [“Applying QoS Features Using the MQC”](#) module.

The Traffic Policing feature is configured in the traffic policy. To configure the Traffic Policing feature, use the following command in policy map configuration mode:

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

For more information about the **police** command, see the [Cisco IOS Quality of Service Solutions Command Reference](#).

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.

For more information about token bucket mechanisms, see the [“Policing and Shaping Overview”](#) module.

Troubleshooting Tips

- Check the interface type. Verify that your interface is not mentioned in the nonsupported interface description in the “[Restrictions](#)” 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

To monitor and maintain the Traffic Policing feature, use the following commands in EXEC mode, as needed:

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.

For more information about the **show policy-map** and **show policy-map interface** commands and how to interpret the information displayed, see the [Cisco IOS Quality of Service Solutions Command Reference](#).

Configuration Examples

This section provides the following configuration example:

- [Configuring a Service Policy that Includes Traffic Policing: Example, page 6](#)

Configuring a Service Policy that Includes Traffic Policing: Example

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.

For additional information on configuring traffic classes and traffic policies, see the “[Applying QoS Features Using the MQC](#)” module.

In this particular example, traffic policing is configured with the average rate at 8000 bits per second, the normal burst size at 2000 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 specified parameters. Packets that conform are transmitted, packets that exceed are assigned a QoS group value of 4 and are transmitted, and packets that violate are dropped.

For more information about token bucket mechanisms, see the [“Policing and Shaping Overview”](#) module.

```
Router(config)# class-map acgroup2
Router(config-cmap)# match access-group 2
Router(config-cmap)# exit
Router(config)# policy-map police
Router(config-pmap)# class acgroup2
Router(config-pmap-c)# police 8000 2000 4000 conform-action transmit exceed-action
set-qos-transmit 4 violate-action drop
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface fastethernet 0/0
Router(config-if)# service-policy input police
```

Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Quality of Service Solutions Command Reference* at http://www.cisco.com/en/US/docs/ios/qos/command/reference/qos_book.html. For information about all Cisco IOS commands, use the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or a Cisco IOS master commands list.

- **police**
- **show policy-map**
- **show policy-map interface**

Glossary

average rate—Maximum long-term average rate of conforming traffic.

conform action—Action to take on packets with a burst size below the rate allowed by the rate limit.

DSCP—differentiated services code point

exceed action—Action to take on packets that exceed the rate limit.

excess burst size—Bytes allowed in a burst before all packets will exceed the rate limit.

normal burst size—Bytes allowed in a burst before some packets will exceed the rate limit. Larger bursts are more likely to exceed the rate limit.

QoS group—Internal QoS group ID for a packet used to determine weighted fair queuing characteristics for that packet.

policing policy—Rate limit, conform actions, and exceed actions that apply to traffic matching a certain criteria.

Versatile Interface Processor (VIP)—Interface card used by Cisco 7500 series and Cisco 7000 series with RSP7000 routers.

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Pulse, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, and Flip Gift Card are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Fast Step, Follow Me Browsing, FormShare, GainMaker, GigaDrive, HomeLink, iLYNX, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website 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. (0908R)

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

© 2007 Cisco Systems, Inc. All rights reserved.