Policer Enhancement: Multiple Actions

First Published: 12.2(8)T
Last Updated: February 28, 2006

This document describes the Policer Enhancement: Multiple Actions feature. 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. The Policer Enhancement: Multiple Actions feature allows you to specify multiple conform, exceed, and violate actions for the marked packets.

History for the Policer Enhancement: Multiple Actions Feature

Release	Modification
12.2(8)T	This feature was introduced.
12.0(26)S	This feature was integrated into Cisco IOS Release 12.0(26)S for the 7200 and 7500 series routers.
12.2(28)SB	This feature was integrated into Cisco IOS Release 12.2(28)SB.

Finding Support Information for Platforms and Cisco IOS Software Images

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

Contents

- Feature Overview, page 2
- Prerequisites, page 3
- Configuration Tasks, page 4
- Monitoring and Maintaining the Multiple Policer Actions, page 5
- Configuration Examples, page 5

CISCO SYSTEMS

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

- Additional References, page 6
- Command Reference, page 7

Feature Overview

This feature 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. With the Policer Enhancement: Multiple Actions feature, you can specify multiple conform, exceed, and violate actions for the marked packets.

You specify the multiple actions by using the *action* argument of the **police** command. The resulting actions are listed in Table 1.

Table 1 Police Command Action Arguments

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

For more information about the **police** command and how to use it with the Policer Enhancement: Multiple Actions feature, see the Command Reference section of this document.

For more information about the Cisco IOS Traffic Policing feature, refer to the “Policing and Shaping” section of the *Cisco IOS Quality of Service Solutions Configuration Guide*, Release 12.2. See also the the Two-Rate Policer feature in Release 12.0(26)S.

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

- 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.
- 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

Prerequisites

- Before configuring the Policer Enhancement: Multiple Actions feature, you should read and understand the following:
  - *Cisco IOS Quality of Service Solutions Configuration Guide*, Release 12.2

    Specifically, the “Configuring Traffic Policing” chapter and the “Policing and Shaping Overview” chapter.
  - *Two-Rate Policer*, Cisco IOS Release 12.2(4)T feature module
- 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. For additional information on CEF or dCEF, refer to the *Cisco IOS Switching Services Configuration Guide*, Release 12.2.
- 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. These tasks are performed using the Modular QoS CLI. For information on the Modular QoS CLI, refer to the “Modular Quality of Service Command-Line Interface Overview” chapter of the *Cisco IOS Quality of Service Solutions Configuration Guide*, Release 12.2.

Configuration Tasks

See the following sections for configuration tasks for the Police Enhancement: Multiple Actions feature. Each task in the list is identified as either required or optional.

- Configuring Multiple Policer Actions (required)
- Verifying the Multiple Policer Actions Configuration (optional)

Configuring Multiple Policer Actions

To configure multiple policer actions, use the following commands beginning in global configuration mode:

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

Verifying the Multiple Policer Actions Configuration

To verify that the multiple policer actions have been configured on the interface, use the following command in EXEC or privileged EXEC mode:

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

To monitor and maintain the multiple policer actions, use the following EXEC or privileged EXEC mode commands, as needed:

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

Configuration Examples

This section provides the following configuration examples:

- Multiple Actions in a Two-Rate Policer Example
- Verifying the Multiple Policer Actions Example

Multiple Actions in a Two-Rate Policer Example

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.

Verifying the Multiple Policer Actions Example

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
```

Additional References

The following sections provide references related to Policer Enhancement: Multiple Actions.

Related Documents

Related Topic	Document Title
Quality of Service	*Cisco IOS Quality of Service Solutions Command Reference*, Release 12.3 *Cisco IOS Quality of Service Solutions Configuration Guide*, Release 12.3
Modular Quality of Service	*Modular Quality of Service Command Line Interface*
Traffic Policing	Two-Rate Policer

Standards

Standards	Title
None	—

MIBs

MIBs	MIBs Link
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://www.cisco.com/go/mibs

RFCs

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

Technical Assistance

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

Command Reference

This section documents modified commands only.

- **police**

police

To configure traffic policing, use the **police** command in policy-map class configuration mode or policy-map class police configuration mode. To remove traffic policing from the configuration, use the **no** form of this command.

police *bps* [*burst-normal*] [*burst-max*] **conform-action** *action* **exceed-action** *action* [**violate-action** *action*]

no police *bps* [*burst-normal*] [*burst-max*] **conform-action** *action* **exceed-action** *action* [**violate-action** *action*]

Syntax Description

bps	Average rate in bits per second. Valid values are 8000 to 200000000.
burst-normal	(Optional) Normal burst size in bytes. Valid values are 1000 to 51200000. The default normal burst size is 1500 bytes.
burst-max	(Optional) Excess burst size in bytes. Valid values are 1,000 to 51200000.
conform-action	Action to take on packets that conform to the rate limit.
exceed-action	Action to take on packets that exceed the rate limit.
violate-action	(Optional) Action to take on packets that violate the normal and maximum burst sizes.
action	Action to take on packets. Specify one of the following keywords: • **drop**—Drops the packet. • **set-clp-transmit** *value*—Sets the ATM Cell Loss Priority (CLP) bit from 0 to 1 on the ATM cell and transmits the packet with the ATM CLP bit set to 1. • **set-discard-class-transmit**—Sets the discard class attribute of a packet and transmits the packet with the new discard class setting. • **set-dscp-transmit** *value*—Sets the IP differentiated services code point (DSCP) value and transmits the packet with the new IP DSCP value setting. • **set-frde-transmit** *value*—Sets the Frame Relay Discard Eligibility (DE) bit from 0 to 1 on the frame relay frame and transmits the packet with the DE bit set to 1. • **set-mpls-experimental-imposition-transmit** *value*—Sets the Multiprotocol Label Switching (MPLS) experimental (EXP) bits (0 to 7) in the imposed label headers and transmits the packet with the new MPLS EXP bit value setting. • **set-mpls-experimental-topmost-transmit** *value*—Sets the MPLS EXP field value in the topmost MPLS label header at the input and/or output interfaces. • **set-prec-transmit** *value*—Sets the IP precedence and transmits the packet with the new IP precedence value setting. • **set-qos-transmit** *value*—Sets the qos-group value and transmits the packet with the new qos-group value setting. • **transmit**—Transmits the packet. The packet is not altered.

Defaults Disabled

Command Modes Policy-map class configuration (when specifying a single action to be applied to a marked packet)

Policy-map class police configuration (when specifying multiple actions to be applied to a marked packet)

Command History

Release	Modification
12.0(5)XE	This **police** command was introduced.
12.1(1)E	This command was integrated in Cisco IOS Release 12.1(1)E.
12.1(5)T	This command was integrated in Cisco IOS Release 12.1(5)T. The **violate-action** keyword was added.
12.2(2)T	The **set-clp-transmit** keyword for the *action* argument was added. The **set-frde-transmit** keyword for the *action* argument was added. However, **the set-frde-transmit** keyword is not supported for AToM traffic in this release. Also, the **set-frde-transmit** keyword is supported only when Frame Relay is implemented on a physical interface without encapsulation. The **set-mpls-exp-transmit** keyword for the *action* argument was added to the **police** command.
12.2(8)T	The command was modified for the Policer Enhancement — Multiple Actions feature. This command can now accommodate multiple actions for packets marked as conforming to, exceeding, or violating a specific rate.
12.2(13)T	In the *action* argument, the **set-mpls-experimental-transmit** keyword was renamed to **set-mpls-experimental-imposition-transmit**.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines Use the **police** command to mark a packet with different quality of service (QoS) values based on conformance to the service-level agreement.

Traffic policing will not be executed for traffic that passes through an interface.

Specifying Multiple Actions

The **police** command allows you to specify multiple policing actions. When specifying multiple policing actions when configuring the **police** command, note the following points:

- You can specify a maximum of four actions at one time.
- You cannot specify contradictory actions such as **conform-action** *transmit* and **conform-action** *drop*.

Using the police Command with the Traffic Policing Feature

The **police** command can be used with the Traffic Policing feature. The Traffic Policing feature works with a token bucket algorithm. Two types of token bucket algorithms are in Cisco IOS Release 12.1(5)T: 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.

The token bucket algorithm for the **police** command that was introduced in Cisco IOS Release 12.0(5)XE is different from the token bucket algorithm for the **police** command introduced in Cisco IOS Release 12.1(5)T. For information on the token bucket algorithm introduced in Release 12.0(5)XE, refer to the *Traffic Policing* document for Release 12.0(5)XE. This document is available on the *New Features for 12.0(5)XE* feature documentation index (under Modular QoS CLI-related feature modules) at www.cisco.com.

The following are explanations of how the token bucket algorithms introduced in Cisco IOS Release 12.1(5)T work.

Token Bucket Algorithm with One Token Bucket

The one token bucket algorithm is used when the **violate-action** option is not specified in the **police** command command-line interface (CLI).

The conform bucket is initially set to the full size (the full size is the number of bytes specified as the normal burst size).

When a packet of a given size (for example, “B” bytes) arrives at specific time (time “T”) the following actions occur:

- Tokens are updated in the conform bucket. If the previous arrival of the packet was at T1 and the current time is T, the bucket is updated with (T - T1) worth of bits based on the token arrival rate. The token arrival rate is calculated as follows:

  (time between packets <which is equal to T - T1> * policer rate)/8 bytes
- If the number of bytes in the conform bucket B is greater than or equal to 0, the packet conforms and the conform action is taken on the packet. If the packet conforms, B bytes are removed from the conform bucket and the conform action is completed for the packet.
- If the number of bytes in the conform bucket B is fewer than 0, the exceed action is taken.

Token Bucket Algorithm with Two Token Buckets

The two-token bucket algorithm is used when the **violate-action** option is specified in the **police** command CLI.

The conform bucket is initially full (the full size is the number of bytes specified as the normal burst size).

The exceed bucket is initially full (the full exceed bucket size is the number of bytes specified in the maximum burst size).

The tokens for both the conform and exceed token buckets are updated based on the token arrival rate, or committed information rate (CIR).

When a packet of given size (for example, “B” bytes) arrives at specific time (time “T”) the following actions occur:

- Tokens are updated in the conform bucket. If the previous arrival of the packet was at T1 and the current arrival of the packet is at t, the bucket is updated with T -T1 worth of bits based on the token arrival rate. The refill tokens are placed in the conform bucket. If the tokens overflow the conform bucket, the overflow tokens are placed in the exceed bucket.

  The token arrival rate is calculated as follows:

  (time between packets <which is equal to T-T1> * policer rate)/8 bytes
- If the number of bytes in the conform bucket - B is greater than or equal to 0, the packet conforms and the conform action is taken on the packet. If the packet conforms, B bytes are removed from the conform bucket and the conform action is taken. The exceed bucket is unaffected in this scenario.

- If the number of bytes in the conform bucket B is less than 0, the excess token bucket is checked for bytes by the packet. If the number of bytes in the exceed bucket B is greater than or equal to 0, the exceed action is taken and B bytes are removed from the exceed token bucket. No bytes are removed from the conform bucket.
- If the number bytes in the exceed bucket B is fewer than 0, the packet violates the rate and the violate action is taken. The action is complete for the packet.

Examples

Token Bucket Algorithm with One Token Bucket Example

The token bucket algorithm for the **police** command that was introduced in Cisco IOS Release 12.0(5)XE is different from the token bucket algorithms introduced in Cisco IOS Release 12.1(5)T. The following example is for the token bucket algorithm with one token bucket introduced in Cisco IOS Release 12.1(5)T.

If the **violate-action** option is not specified when you configure a policy with the **police** command in Cisco IOS Release 12.1(5)T onward, the token bucket algorithm uses one token bucket. If the **violate-action** option is specified, the token bucket algorithm uses two token buckets. In the following example, the **violate-action** option is not specified, so the token bucket algorithm only uses one token bucket.

The following configuration shows users how to define a traffic class (using the **class-map** command) and associate the match criteria from the traffic class with the traffic policing configuration, which is configured in the service policy (using the **policy-map** command). The **service-policy** command is then used to attach this service policy to the interface.

In this particular example, traffic policing is configured with the average rate at 8000 bits per second and the normal burst size at 1000 bytes for all packets leaving Fast Ethernet interface 0/0:

```
Router(config)# class-map access-match
Router(config-cmap)# match access-group 1
Router(config-cmap)# exit
Router(config)# policy-map police-setting
Router(config-pmap)# class access-match
Router(config-pmap-c)# police 8000 1000 conform-action transmit exceed-action drop
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface fastethernet 0/0
Router(config-if)# service-policy output police-setting
```

The treatment of a series of packets leaving Fast Ethernet interface 0/0 depends on the size of the packet and the number of bytes remaining in the conform bucket. These packets are policed based on the following rules:

- Tokens are updated in the conform bucket. If the previous arrival of the packet was at t1 and the current time is t, the bucket is updated with T -T1 worth of bits based on the token arrival rate. The token arrival rate is calculated as follows:

  (time between packets <which is equal to T - T1> * policer rate)/8 bytes
- If the number of bytes in the conform bucket B is greater than or equal to 0, the packet conforms and the conform action is taken on the packet. If the packet conforms, B bytes are removed from the conform bucket and the conform action is completed for the packet.
- If the number of bytes in the conform bucket B is fewer than 0, the exceed action is taken.

In this example, the initial token buckets starts full at 1000 bytes. If a 450-byte packet arrives, the packet conforms because enough bytes are available in the conform token bucket. The conform action (send) is taken by the packet and 450 bytes are removed from the conform token bucket (leaving 550 bytes).

If the next packet arrives 0.25 seconds later, 250 bytes are added to the token bucket ((0.25 * 8000)/8), leaving 800 bytes in the token bucket. If the next packet is 900 bytes, the packet exceeds and the exceed action (drop) is taken. No bytes are taken from the token bucket.

Token Bucket Algorithm with Two Token Buckets Example

If the **violate-action** option is specified when you configure a policy with the **police** command in Cisco IOS Release 12.1(5)T onward, the token bucket algorithm uses two token buckets. The following example uses the token bucket algorithm with two token buckets.

The following configuration shows users how to define a traffic class (using the **class-map** command) and associate the match criteria from the traffic class with the traffic policing configuration, which is configured in the service policy (using the **policy-map** command). The **service-policy** command is then used to attach this service policy to the interface.

In this particular example, traffic policing is configured with the average rate at 8000 bits per second, the normal burst size at 1000 bytes, and the excess burst size at 1000 bytes for all packets leaving Fast Ethernet interface 0/0.

```
Router(config)# class-map access-match
Router(config-cmap)# match access-group 1
Router(config-cmap)# exit
Router(config)# policy-map police-setting
Router(config-pmap)# class access-match
Router(config-pmap-c)# police 8000 1000 1000 conform-action transmit exceed-action
set-qos-transmit 1 violate-action drop
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface fastethernet 0/0
Router(config-if)# service-policy output police-setting
```

The treatment of a series of packets leaving Fast Ethernet interface 0/0 depends on the size of the packet and the number of bytes remaining in the conform and exceed token buckets. The series of packets are policed based on the following rules:

- If the previous arrival of the packet was at T1 and the current arrival of the packet is at T, the bucket is updated with T -T1 worth of bits based on the token arrival rate. The refill tokens are placed in the conform bucket. If the tokens overflow the conform bucket, the overflow tokens are placed in the exceed bucket. The token arrival rate is calculated as follows:

  (time between packets <which is equal to T - T1> * policer rate)/8 bytes

- If the number of bytes in the conform bucket B is greater than or equal to 0, the packet conforms and the conform action is taken on the packet. If the packet conforms, B bytes are removed from the conform bucket and the conform action is taken. The exceed bucket is unaffected in this scenario.
- If the number of bytes in the conform bucket B is less than 0, the excess token bucket is checked for bytes by the packet. If the number of bytes in the exceed bucket B is greater than or equal to 0, the exceed action is taken and B bytes are removed from the exceed token bucket. No bytes are removed from the conform bucket in this scenario.
- If the number bytes in the exceed bucket B is fewer than 0, the packet violates the rate and the violate action is taken. The action is complete for the packet.

In this example, the initial token buckets starts full at 1000 bytes. If a 450-byte packet arrives, the packet conforms because enough bytes are available in the conform token bucket. The conform action (send) is taken by the packet and 450 bytes are removed from the conform token bucket (leaving 550 bytes).

If the next packet arrives 0.25 seconds later, 250 bytes are added to the conform token bucket ((0.25 * 8000)/8), leaving 800 bytes in the conform token bucket. If the next packet is 900 bytes, the packet does not conform because only 800 bytes are available in the conform token bucket.

The exceed token bucket, which starts full at 1000 bytes (as specified by the excess burst size) is then checked for available bytes. Because enough bytes are available in the exceed token bucket, the exceed action (set the QoS transmit value of 1) is taken and 900 bytes are taken from the exceed bucket (leaving 100 bytes in the exceed token bucket.

If the next packet arrives 0.40 seconds later, 400 bytes are added to the token buckets ((.40 * 8000)/8). Therefore, the conform token bucket now has 1000 bytes (the maximum number of tokens available in the conform bucket) and 200 bytes overflow the conform token bucket (because it only 200 bytes were needed to fill the conform token bucket to capacity). These overflow bytes are placed in the exceed token bucket, giving the exceed token bucket 300 bytes.

If the arriving packet is 1000 bytes, the packet conforms because enough bytes are available in the conform token bucket. The conform action (transmit) is taken by the packet, and 1000 bytes are removed from the conform token bucket (leaving 0 bytes).

If the next packet arrives 0.20 seconds later, 200 bytes are added to the token bucket ((.20 * 8000)/8). Therefore, the conform bucket now has 200 bytes. If the arriving packet is 400 bytes, the packet does not conform because only 200 bytes are available in the conform bucket. Similarly, the packet does not exceed because only 300 bytes are available in the exceed bucket. Therefore, the packet violates and the violate action (drop) is taken.

Conforming to the MPLS EXP Value Example

The following example shows that if packets conform to the rate limit, the MPLS EXP field is set to 5. If packets exceed the rate limit, the MPLS EXP field is set to 3.

```
policy-map input-IP-dscp
  class dscp24
   police 8000 1500 1000
     conform-action set-mpls-experimental-imposition-transmit 5
     exceed-action set-mpls-experimental-imposition-transmit 3
     violate-action drop
```

Related Commands

Command	Description
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
service-policy	Specifies the name of the service policy to be attached to the interface.
show policy-map	Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps.
show policy-map interface	Displays the configuration of all classes configured for all service policies on the specified interface or displays the classes for the service policy for a specific PVC on the interface.