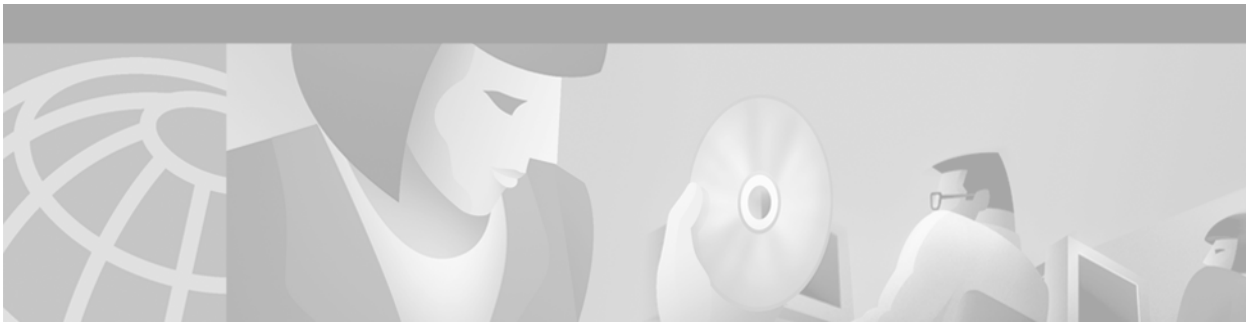

Configuring Traffic Policing

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

For complete conceptual information, see the section "Traffic Policing" in the "Policing and Shaping Overview" chapter of this book.

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

To identify the hardware platform or software image information associated with a feature, use the Feature Navigator on Cisco.com to search for information about the feature or refer to the software release notes for a specific release. For more information, see the "Identifying Supported Platforms" section in the "Using Cisco IOS Software" chapter in this book.

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)
- Verifying the Traffic Policing Configuration (Optional)
- Monitoring and Maintaining Traffic Policing (Optional)

See the end of this chapter 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 QoS Command-Line Interface (CLI). For information on the Modular QoS CLI, see the chapter "Configuring the Modular Quality of Service Command-Line Interface" in this book.

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)# police` *bps burst-normal burst-max* `conform-action` *action* `exceed-action` *action* `violate-action` *action*	Specifies a maximum bandwidth usage by a traffic class.The **police** 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
drop	Drops the packet.
set-prec-transmit *new-prec*	Sets the IP precedence and sends the packet.
set-qos-transmit *new-qos*	Sets the QoS group and sends the packet.
set-dscp-transmit *new-dscp*	Sets the differentiated services code point (DSCP) value and sends the packet.
transmit	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 "What Is a Token Bucket?" section of the"Policing and Shaping Overview" chapter of this book.

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

Traffic Policing Configuration Examples

The following sections provide Traffic Policing configuration examples:

- Traffic Policy that Includes Traffic Policing Example
- Verifying the Configuration Example

For information on how to configure the Traffic Policing feature, see the section "Traffic Policing Configuration Task List" in this chapter.

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 chapter "Configuring the Modular Quality of Service Command-Line Interface" in this book.

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 "What Is a Token Bucket?" section of the "Policing and Shaping Overview" chapter of this book.

```
7200-uut(config)# class-map acgroup2
7200-uut(config-cmap)# match access-group 2
7200-uut(config-cmap)# exit
7200-uut(config)# policy-map police
7200-uut(config-pmap)# class acgroup2
7200-uut(config-pmap-c)# police 8000 2000 4000 conform-action transmit exceed-action
set-qos-transmit 4 violate-action drop
7200-uut(config-pmap-c)# exit
7200-uut(config-pmap)# exit
7200-uut(config)# interface fastethernet 0/0
7200-uut(config-if)# service-policy input police
```

Verifying the Configuration Example

The following example verifies that the Traffic Policing feature is configured on your interface. If the feature is configured on your interface, the **show policy-map interface** command output displays policing statistics.

```
Router# show policy-map interface

 Ethernet1/7
  service-policy output: x
    class-map: a (match-all)
      0 packets, 0 bytes
      5 minute rate 0 bps
      match: ip precedence 0
      police:
        1000000 bps, 10000 limit, 10000 extended limit
        conformed 0 packets, 0 bytes; action: transmit
        exceeded 0 packets, 0 bytes; action: drop
        conformed 0 bps, exceed 0 bps, violate 0 bps
```