



# Configuring Traffic Policing

---

## Feature History

Release	Modification
Cisco IOS	For information about feature support in Cisco IOS software, use Cisco Feature Navigator.

This module describes the tasks for configuring the Traffic Policing feature.

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.

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.

## Traffic Policing Configuration Task List

To configure the Traffic Policing feature, perform the tasks described in the following sections. The task in the first section is required; the tasks in the remaining section are optional.

- [Configuring Traffic Policing](#) (Required)
- [Monitoring and Maintaining Traffic Policing](#) (Optional)

See the end of this module for the section [“Traffic Policing Configuration Examples.”](#)

## 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 Modular Quality of Service (QoS) Command-Line Interface (CLI) (MQC). For information about the MQC, see the [“Applying QoS Features Using the MQC”](#) module.



---

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

© 2007 Cisco Systems, Inc. All rights reserved.

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

Command	Purpose
Router(config-pmap-c)# <b>police</b> <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. The <b>police</b> command polices traffic based on a token bucket algorithm. The variables in the token bucket algorithm are set in this command line.

The command syntax of the **police** command allows you to specify the action to be taken on a packet when you enable the *action* keyword. The resulting action corresponding to the keyword choices are listed in [Table 12](#).

**Table 12** *police Command Action Keywords*

Keyword	Resulting Action
<i>drop</i>	Drops the packet.
<b>set-prec-transmit</b> <i>new-prec</i>	Sets the IP precedence and sends the packet.
<b>set-qos-transmit</b> <i>new-qos</i>	Sets the QoS group and sends the packet.
<b>set-dscp-transmit</b> <i>new-dscp</i>	Sets the differentiated services code point (DSCP) value and sends the packet.
<b>transmit</b>	Sends the packet.

For more information about the **police** command, refer to 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 a description of a single token bucket algorithm and an explanation of how it works, see the “[Policing and Shaping Overview](#)” module.

## Verifying the Traffic Policing Configuration

To verify that the Traffic Policing feature is configured on your interface, use the following command in EXEC mode:

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

## 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# <b>show policy-map</b>	Displays all configured traffic policies.
Router# <b>show policy-map</b> <i>policy-map-name</i>	Displays the user-specified traffic policy.
Router# <b>show policy-map interface</b>	Displays statistics and configurations of all input and output policies 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, refer to the [Cisco IOS Quality of Service Solutions Command Reference](#).

## Traffic Policing Configuration Examples

The following section provides an Traffic Policing configuration example:

- [Traffic Policy that Includes Traffic Policing: Example, page 3](#)

For information on how to configure the Traffic Policing feature, see the section “[Traffic Policing Configuration Task List](#)” in this module.

### Traffic Policy that Includes Traffic Policing: Example

The following configuration example 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 sent, packets that exceed are assigned a QoS group value of 4 and are sent, and packets that violate are dropped.

For a description of a token bucket and an explanation of how a token bucket works, 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
```

---

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.