# QoS: Color-Aware Policer

**First Published: August 26, 2003**
**Last Updated: February 28, 2006**

The QoS: Color-Aware Policer enables a "color-aware" method of traffic policing. This feature allows you to police traffic according to the color classification of a packet. The packet color classification is based on packet matching criteria defined for two user-specified traffic classes—the conform-color class and the exceed-color class. These two traffic classes are created using the **conform-color** command and the metering rates are defined using the **police** command.

**History for the QoS: Color-Aware Policer Featurer**

| Release | Modification |
|---|---|
| 12.0(26)S | This feature was introduced. |
| 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



CISCO SYSTEMS

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

# Information About the Color-Aware Policer

To configure the Color-Aware Policer, you should understand the following concepts:



## Benefits

### Extended Traffic Policing Functionality

The Color-Aware Policer extends the functionality of the quality of service (QoS) traffic policing feature. It allows you to police traffic on the basis of the packet color classification in color-aware mode.

### Improved SLA Provisioning

The Color-Aware Policer allows you to provision enhanced Service Level Agreements (SLAs) across the DiffServ domain.

### Full Compliance with Industry-Standard RFCs

This feature fully complies with the following two industry-standard RFCs:

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

### Use of Preexisting Packet Marking from Other Traffic Policers

Cisco IOS software includes a number of traffic policing features, including the Two-Rate Policer. The Color-Aware Policer takes into account any preexisting markings that may be set for a packet by another traffic policer (for example, the Two-Rate Policer) configured at a previous network node. At the node where color-aware policing is configured, these preexisting markings are then used in determining the appropriate color-aware policing action for the packet.

For example, two-rate policing may be configured on a node upstream in the network. The Two-Rate Policer has marked a packet as violate-color. The Color-Aware Policer takes this violate-color marking into account when determining the appropriate policing action. In color-aware policing, the violate-color packet would never receive the action associated with either the conform-color packets or exceed-color packets. This way, tokens for violating packets are never taken from the metering token buckets at the color-aware policing node.

## Color-Aware Mode

The Cisco IOS traffic policing software polices traffic on the basis of metering rates such as the committed information rate (CIR), the peak information rate (PIR), their associated burst sizes, and any policing actions (such as transmit or drop) configured for the traffic. These metering rates, sizes, and policing actions are specified using the **police** command.

This feature allows you to police traffic in color-aware mode. In the color-aware mode, packet matching criteria will first be specified using the **class-map** command. Then a policy map will be configured to create classes, enable color-aware traffic policing, and create two classes used specifically for color-aware policing—the conform-color class and the exceed-color class.

The conform-color class and the exceed-class are created by using the **conform-color** command (described later in this document). The **police** command is used in conjunction with the **conform-color** command to specify the policing actions to be taken on packets in the conform-color class and the exceed-color class.

With color-aware policing, packets are classified as either conform-color packets, exceed-color packets, or violate-color packets. The metering treatment the packet receives varies by the classification, as described below:

- Packets belonging to the conform-color class are metered against both the CIR and the PIR.
- Packets belonging to the exceed-color class are metered against the PIR only.
- Packets belonging to the violate-color class are not metered against either the CIR or the PIR.

The **police** command is then used to specify the following items:

- The CIR and PIR
- The conform burst (bc) size
- The excess burst (be) size
- The policing actions to be taken on the packet

Color-aware mode can be used with either single-rate traffic policing or two-rate traffic policing.

## Color-Aware Mode of Single-Rate Traffic Policing

Networks police traffic by limiting the input or output transmission rate of a class of traffic on the basis of 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).

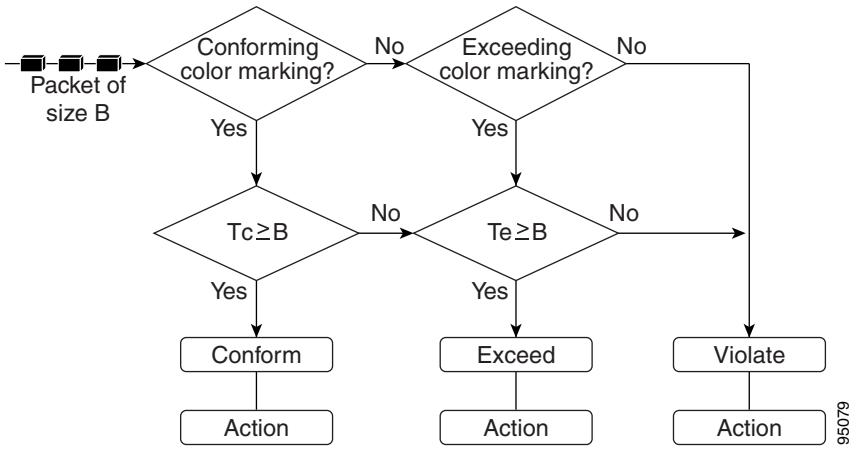
Single-rate traffic policing (often referred to simply as traffic policing) limits the input or output transmission rate of a class of traffic on the basis of user-defined criteria. It allows you to control the maximum rate of traffic transmitted or received on an interface.

Traffic policing works by using a token bucket algorithm. 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.

### Single-Rate Color-Aware Mode Functionality

The flow chart in Figure 1 illustrates the algorithm used for handling traffic in color-aware single-rate traffic policing.

***Figure 1 Traffic Flow Algorithm Used in Color-Aware Single-Rate Traffic Policing***




In the above flow chart, a packet of size B arrives at the interface. Tc indicates the number of tokens in the CIR token bucket, and Tb indicates the number of tokens in the excess token bucket.

When a packet of size B bytes arrives at the interface, the packet is evaluated as to whether it is marked as either a conform-color packet, an exceed-color packet, or a packet with no color marking. Then the following actions are performed on the packet in the order shown below:

1. If the packet is marked conform-color, and Tc is greater than or equal to B, the conform action is applied to the packet, and Tc is decremented by B.
2. Otherwise, if the packet is marked conform-color or exceed-color, and Te is greater than or equal to B, the exceed action is applied to the packet, and Te is decremented by B.
3. Otherwise, for all other packets, the violate action is applied to the packet.

#### Policing Actions

The algorithm provides users with three actions for each packet: a conform action, an exceed action, and an optional violate action. A conform action is applied to the conforming packets, an exceed action is applied to the exceeding packets, and an violate action is applied to the violating packets. Users can specify these actions. For instance, conforming packets can sent, exceeding packets can sent with a decreased priority, and violating packets can be dropped.

## Color-Aware Mode of Two-Rate Traffic Policing

Networks police traffic by limiting the input or output transmission rate of a class of traffic on the basis of 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 CoS.

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

Two-rate traffic policing uses two token buckets—Tc and Tp—for policing traffic at two independent rates. The Tc token bucket contains the tokens in the CIR bucket. The Tp token bucket contains the tokens in the PIR bucket.

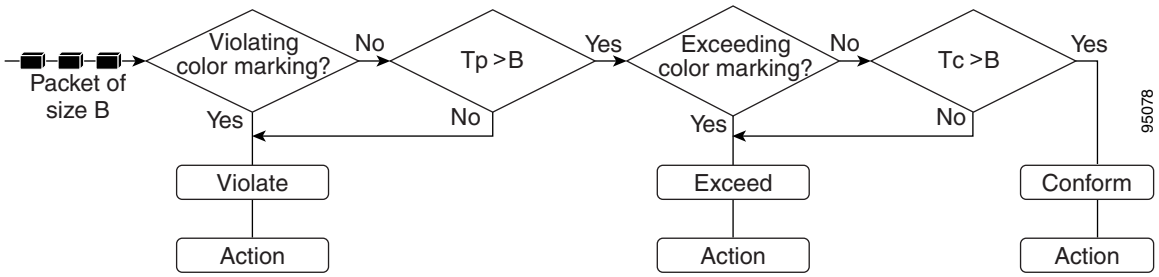
Note the following points about the two token buckets:

- The Tc token bucket is updated at the CIR value each time a packet arrives at the interface. The Tc token bucket can contain up to the confirm burst (Bc) value.
- The Tp token bucket is updated at the PIR value each time a packet arrives at the interface. The Tp token bucket can contain up to the peak burst (Be) value.

## Two-Rate Color-Aware Mode Functionality

The flow chart in Figure 2 illustrates the algorithm used for handling traffic in color-aware two-rate traffic policing.

***Figure 2 Traffic Flow Algorithm Used in Color-Aware Two-Rate Traffic Policing***




In the above illustration, a packet of size B arrives at the interface. Tc indicates the number of tokens in the CIR token bucket, and Tp indicates the number of tokens in PIR token bucket.

When a packet of size B bytes arrives at the interface, the packet is evaluated as to whether it is marked as either an exceed-color packet or a violate-color packet. Then the following actions are performed on the packet in the order shown below:

1. If the packet is marked violate-color, or Tp is less than B, the violate action is applied to the packet. Tp is not decremented.
2. Otherwise, if the packet is marked exceed-color, and Tc is less than B, the exceed action is applied to the packet, and Tc bucket is decremented by B.
3. Otherwise, for all other packets, the conform action is applied to the packet, and both the Tc and Tp are decremented by B.

### Policing Actions

The algorithm provides users with three actions for each packet: a conform action, an exceed action, and an optional violate action. A conform action is applied to the conforming packets, an exceed action is applied to the exceeding packets, and an violate action is applied to the violating packets. Users can specify these actions. For instance, conforming packets can sent, exceeding packets can sent with a decreased priority, and violating packets can be dropped.

## Packet Matching Criteria

The first process in configuring color-aware policing is to create a class map. The class map is used to specify packet matching criteria.For instance, you can configure the class map to match packets based on a precedence level, a CoS value, or a differentiated services code point (DSCP) value. The match criteria is set with a specific **match** command. For example, to match packets based on a precedence value, use the **match precedence** command.

The **match** commands that can be used in a class map to establish packet matching criteria include the commands listed in Table 1.

*Table 1 match Commands Used to Establish Packet Matching Criteria*

| Command | Description |
|---|---|
| **match cos** | Matches a packet based on a Layer 2 CoS value. |
| **match dscp** | Identifies a specific DSCP value as a match criterion. |
| **match fr-dlci** | Specifies the Frame Relay data-link connection identifier (DLCI) number as a match criterion. |
| **match mpls experimental** | Specifies the value of the Multiprotocol Label Switching (MPLS) experimental (EXP) field as a match criterion. |
| **match precedence** | Identifies IP precedence values as match criterion. |
| **match qos-group** | Identifies a specific QoS group value as a match criterion. |

The specific **match** commands that can be used to match packets vary from Cisco IOS release to Cisco IOS release. For more information about the **match** commands, refer to the documentation for your Cisco IOS release.

# How to Configure Color-Aware Policing

This section contains the following procedures:

- Creating a Class Map, page 6 (required)
- Configuring a Policy Map, page 8 (required)
- Attaching the Policy Map, page 10 (required)
- Verifying the Configuration, page 11 (optional)

## Creating a Class Map

A class map is used to specify packet matching criteria. To create a class map, use the commands in the following sections.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **class-map** [**match-all** | **match-any**] *class-map-name*

4. **match** [**ip**] **precedence** *ip-precedence-value*
5. **exit**
6. **class-map** [**match-all** | **match-any**] *class-map-name*
7. **match** [**ip**] **precedence** *ip-precedence-value*
8. **exit**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **class-map** [**match-all** \| **match-any**] *class-map-name*<br><br>**Example:**<br>`Router(config)# class-map conform_color_map` | Creates the conform-color class-map used for specifying packet matching criterion and enters class-map configuration mode.<br>**Note** The optional **match-all** and **match-any** keywords determine how packets are evaluated when multiple match criteria exist. Packets must meet either all of the match criteria (**match-all**) or one of the match criteria (**match-any**) to be considered a member of the class.<br>• Enter the class-map name. |
| **Step 4** | **match** [**ip**] **precedence** *ip-precedence-value*<br><br>`Router(config-cmap)# match ip precedence 5` | (Optional) Specifies the IP precedence value as the match criterion.<br>• Enter the IP precedence value.<br>**Note** In this example, the IP precedence value was used as the match criterion. Other criteria (for example, the CoS value, the DSCP, or the MPLS EXP value) can be used. Match criteria are specified by using the various **match** commands. Use the **match** command that is appropriate for your network. For a list of match commands that are available, see Table 1. |
| **Step 5** | **exit**<br><br>**Example:**<br>`Router(config-cmap)# exit` | (Optional) Exits class-map configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 6** | **class-map** [**match-all** \| **match-any**] *class-map-name*<br><br>**Example:**<br>`Router(config)# class-map exceed_color_map` | Creates the exceed-color class-map used for specifying packet matching criterion and enters class-map configuration mode.<br><br>**Note** The optional **match-all** and **match-any** keywords determine how packets are evaluated when multiple match criteria exist. Packets must meet either all of the match criteria (**match-all**) or one of the match criteria (**match-any**) to be considered a member of the class.<br><br>• Enter the class-map name. |
| **Step 7** | **match** [**ip**] **precedence** *ip-precedence-value*<br><br>`Router(config-cmap)# match ip precedence 3` | (Optional) Specifies the IP precedence value as the match criterion.<br><br>• Enter the IP precedence value.<br><br>**Note** In this example, the IP precedence value was used as the match criterion. Other criteria (for example, the CoS value, the DSCP, or the MPLS EXP value) can be used. Match criteria are specified by using the various **match** commands. Use the **match** command that is appropriate for your network. For a list of match commands that are available, see Table 1. |
| **Step 8** | **exit**<br><br>**Example:**<br>`Router(config-cmap)# exit` | (Optional) Exits class-map configuration mode. |

# Configuring a Policy Map

A policy map determines the specific QoS feature that will be applied to the packets in a specific class. For instance, a policy map can be used to configure traffic shaping, Weight Random Early Detection (WRED), or, as in this case, color-aware traffic policing.

To configure a policy map for color-aware traffic policing, use the commands in the following sections:

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map** *policy-map-name*
4. **class** {*class-name* | **class-default**}
5. **police cir** *cir* [**bc** *conform-burst*] **pir** *pir* [**be** *peak-burst*] [**conform-action** *action* [**exceed-action** *action* [**violate-action** *action*]]]
6. **conform-color** *class-map-name* [**exceed-color** *class-map-name*]
7. **exit**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **policy-map** *policy-map-name*<br><br>**Example:**<br>`Router(config)# policy-map color` | Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy and enters policy-map configuration mode.<br>• Enter the policy map name. |
| **Step 4** | **class** {*class-name* \| **class-default**}<br><br>**Example:**<br>`Router(config-pmap)# class ccolor` | Creates the specified class (or the default class) and enters policy-map class configuration mode.<br>• Enter name of the class you want to create or type **class-default** (to specify the default class). |
| **Step 5** | **police cir** *cir* [**bc** *conform-burst*] **pir** *pir* [**be** *peak-burst*] [**conform-action** *action* [**exceed-action** *action* [**violate-action** *action*]]]<br><br>**Example:**<br>`Router(config-pmap-c)# police cir 8000 bc 5000 pir 8000 be 5000 conform-action transmit exceed-action set-prec-transmit 4 violate-action drop` | Configures traffic policing on the basis of the specified rates and optional actions, and enters policy-map class police configuration mode.<br>• Enter the CIR and any optional values and actions, if applicable. |
| **Step 6** | **conform-color** *class-map-name* [**exceed-color** *class-map-name*]<br><br>**Example:**<br>`Router(config-pmap-c-police)# conform-color c1 exceed-color c2` | Enables color-aware traffic policing and creates the conform-color and exceed-color class-maps used for color-aware traffic policing.<br>The **conform-color** *class-map-name* command creates the conform-color class. The **exceed-color** *class-map-name* option creates the exceed-color class.<br>• Enter the class-map name or names. |
| **Step 7** | **exit**<br><br>**Example:**<br>`Router(config-pmap-c-police)# exit` | (Optional) Returns to global configuration mode. |

# Attaching the Policy Map

The policy map you have created must be attached to the appropriate interface or ATM permanent virtual circuit (PVC). For example, you may have to attach policy maps to either the input or the output interface on either the ingress or the egress router.

To attach a policy map to the appropriate interface or ATM PVC, use the commands in the following sections:

## SUMMARY STEPS

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

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **interface** *type number* [*name-tag*]<br><br>**Example:**<br>`Router(config)# interface FastEthernet1/0.1` | Configures the interface type specified and enters interface configuration mode.<br>• Enter interface type. |
| **Step 4** | **pvc** [*name*] *vpi*/*vci* [**ilmi** \| **qsaal** \| **smds**]<br><br>**Example:**<br>`Router(config-if)# pvc cisco 0/16 ilmi` | (Optional) Creates or assigns a name to an ATM PVC, specifies the encapsulation type on an ATM PVC, and enters ATM VC configuration mode.<br>**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 Step 5.<br>• Enter the PVC name. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 5** | **service-policy** {**input** \| **output**} *policy-map-name*<br><br>**Example:**<br>`Router(config-if)# service-policy input policy1` | Specifies the name of the policy map to be attached to the *input or output* direction of the interface.<br><br>**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.<br><br>• Enter the policy map name. |
| **Step 6** | **exit**<br><br>**Example:**<br>`Router(config-if)# exit` | (Optional) Exits interface configuration mode. |

# Verifying the Configuration

This task allows you to verify that you created the configuration you intended and that the feature is functioning correctly. To verify the configuration, use the commands in the following sections:

## SUMMARY STEPS

1. **enable**
2. **show policy-map**
3. **show policy-map interface** *interface-name*
4. **exit**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **show policy-map**<br><br>**Example:**<br>`Router# show policy-map` | Displays all configured policy maps. |
| **Step 3** | **show policy-map interface** *interface-name*<br><br>**Example:**<br>`Router# show policy-map interface serial4/0` | 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.<br>• Enter the interface name. |
| **Step 4** | **exit**<br><br>**Example:**<br>`Router(config-if)# exit` | (Optional) Exits interface configuration mode. |

## Troubleshooting Tips

The commands in the "Verifying the Configuration" 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 transmisson (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 Color-Aware Policing

This section provides the following configuration example:



## Color-Aware Policing: Example

The following example shows color-aware policing configured in a policy map called "color." Before the feature was configured, the **class-map** command was used to create two classes called "c1" and "c2," respectively. These two classes were configured as shown below:

```
class-map c1
 match ip prec 5
class-map c2
 match ip prec 3
```

With the two classes created, color-aware policing is configured as shown below:

```
Router# enable
Router# configure terminal
Router(config)# policy-map color
Router(config-pmap)# class ccolor
Router(config-pmap-c)# police cir 8000 bc 5000 pir 8000 be 5000 conform-action transmit
exceed-action set-prec-transmit 4 violate-action drop
Router(config-pmap-c-police)# conform-color c1 exceed-color c2
```

**Note** The traffic class (in this example, ccolor) must still be created using the Modular QoS Command-Line Interface (CLI) (MQC).

With color-aware policing configured as shown, the following results occur based on the CIR, the PIR, and the conform actions, exceed actions, and violate actions specified by the **police** command:

- Packets that have metering rates less than or equal to the CIR and belong to class c1 (conform-color) are policed as conforming to the rate. These packets are also policed according to the conform action specified by the **police** command. In this instance, the packets will be transmitted.
- Packets that have metering rates between the CIR and the PIR and belong to either class c1 (conform-color) or class c2 (exceed-color) are policed as exceeding the CIR. These packets are also policed according to the exceed action specified by the **police** command. In this instance, the precedence value of the packets will be set and the packets transmitted.
- Packets that have metering rates higher than the PIR or belong to *neither* class c1 *or* class c2 are policed as violating the rate. These packets are also policed according to the violate action specified by the **police** command. In this instance, the packets will be dropped.

# Additional References

The following sections provide references related to the Color-Aware Policing feature:

## Related Documents

| Related Topic | Document Title |
|---|---|
| QoS commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples | *Cisco IOS Quality of Service Solutions Command Reference*, Release 12.3T |
| Additional information about configuring traffic policing | "Policing and Shaping" chapter in *Cisco IOS Quality of Service Solutions Configuration Guide*, Release 12.3 |
| MQC | "Configuring the Modular Quality of Service Command-Line Interface" chapter in *Cisco IOS Quality of Service Solutions Configuration Guide*, Release 12.3 |
| Two-rate traffic policing | "*Two-Rate Policer*" Cisco IOS Release 12.2(4)T feature module |
| Traffic policing using multiple policer actions | *Policer Enhancement — Multiple Actions*, Cisco IOS Release 12.2(8)T feature module |
| Percentage-based traffic policing and shaping | *Percentage-Based Policing and Shaping*, Cisco IOS Release 12.2(13)T feature module |
| Three-level hierarchical policing | *Modular QoS CLI (MQC) Three-Level Hierarchical Policer*, Cisco IOS Release 12.2(13)T feature module |

## Standards

| Standards | Title |
|---|---|
| None | — |

## MIBs

| MIBs | MIBs Link |
|---|---|
| • CISCO-CLASS-BASED-QOS-MIB<br>• 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:<br>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 new and modified commands. All other commands used with this feature are documented in the Cisco IOS Release 12.3T command reference publications.

### New Commands

- **conform-color**

### Modified Commands

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

# conform-color

To enable color-aware traffic policing and create the conform-color and exceed-color class maps used for color-aware traffic policing, use the **conform-color** command in policy-map class police configuration mode. To disable the color-aware mode of traffic policing, use the **no** form of this command.

**conform-color** *class-map-name* [**exceed-color** *class-map-name*]

**no conform-color**

## Syntax Description

| | |
|---|---|
| *class-map-name* | Specifies the name of the conform-color class map. This is the class map in which packets conforming to the traffic policing color will be placed. The class-map name can be a maximum of 40 alphanumeric characters. |
| **exceed-color** | (Optional) Indicates that an exceed-color class-map name will be specified. |
| *class-map-name* | (Optional) Specifies the name of the exceed-color class map. This is the class map in which packets exceeding the traffic policing color will be placed. The name can be a maximum of 40 alphanumeric characters. |

## Defaults

No default behavior or values

## Command Modes

Policy-map class police configuration

## Command History

| Release | Modification |
|---|---|
| 12.0(26)S | This command was introduced. |
| 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB. |

## Usage Guidelines

The **conform-color** command is used in conjunction with the **police** command to configure color-aware policing. The **police** command specifies the committed information rate (CIR), conform burst (bc) size, peak information rate (PIR), and excess burst (be) size used to police packets. The **police** command is also used to specify any optional policing actions (such as transmit, set-clp-transmit, or drop) that can be performed on packets conforming to, exceeding, or violating the specified rates.

When using the **conform-color** command, note the following points:

- If the **exceed-color** keyword and corresponding *class-map-name* argument are not specified, all packets not belonging to the specified conform-color class will belong to the exceed-color class.
- If *both* the conform-color and exceed-color class-map names are specified, packets not belonging to *either* the conform-color class or the exceed-color class will belong to the violate-color class.

## Examples

The following example shows color-aware policing configured in a policy map called "color." Before the feature was configured, the **class-map** command was used to create two classes called "c1" and "c2," respectively. These two classes were configured as shown below:

```
class-map c1
 match ip prec 5
class-map c2
 match ip prec 3
```

With the two classes created, color-aware policing is configured as shown below:

```
Router# enable
Router# configure terminal
Router(config)# policy-map color
Router(config-pmap)# class ccolor
Router(config-pmap-c)# police cir 8000 bc 5000 pir 8000 be 5000 conform-action transmit
exceed-action set-prec-transmit 4 violate-action drop
Router(config-pmap-c-police)# conform-color c1 exceed-color c2
```

With color-aware policing configured as shown, the following results occur on the basis of the CIR, the PIR, and the conform actions, exceed actions, and violate actions specified by the **police** command:

- Packets that have metering rates less than or equal to the CIR and belong to class c1 are policed as conforming to the rate. These packets are also policed according to the conform action specified by the **police** command. In this instance, the packets will be transmitted.
- Packets that have metering rates between the CIR and the PIR and belong to class c1 or c2 are policed as exceeding the CIR. These packets are also policed according to the exceed action specified by the **police** command. In this instance, the precedence value of the packets will be set and the packets transmitted.
- Packets that have metering rates higher than the PIR, or belong to *neither* class c1 *or* c2 are policed as violating the rate. These packets are also policed according to the violate action specified by the **police** command. In this instance, the packets will be dropped.

## Related Commands

| Command | Description |
|---|---|
| **class-map** | Creates a class map to be used for matching packets to a specified class. |
| **match precedence** | Identifies IP precedence values as match criteria. |
| **police** | Configures traffic policing. |
| **police (two rates)** | Configures traffic policing using two rates, the CIR and the PIR. |
| **policy-map** | Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy. |

# show policy-map

To display the configuration of all classes for a specified service policy map or all classes for all existing policy maps, use the **show policy-map** command in EXEC mode.

**show policy-map** [*policy-map*]

## Syntax Description

| | |
|---|---|
| *policy-map* | (Optional) Name of the service policy map whose complete configuration is to be displayed. |

## Command Default

All existing policy map configurations are displayed.

## Command Modes

EXEC

## Command History

| Release | Modification |
|---|---|
| 12.0(5)T | This command was introduced. |
| 12.0(5)XE | This command was integrated into Cisco IOS Release 12.0(5)XE. |
| 12.0(7)S | This command was integrated into Cisco IOS Release 12.0(7)S. |
| 12.1(1)E | This command was integrated into Cisco IOS Release 12.1(1)E. |
| 12.2(13)T | The output of this command was modified for the Percentage-Based Policing and Shaping feature and includes the bandwidth percentage used when calculating traffic policing and shaping. |
| 12.0(28)S | The output of this command was modified for the QoS: Percentage-Based Policing feature to display the committed (conform) burst (bc) and excess (peak) burst (be) sizes in milliseconds (ms). |
| 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB. |

## Usage Guidelines

The **show policy-map** command displays the configuration of a service policy map created using the **policy-map** command. You can use the **show policy-map** command to display all class configurations comprising any existing service policy map, whether or not that service policy map has been attached to an interface.

## Examples

The following is sample output from the **show policy-map** command. This sample output displays the contents of a policy map called "policy1." In policy 1, traffic policing on the basis of a committed information rate (CIR) of 20 percent has been configured, and the bc and be have been specified in milliseconds. As part of the traffic policing configuration, optional conform, exceed, and violate actions have been specified.

```
Router# show policy-map policy1

  Policy Map policy1
    Class class1
     police cir percent 20 bc 300 ms pir percent 40 be 400 ms
```

```
conform-action transmit
exceed-action drop
violate-action drop
```

Table 2 describes the significant fields shown in the display.

*Table 2 show policy-map Field Descriptions*

| Field | Description |
|---|---|
| Policy Map | Name of policy map displayed. |
| Class | Name of class configured in policy map displayed. |
| police | Indicates that traffic policing on the basis of specified percentage of bandwidth has been enabled. The committed burst (bc) and excess burst (be) sizes have been specified in milliseconds (ms), and optional conform, exceed, and violate actions have been specified. |

## 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. |
| **show policy-map class** | Displays the configuration for the specified class of the specified policy map. |
| **show policy-map interface** | 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. |

# show policy-map interface

To display 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, use the **show policy-map interface** command in privileged EXEC mode.

**show policy-map interface** [**type access-control**] *interface-name* [**vc** [*vpi*/] *vci*] [**dlci** *dlci*] [**input | output**]

### ATM Shared Port Adapter

**show policy-map interface atm** *slot*/*subslot*/*port*[**.***subinterface*]

## Syntax Description

| | |
|---|---|
| **type access-control** | (Optional) Displays class maps configured to determine the exact pattern to look for in the protocol stack of interest. |
| *interface-name* | Name of the interface or subinterface whose policy configuration is to be displayed. |
| **vc** | (Optional) For ATM interfaces only, shows the policy configuration for a specified PVC. The name can be up to 16 characters long. |
| *vpi*/ | (Optional) ATM network virtual path identifier (VPI) for this PVC. On the Cisco 7200 and 7500 series routers, this value ranges from 0 to 255.<br>The *vpi* and *vci* arguments cannot both be set to 0; if one is 0, the other cannot be 0. |
| *vci* | (Optional) ATM network virtual channel identifier (VCI) for this PVC. This value ranges from 0 to 1 less than the maximum value set for this interface by the **atm vc-per-vp** command. Typically, the lower values 0 to 31 are reserved for specific traffic (F4 Operation, Administration, and Maintenance (OAM), switched virtual circuit (SVC) signaling, Integrated Local Management Interface (ILMI), and so on) and should not be used.<br>The VCI is a 16-bit field in the header of the ATM cell. The VCI value is unique only on a single link, not throughout the ATM network, because it has local significance only.<br>The *vpi* and *vci* arguments cannot both be set to 0; if one is 0, the other cannot be 0. |
| **dlci** | (Optional) Indicates that a specific PVC for which policy configuration will be displayed. |
| *dlci* | (Optional) A specific data-link connection identifier (DLCI) number used on the interface. Policy configuration for the corresponding PVC will be displayed when a DLCI is specified. |
| **input** | (Optional) Indicates that the statistics for the attached input policy will be displayed. |
| **output** | (Optional) Indicates that the statistics for the attached output policy will be displayed. |

| | |
|---|---|
| *slot* | (ATM Shared Port Adapter only) Chassis slot number. Refer to the appropriate hardware manual for slot information. For SIPs, refer to the platform-specific SPA hardware installation guide or the corresponding "Identifying Slots and Subslots for SIPs and SPAs" topic in the platform-specific SPA software configuration guide. |
| */subslot* | (ATM Shared Port Adapter only) Secondary slot number on a SPA interface processor (SIP) where a SPA is installed. Refer to the platform-specific SPA hardware installation guide and the corresponding "Specifying the Interface Address on a SPA" topic in the platform-specific SPA software configuration guide for subslot information. |
| */port* | (ATM Shared Port Adapter only) Port or interface number. Refer to the appropriate hardware manual for port information. For SPAs, refer to the corresponding "Specifying the Interface Address" topics in the platform-specific SPA software configuration guide. |
| *.subinterface* | (ATM Shared Port Adapter only—Optional) Subinterface number. The number that precedes the period must match the number to which this subinterface belongs. The range is 1 to 4,294,967,293. |

## Defaults

The absence of both the forward slash (/) and a *vpi* value defaults the *vpi* value to 0. If this value is omitted, information for all virtual circuits (VCs) on the specified ATM interface or subinterface is displayed.

### ATM Shared Port Adapter

When used with the ATM shared port adapter, this command has no default behavior or values.

## Command Modes

Privileged EXEC

### ATM Shared Port Adapter

When used with the ATM shared port adapter, EXEC or privileged EXEC.

## Command History

| Release | Modification |
|---|---|
| 12.0(5)T | This command was introduced. |
| 12.0(5)XE | This command was integrated into Cisco IOS Release 12.0(5)XE. |
| 12.0(7)S | This command was integrated into Cisco IOS Release 12.0(7)S. |
| 12.1(1)E | This command was integrated into Cisco IOS Release 12.1(1)E. |
| 12.1(2)T | This command was modified to display information about the policy for all Frame Relay PVCs on the interface, or, if a DLCI is specified, the policy for that specific PVC. This command was also modified to display the total number of packets marked by the quality of service (QoS) set action. |
| 12.1(3)T | This command was modified to display per-class accounting statistics. |
| 12.2(4)T | This command was modified for two-rate traffic policing. It now can display burst parameters and associated actions. |

| Release | Modification |
|---|---|
| 12.2(8)T | The command was modified for the Policer Enhancement — Multiple Actions feature and the WRED — Explicit Congestion Notification (ECN) feature.<br><br>For the Policer Enhancement — Multiple Actions feature, the command was modified to display the multiple actions configured for packets conforming to, exceeding, or violating a specific rate.<br><br>For the WRED — Explicit Congestion Notification (ECN) feature, the command displays ECN marking information |
| 12.2(13)T | The following modifications were made:<br><br>• This command was modified for the Percentage-Based Policing and Shaping feature.<br><br>• This command was modified for the Class-Based RTP and TCP Header Compression feature.<br><br>• This command was modified as part of the Modular QoS CLI (MQC) Unconditional Packet Discard feature. Traffic classes in policy maps can now be configured to discard packets belonging to a specified class.<br><br>• This command was modified to display the Frame Relay DLCI number as a criterion for matching traffic inside a class map.<br><br>• This command was modified to display Layer 3 packet length as a criterion for matching traffic inside a class map.<br><br>• This command was modified for the Enhanced Packet Marking feature. A mapping table (table map) can now be used to convert and propagate packet-marking values. |
| 12.2(15)T | This command was modified to display Frame Relay voice-adaptive traffic-shaping information. |
| 12.0(28)S | This command was modified for the QoS: Percentage-Based Policing feature to include milliseconds when calculating the committed (conform) burst (bc) and excess (peak) burst (be) sizes. |
| 12.3(14)T | This command was modified to display bandwidth estimation parameters. |
| 12.2(18)SXE | This command was integrated into Cisco IOS Release 12.2(18)SXE. This command was modified to display aggregate WRED statistics for the ATM shared port adapter. Note that changes were made to the syntax, defaults, and command modes. These changes are labelled “ATM Shared Port Adapter.” |
| 12.4(4)T | The **type access-control** keywords were added to support flexible packet matching. |
| 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB and its output was modified to display either legacy (nondistributed processing) QoS or hierarchical queueing framework (HQF) parameters on FR interfaces or PVCs. |

## Usage Guidelines

The **show policy-map interface** command displays the packet statistics for classes on the specified interface or the specified PVC only if a service policy has been attached to the interface or the PVC.

You can use the *interface-name* argument to display output for a PVC only for enhanced ATM port adapters (PA-A3) that support per-VC queueing.

The counters displayed after the **show policy-map interface** command is entered are updated only if congestion is present on the interface.

The **show policy-map interface** command displays policy information about Frame Relay PVCs only if Frame Relay Traffic Shaping (FRTS) is enabled on the interface.

The **show policy-map interface** command displays ECN marking information only if ECN is enabled on the interface.

To determine if shaping is active with HQF, check the queue depth field of the "(queue depth/total drops/no-buffer drops)" line in the **show policy-map interface** command output.

## Examples

This section provides sample output from typical **show policy-map interface** commands. Depending upon the interface in use and the options enabled, the output you see may vary slightly from the ones shown below.

### Example of Weighted Fair Queueing (WFQ) on Serial Interface

The following sample output of the **show policy-map interface** command displays the statistics for the serial 3/1 interface, to which a service policy called mypolicy (configured as shown below) is attached. Weighted fair queueing (WFQ) has been enabled on this interface. See Table 3 for an explanation of the significant fields that commonly appear in the command output.

```
policy-map mypolicy
  class voice
    priority 128
  class gold
   bandwidth 100
  class silver
   bandwidth 80
   random-detect

Router# show policy-map interface serial3/1 output

 Serial3/1

  Service-policy output: mypolicy

    Class-map: voice (match-all)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: ip precedence 5
      Weighted Fair Queueing
        Strict Priority
        Output Queue: Conversation 264
        Bandwidth 128 (kbps) Burst 3200 (Bytes)
        (pkts matched/bytes matched) 0/0
        (total drops/bytes drops) 0/0

    Class-map: gold (match-all)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: ip precedence 2
      Weighted Fair Queueing
        Output Queue: Conversation 265
        Bandwidth 100 (kbps) Max Threshold 64 (packets)
        (pkts matched/bytes matched) 0/0
        (depth/total drops/no-buffer drops) 0/0/0

    Class-map: silver (match-all)
      0 packets, 0 bytes
```

```
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: ip precedence 1
      Weighted Fair Queueing
        Output Queue: Conversation 266
        Bandwidth 80 (kbps)
        (pkts matched/bytes matched) 0/0
        (depth/total drops/no-buffer drops) 0/0/0
         exponential weight: 9
         mean queue depth: 0

class     Transmitted       Random drop      Tail drop    Minimum Maximum  Mark
          pkts/bytes        pkts/bytes       pkts/bytes    thresh  thresh  prob
0             0/0               0/0              0/0          20      40  1/10
1             0/0               0/0              0/0          22      40  1/10
2             0/0               0/0              0/0          24      40  1/10
3             0/0               0/0              0/0          26      40  1/10
4             0/0               0/0              0/0          28      40  1/10
5             0/0               0/0              0/0          30      40  1/10
6             0/0               0/0              0/0          32      40  1/10
7             0/0               0/0              0/0          34      40  1/10
rsvp          0/0               0/0              0/0          36      40  1/10

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

### Example of Traffic Shaping on Serial Interface

The following sample output from the **show policy-map interface** command displays the statistics for the serial 3/2 interface, to which a service policy called p1 (configured as shown below) is attached. Traffic shaping has been enabled on this interface. See Table 3 for an explanation of the significant fields that commonly appear in the command output.

```
policy-map p1
  class c1
   shape average 320000

Router# show policy-map interface serial3/2 output

 Serial3/2

  Service-policy output: p1

    Class-map: c1 (match-all)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: ip precedence 0
      Traffic Shaping
        Target    Byte   Sustain   Excess    Interval  Increment Adapt
        Rate      Limit  bits/int  bits/int  (ms)      (bytes)   Active
        320000    2000   8000      8000      25        1000      -

        Queue     Packets   Bytes     Packets   Bytes     Shaping
        Depth                         Delayed   Delayed   Active
        0         0         0         0         0         no

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

Table 3 describes significant fields commonly shown in the displays. The fields in the table are grouped according to the relevant QoS feature.

***Table 3 show policy-map interface Field Descriptions [1]***

| Field | Description |
|---|---|
| **Fields Associated with Classes or Service Policies** | |
| Service-policy output | Name of the output service policy applied to the specified interface or VC. |
| Class-map | Class of traffic being displayed. Output is displayed for each configured class in the policy. The choice for implementing class matches (for example, match-all or match-any) can also appear next to the traffic class. |
| packets and bytes | Number of packets (also shown in bytes) identified as belonging to the class of traffic being displayed. |
| offered rate | Rate, in kbps, of packets coming in to the class.<br>**Note** If the packets are compressed over an outgoing interface, the improved packet rate achieved by packet compression is not reflected in the offered rate. Also, if the packets are classified *before* they enter a combination of tunnels (for example, a generic routing encapsulation (GRE) tunnel and an IP Security (IPSec) tunnel), the offered rate does not include all the extra overhead associated with tunnel encapsulation in general. Depending on the configuration, the offered rate may include no overhead, may include the overhead for only *one* tunnel encapsulation, or may include the overhead for *all* tunnel encapsulations. In most of the GRE and IPSec tunnel configurations, the offered rate includes the overhead for GRE tunnel encapsulation only. |
| drop rate | Rate, in kbps, at which packets are dropped from the class. The drop rate is calculated by subtracting the number of successfully transmitted packets from the offered rate. |
| **Note** In distributed architecture platforms (such as the C7500), the value of the transfer rate, calculated as the difference between the offered rate and the drop rate counters, can sporadically deviate from the average by up to 20 percent or more. This can occur while no corresponding burst is registered by independent traffic analyser equipment. | |
| Match | Match criteria specified for the class of traffic. Choices include criteria such as IP precedence, IP differentiated services code point (DSCP) value, Multiprotocol Label Switching (MPLS) experimental (EXP) value, access groups, and QoS groups. For more information about the variety of match criteria options available, refer to the chapter “Configuring the Modular Quality of Service Command-Line Interface” in the *Cisco IOS Quality of Service Solutions Configuration Guide*. |
| **Fields Associated with Queueing (If Enabled)** | |
| Output Queue | The weighted fair queueing (WFQ) conversation to which this class of traffic is allocated. |
| Bandwidth | Bandwidth, in either kbps or percentage, configured for this class and the burst size. |

*Table 3 show policy-map interface Field Descriptions [1] (continued)*

| Field | Description |
|---|---|
| pkts matched/bytes matched | Number of packets (also shown in bytes) matching this class that were placed in the queue. This number reflects the total number of matching packets queued at any time. Packets matching this class are queued only when congestion exists. If packets match the class but are never queued because the network was not congested, those packets are not included in this total. However, if process switching is in use, the number of packets is always incremented even if the network is not congested. |
| depth/total drops/no-buffer drops | Number of packets discarded for this class. No-buffer indicates that no memory buffer exists to service the packet. |
| **Fields Associated with Weighted Random Early Detection (WRED) (If Enabled)** | |
| exponential weight | Exponent used in the average queue size calculation for a WRED parameter group. |
| mean queue depth | Average queue depth based on the actual queue depth on the interface and the exponential weighting constant. It is a fluctuating average. The minimum and maximum thresholds are compared against this value to determine drop decisions. |
| class | IP precedence level. |
| Transmitted pkts/bytes | Number of packets (also shown in bytes) passed through WRED and not dropped by WRED.<br>**Note** If there is insufficient memory in the buffer to accommodate the packet, the packet can be dropped *after* the packet passes through WRED. Packets dropped because of insufficient memory in the buffer (sometimes referred to as "no-buffer drops") are not taken into account by the WRED packet counter. |
| Random drop pkts/bytes | Number of packets (also shown in bytes) randomly dropped when the mean queue depth is between the minimum threshold value and the maximum threshold value for the specified IP precedence level. |
| Tail drop pkts/bytes | Number of packets dropped when the mean queue depth is greater than the maximum threshold value for the specified IP precedence level. |
| Minimum thresh | Minimum threshold. Minimum WRED threshold in number of packets. |
| Maximum thresh | Maximum threshold. Maximum WRED threshold in number of packets. |
| Mark prob | Mark probability. Fraction of packets dropped when the average queue depth is at the maximum threshold. |
| **Fields Associated with Traffic Shaping (If Enabled)** | |
| Target Rate | Rate used for shaping traffic. |
| Byte Limit | Maximum number of bytes that can be transmitted per interval. Calculated as follows:<br>((Bc+Be) /8) x 1 |
| Sustain bits/int | Committed burst (Bc) rate. |
| Excess bits/int | Excess burst (Be) rate. |
| Interval (ms) | Time interval value in milliseconds (ms). |

*Table 3 show policy-map interface Field Descriptions [1] (continued)*

| Field | Description |
|---|---|
| Increment (bytes) | Number of credits (in bytes) received in the token bucket of the traffic shaper during each time interval. |
| Queue Depth | Current queue depth of the traffic shaper. |
| Packets | Total number of packets that have entered the traffic shaper system. |
| Bytes | Total number of bytes that have entered the traffic shaper system. |
| Packets Delayed | Total number of packets delayed in the queue of the traffic shaper before being transmitted. |
| Bytes Delayed | Total number of bytes delayed in the queue of the traffic shaper before being transmitted. |
| Shaping Active | Indicates whether the traffic shaper is active. For example, if a traffic shaper is active, and the traffic being sent exceeds the traffic shaping rate, a "yes" appears in this field. |

1. A number in parentheses may appear next to the service-policy output name, class-map name, and match criteria information. The number is for Cisco internal use only and can be disregarded.

### Example of Precedence-Based Aggregate WRED on ATM Shared Port Adapter

The following sample output of the **show policy-map interface** command displays the statistics for the ATM shared port adapter interface 4/1/0.10, to which a service policy called prec-aggr-wred (configured as shown below) is attached. Because aggregate WRED has been enabled on this interface, the class through Mark Prob statistics are aggregated by subclasses. See Table 4 for an explanation of the significant fields that commonly appear in the command output.

```
Router(config)# policy-map prec-aggr-wred
Router(config-pmap)# class class-default
Router(config-pmap-c)# random-detect aggregate
Router(config-pmap-c)# random-detect precedence values 0 1 2 3 minimum thresh 10
maximum-thresh 100 mark-prob 10
Router(config-pmap-c)# random-detect precedence values 4 5 minimum-thresh 40
maximum-thresh 400 mark-prob 10
Router(config-pmap-c)# random-detect precedence values 6 minimum-thresh 60 maximum-thresh
600 mark-prob 10
Router(config-pmap-c)# random-detect precedence values 7 minimum-thresh 70 maximum-thresh
700 mark-prob 10
Router(config-pmap-c)# interface ATM4/1/0.10 point-to-point
Router(config-subif)# ip address 10.0.0.2 255.255.255.0
Router(config-subif)# pvc 10/110
Router(config-subif)# service-policy output prec-aggr-wred


Router# show policy-map interface a4/1/0.10

 ATM4/1/0.10: VC 10/110 -

  Service-policy output: prec-aggr-wred

    Class-map: class-default (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
        Exp-weight-constant: 9 (1/512)
        Mean queue depth: 0
```

```
      class       Transmitted     Random drop      Tail drop     Minimum   Maximum  Mark
pkts/bytespkts/bytespkts/bytesthreshthreshprob

      0  1  2  3       0/0              0/0             0/0           10      100  1/10
      4  5             0/0              0/0             0/0           40      400  1/10
      6                0/0              0/0             0/0           60      600  1/10
      7                0/0              0/0             0/0           70      700  1/10
```

### Example of DSCP-Based Aggregate WRED on ATM Shared Port Adapter

The following sample output of the **show policy-map interface** command displays the statistics for the ATM shared port adapter interface 4/1/0.11, to which a service policy called dscp-aggr-wred (configured as shown below) is attached. Because aggregate WRED has been enabled on this interface, the class through Mark Prob statistics are aggregated by subclasses. See Table 4 for an explanation of the significant fields that commonly appear in the command output.

```
Router(config)# policy-map dscp-aggr-wred
Router(config-pmap)# class class-default
Router(config-pmap-c)# random-detect dscp-based aggregate minimum-thresh 1 maximum-thresh
10 mark-prob 10
Router(config-pmap-c)# random-detect dscp values 0 1 2 3 4 5 6 7 minimum-thresh 10
maximum-thresh 20 mark-prob 10
Router(config-pmap-c)# random-detect dscp values 8 9 10 11 minimum-thresh 10
maximum-thresh 40 mark-prob 10
Router(config)# interface ATM4/1/0.11 point-to-point
Router(config-subif)# ip address 10.0.0.2 255.255.255.0
Router(config-subif)# pvc 11/101
Router(config-subif)# service-policy output dscp-aggr-wred


Router# show policy-map interface a4/1/0.11

 ATM4/1/0.11: VC 11/101 -

  Service-policy output: dscp-aggr-wred

    Class-map: class-default (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
        Exp-weight-constant: 0 (1/1)
        Mean queue depth: 0
        class       Transmitted     Random drop      Tail drop     Minimum   Maximum  Mark
                  pkts/bytespkts/bytespkts/bytesthreshthreshprob
        default           0/0              0/0             0/0             1       10  1/10
        0  1  2  3
        4  5  6  7        0/0              0/0             0/0           10       20  1/10
        8  9  10 11       0/0              0/0             0/0           10       40  1/10
```

Table 4 describes the significant fields shown in the display when aggregate WRED is configured for an ATM shared port adapter.

***Table 4 show policy-map interface Field Descriptions—Configured for Aggregate WRED on ATM Shared Port Adapter***

| Field | Description |
|---|---|
| exponential weight | Exponent used in the average queue size calculation for a Weighted Random Early Detection (WRED) parameter group. |
| mean queue depth | Average queue depth based on the actual queue depth on the interface and the exponential weighting constant. It is a fluctuating average. The minimum and maximum thresholds are compared against this value to determine drop decisions. |
| **Note** When Aggregate Weighted Random Early Detection (WRED) is enabled, the following WRED statistics will be aggregated based on their subclass (either their IP precedence or differentiated services code point (DSCP) value). | |
| class | IP precedence level or differentiated services code point (DSCP) value. |
| Transmitted pkts/bytes | Number of packets (also shown in bytes) passed through WRED and not dropped by WRED.<br>**Note** If there is insufficient memory in the buffer to accommodate the packet, the packet can be dropped *after* the packet passes through WRED. Packets dropped because of insufficient memory in the buffer (sometimes referred to as "no-buffer drops") are not taken into account by the WRED packet counter. |
| Random drop pkts/bytes | Number of packets (also shown in bytes) randomly dropped when the mean queue depth is between the minimum threshold value and the maximum threshold value for the specified IP precedence level or DSCP value. |
| Tail drop pkts/bytes | Number of packets dropped when the mean queue depth is greater than the maximum threshold value for the specified IP precedence level or DSCP value. |
| Minimum thresh | Minimum threshold. Minimum WRED threshold in number of packets. |
| Maximum thresh | Maximum threshold. Maximum WRED threshold in number of packets. |
| Mark prob | Mark probability. Fraction of packets dropped when the average queue depth is at the maximum threshold. |

#### Frame Relay Voice-Adaptive Traffic-Shaping show policy interface Command Example

The following sample output shows that Frame Relay voice-adaptive traffic shaping is currently active and has 29 seconds left on the deactivation timer. With traffic shaping active and the deactivation time set, this means that the current sending rate on DLCI 201 is minCIR, but if no voice packets are detected for 29 seconds, the sending rate will increase to CIR.

```
Router# show policy interface Serial3/1.1

 Serial3/1.1:DLCI 201 -

  Service-policy output:MQC-SHAPE-LLQ1

    Class-map:class-default (match-any)
      1434 packets, 148751 bytes
```

```
  30 second offered rate 14000 bps, drop rate 0 bps
  Match:any
  Traffic Shaping
       Target/Average   Byte   Sustain   Excess    Interval  Increment
         Rate           Limit  bits/int  bits/int  (ms)      (bytes)
        63000/63000     1890   7560      7560      120       945

    Adapt  Queue     Packets   Bytes     Packets   Bytes     Shaping
    Active Depth                       Delayed   Delayed   Active
    BECN   0         1434      162991    26        2704      yes
    Voice Adaptive Shaping active, time left 29 secs
```

Table 5 describes the significant fields shown in the display. Significant fields that are not described in Table 5 are described in Table 3, "show policy-map interface Field Descriptions."

***Table 5 show policy-map interface Field Descriptions—Configured for Frame Relay Voice-Adaptive Traffic Shaping***

| Field | Description |
|---|---|
| Voice Adaptive Shaping active/inactive | Indicates whether Frame Relay voice-adaptive traffic shaping is active or inactive. |
| time left | Number of seconds left on the Frame Relay voice-adaptive traffic shaping deactivation timer. |

### Two-Rate Traffic Policing show policy-map interface Command Example

The following is sample output from the **show policy-map interface** command when two-rate traffic policing has been configured. In the example below, 1.25 Mbps of traffic is sent ("offered") to a policer class.

```
Router# show policy-map interface serial3/0

 Serial3/0

  Service-policy output: policy1

   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
```

The two-rate traffic policer marks 500 kbps of traffic as conforming, 500 kbps of traffic as exceeding, and 250 kbps of traffic as violating the specified rate. Packets marked as conforming will be sent as is, and packets marked as exceeding will be marked with IP Precedence 2 and then sent. Packets marked as violating the specified rate are dropped.

Table 6 describes the significant fields shown in the display.

*Table 6 show policy-map interface Field Descriptions—Configured for Two-Rate Traffic Policing*

| Field | Description |
|---|---|
| police | Indicates that the **police** command has been configured to enable traffic policing. Also, displays the specified CIR, conform burst size, peak information rate (PIR), and peak burst size used for marking packets. |
| conformed | Displays the action to be taken on packets conforming to a specified rate. Displays the number of packets and bytes on which the action was taken. |
| exceeded | Displays the action to be taken on packets exceeding a specified rate. Displays the number of packets and bytes on which the action was taken. |
| violated | Displays the action to be taken on packets violating a specified rate. Displays the number of packets and bytes on which the action was taken. |

### Multiple Traffic Policing Actions show policy-map interface Command Example

The following is sample output from the **show policy-map** command when the Policer Enhancement — Multiple Actions feature has been configured. The sample output from the **show policy-map interface** command displays the statistics for the serial 3/2 interface, to which a service policy called "police" (configured as shown below) is attached.

```
policy-map police
  class class-default
   police cir 1000000 pir 2000000
     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

Router# show policy-map interface serial3/2

Serial3/2: DLCI 100 -

Service-policy output: police

    Class-map: class-default (match-any)
      172984 packets, 42553700 bytes
      5 minute offered rate 960000 bps, drop rate 277000 bps
      Match: any
     police:
         cir 1000000 bps, bc 31250 bytes, pir 2000000 bps, be 31250 bytes
       conformed 59679 packets, 14680670 bytes; actions:
         transmit
exceeded 59549 packets, 14649054 bytes; actions:
         set-prec-transmit 4
         set-frde-transmit
       violated 53758 packets, 13224468 bytes; actions:
         set-prec-transmit 2
         set-frde-transmit
       conformed 340000 bps, exceed 341000 bps, violate 314000 bps
```

The sample output from **show policy-map interface** command shows the following:

- 59679 packets were marked as conforming packets (that is, packets conforming to the CIR) and were transmitted unaltered.
- 59549 packets were marked as exceeding packets (that is, packets exceeding the CIR but not exceeding the PIR). Therefore, the IP Precedence value of these packets was changed to an IP Precedence level of 4, the discard eligibility (DE) bit was set to 1, and the packets were transmitted with these changes.
- 53758 packets were marked as violating packets (that is, exceeding the PIR). Therefore, the IP Precedence value of these packets was changed to an IP Precedence level of 2, the DE bit was set to 1, and the packets were transmitted with these changes.

**Note** Actions are specified by using the *action* argument of the **police** command. For more information about the available actions, see the **police** command reference page.

Table 7 describes the significant fields shown in the display.

***Table 7 show policy-map interface Field Descriptions—Configured for Multiple Traffic Policing Actions***

| Field | Description |
|---|---|
| police | Indicates that the **police** command has been configured to enable traffic policing. Also, displays the specified CIR, conform burst size (BC), PIR, and peak burst size (BE) used for marking packets. |
| conformed, packets, bytes, actions | Displays the number of packets (also shown in bytes) marked as conforming to a specified rate and the actions taken on the packet. If there are multiple actions, each action is listed separately. |
| exceeded, packets, bytes, actions | Displays the number of packets (also shown in bytes) marked as exceeding a specified rate and the actions taken on the packet. If there are multiple actions, each action is listed separately. |
| violated, packets, bytes, actions | Displays the number of packets (also shown in bytes) marked as violating a specified rate and the actions taken on the packet. If there are multiple actions, each action is listed separately. |

#### Explicit Congestion Notification show policy-map interface Command Example

The following is sample output from the **show policy-map interface** command when the WRED — Explicit Congestion Notification (ECN) feature has been configured. The words “explicit congestion notification” included in the output indicate that ECN has been enabled.

```
Router# show policy-map interface Serial4/1

 Serial4/1

  Service-policy output:policy_ecn
        Class-map:prec1 (match-all)
          1000 packets, 125000 bytes
          30 second offered rate 14000 bps, drop rate 5000 bps
          Match:ip precedence 1
          Weighted Fair Queueing
            Output Queue:Conversation 42
            Bandwidth 20 (%)
            Bandwidth 100 (kbps)
            (pkts matched/bytes matched) 989/123625
```

```
   (depth/total drops/no-buffer drops) 0/455/0
        exponential weight:9
        explicit congestion notification
        mean queue depth:0

class   Transmitted  Random drop  Tail drop   Minimum     Maximum     Mark
        pkts/bytes   pkts/bytes    pkts/bytes threshold   threshold   probability
  0       0/0          0/0          0/0          20          40         1/10
  1     545/68125      0/0          0/0          22          40         1/10
  2       0/0          0/0          0/0          24          40         1/10
  3       0/0          0/0          0/0          26          40         1/10
  4       0/0          0/0          0/0          28          40         1/10
  5       0/0          0/0          0/0          30          40         1/10
  6       0/0          0/0          0/0          32          40         1/10
  7       0/0          0/0          0/0          34          40         1/10
rsvp      0/0          0/0          0/0          36          40         1/10
class   ECN Mark
        pkts/bytes
  0     0/0
  1    43/5375
  2     0/0
  3     0/0
  4     0/0
  5     0/0
  6     0/0
  7     0/0
rsvp    0/0
```

Table 8 describes the significant fields shown in the display.

***Table 8 show policy-map interface Field Descriptions—Configured for ECN***

| Field | Description |
|---|---|
| explicit congestion notification | Indication that Explicit Congestion Notification is enabled. |
| mean queue depth | Average queue depth based on the actual queue depth on the interface and the exponential weighting constant. It is a moving average. The minimum and maximum thresholds are compared against this value to determine drop decisions. |
| class | IP precedence value. |
| Transmitted pkts/bytes | Number of packets (also shown in bytes) passed through WRED and not dropped by WRED.<br>**Note** If there is insufficient memory in the buffer to accommodate the packet, the packet can be dropped *after* the packet passes through WRED. Packets dropped because of insufficient memory in the buffer (sometimes referred to as "no-buffer drops") are not taken into account by the WRED packet counter. |
| Random drop pkts/bytes | Number of packets (also shown in bytes) randomly dropped when the mean queue depth is between the minimum threshold value and the maximum threshold value for the specified IP precedence value. |
| Tail drop pkts/bytes | Number of packets dropped when the mean queue depth is greater than the maximum threshold value for the specified IP precedence value. |
| Minimum threshold | Minimum WRED threshold in number of packets. |

*Table 8 show policy-map interface Field Descriptions—Configured for ECN (continued)*

| Field | Description |
|---|---|
| Maximum threshold | Maximum WRED threshold in number of packets. |
| Mark probability | Fraction of packets dropped when the average queue depth is at the maximum threshold. |
| ECN Mark pkts/bytes | Number of packets (also shown in bytes) marked by ECN. |

### Class-Based RTP and TCP Header Compression show policy-map interface Command Example

The following sample output from the **show policy-map interface** command shows the RTP header compression has been configured for a class called "prec2" in the policy map called "p1".

The **show policy-map interface** command output displays the type of header compression configured (RTP), the interface to which the policy map called "p1" is attached (Serial 4/1), the total number of packets, the number of packets compressed, the number of packets saved, the number of packets sent, and the rate at which the packets were compressed (in bits per second (bps)).

In this example, User Datagram Protocol (UDP)/RTP header compressions have been configured, and the compression statistics are included at the end of the display.

```
Router# show policy-map interface Serial4/1

Serial4/1

Service-policy output:p1

    Class-map:class-default (match-any)
      1005 packets, 64320 bytes
      30 second offered rate 16000 bps, drop rate 0 bps
      Match:any
compress:
          header ip rtp
          UDP/RTP Compression:
          Sent:1000 total, 999 compressed,
                41957 bytes saved, 17983 bytes sent
                3.33 efficiency improvement factor
                99% hit ratio, five minute miss rate 0 misses/sec, 0 max
                 rate 5000 bps
```

Table 9 describes the significant fields shown in the display.

*Table 9 show policy-map interface Field Descriptions—Configured for Class-Based RTP and TCP Header Compression[1]*

| Field | Description |
|---|---|
| Service-policy output | Name of the output service policy applied to the specified interface or VC. |
| Class-map | Class of traffic being displayed. Output is displayed for each configured class in the policy. The choice for implementing class matches (for example, match-all or match-any) can also appear next to the traffic class. |
| packets, bytes | Number of packets (also shown in bytes) identified as belonging to the class of traffic being displayed. |

*Table 9 show policy-map interface Field Descriptions—Configured for Class-Based RTP and TCP Header Compression[1] (continued)*

| Field | Description |
|---|---|
| offered rate | Rate, in kbps, of packets coming in to the class.<br>**Note** If the packets are compressed over an outgoing interface, the improved packet rate achieved by packet compression is not reflected in the offered rate. Also, if the packets are classified *before* they enter a combination of tunnels (for example, a generic routing encapsulation (GRE) tunnel and an IP Security (IPSec) tunnel), the offered rate does not include all the extra overhead associated with tunnel encapsulation in general. Depending on the configuration, the offered rate may include no overhead, may include the overhead for only *one* tunnel encapsulation, or may include the overhead for *all* tunnel encapsulations. In most of the GRE and IPSec tunnel configurations, the offered rate includes the overhead for GRE tunnel encapsulation only. |
| UDP/RTP Compression | Indicates that RTP header compression has been configured for the class. |
| Sent total | Count of every packet sent, both compressed packets and full-header packets. |
| Sent compressed | Count of number of compressed packets sent. |
| bytes saved | Total number of bytes saved (that is, bytes not needing to be sent). |
| bytes sent | Total number of bytes sent for both compressed and full-header packets. |
| efficiency improvement factor | The percentage of increased bandwidth efficiency as a result of header compression. For example, with RTP streams, the efficiency improvement factor can be as much as 2.9 (or 290 percent). |
| hit ratio | Used mainly for troubleshooting purposes, this is the percentage of packets found in the context database. In most instances, this percentage should be high. |
| five minute miss rate | The number of new traffic flows found in the last five minutes. |
| misses/sec<br>max | The average number of new traffic flows found per second, and the highest rate of new traffic flows to date. |
| rate | The actual traffic rate (in bits per second) after the packets are compressed. |

1. A number in parentheses may appear next to the service-policy output name and the class-map name. The number is for Cisco internal use only and can be disregarded.

### Modular QoS CLI (MQC) Unconditional Packet Discard show policy-map interface Command Example

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

 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
```

Table 10 describes the significant fields shown in the display.

***Table 10 show policy-map interface Field Descriptions—Configured for MQC Unconditional Packet Discard[1]***

| Field | Description |
|---|---|
| Service-policy output | Name of the output service policy applied to the specified interface or VC. |
| Class-map | Class of traffic being displayed. Output is displayed for each configured class in the policy. The choice for implementing class matches (for example, match-all or match-any) can also appear next to the traffic class. |
| packets, bytes | Number of packets (also shown in bytes) identified as belonging to the class of traffic being displayed. |
| offered rate | Rate, in kbps, of packets coming in to the class.<br>**Note** If the packets are compressed over an outgoing interface, the improved packet rate achieved by packet compression is not reflected in the offered rate. Also, if the packets are classified *before* they enter a combination of tunnels (for example, a generic routing encapsulation (GRE) tunnel and an IP Security (IPSec) tunnel), the offered rate does not include all the extra overhead associated with tunnel encapsulation in general. Depending on the configuration, the offered rate may include no overhead, may include the overhead for only *one* tunnel encapsulation, or may include the overhead for *all* tunnel encapsulations. In most of the GRE and IPSec tunnel configurations, the offered rate includes the overhead for GRE tunnel encapsulation only. |
| drop rate | Rate, in kbps, at which packets are dropped from the class. The drop rate is calculated by subtracting the number of successfully transmitted packets from the offered rate. |

*Table 10 show policy-map interface Field Descriptions—Configured for MQC Unconditional Packet Discard[1] (continued)*

| Field | Description |
|---|---|
| **Note** | In distributed architecture platforms (such as the C7500), the value of the tranfer rate, calculated as the difference between the offered rate and the drop rate counters, can sporadically diviate from the average by up to 20 percent or more. This can occur while no corresponding burst is registered by independent traffic analyser equipment |
| Match | Match criteria specified for the class of traffic. Choices include criteria such as the Layer 3 packet length, IP precedence, IP DSCP value, MPLS experimental value, access groups, and QoS groups. For more information about the variety of match criteria options available, refer to the chapter "Configuring the Modular Quality of Service Command-Line Interface" in the *Cisco IOS Quality of Service Solutions Configuration Guide*. |
| drop | Indicates that the packet discarding action for all the packets belonging to the specified class has been configured. |

1. A number in parentheses may appear next to the service-policy output name and the class-map name. The number is for Cisco internal use only and can be disregarded.

### Percentage-Based Policing and Shaping show policy-map interface Command Example

The following sample output from the **show policy-map interface** command shows traffic policing configured using a CIR based on a bandwidth of 20 percent. The CIR and committed burst (Bc) in milliseconds (ms) are included in the display.

```
Router# show policy-map interface Serial3/1

 Serial3/1

  Service-policy output: mypolicy

    Class-map: gold (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
      police:
          cir 20 % bc 10 ms
          cir 2000000 bps, bc 2500 bytes
          pir 40 % be 20 ms
          pir 4000000 bps, be 10000 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
```

Table 11 describes the significant fields shown in the display.

*Table 11 show policy-map interface Field Descriptions—Configured for Percentage-Based Policing and Shaping[1]*

| Field | Description |
|---|---|
| Service-policy output | Name of the output service policy applied to the specified interface or VC. |
| Class-map | Class of traffic being displayed. Output is displayed for each configured class in the policy. The choice for implementing class matches (for example, match-all or match-any) can also appear next to the traffic class. |
| packets, bytes | Number of packets (also shown in bytes) identified as belonging to the class of traffic being displayed. |
| offered rate | Rate, in kbps, of packets coming in to the class.<br>**Note** If the packets are compressed over an outgoing interface, the improved packet rate achieved by packet compression is not reflected in the offered rate. Also, if the packets are classified *before* they enter a combination of tunnels (for example, a generic routing encapsulation (GRE) tunnel and an IP Security (IPSec) tunnel), the offered rate does not include all the extra overhead associated with tunnel encapsulation in general. Depending on the configuration, the offered rate may include no overhead, may include the overhead for only *one* tunnel encapsulation, or may include the overhead for *all* tunnel encapsulations. In most of the GRE and IPSec tunnel configurations, the offered rate includes the overhead for GRE tunnel encapsulation only. |
| police | Indicates that traffic policing based on a percentage of bandwidth has been enabled. Also, displays the bandwidth percentage, the CIR, and the committed burst (Bc) size in ms. |
| conformed, actions | Displays the number of packets and bytes marked as conforming to the specified rates, and the action to be taken on those packets. |
| exceeded, actions | Displays the number of packets and bytes marked as exceeding the specified rates, and the action to be taken on those packets. |

1. A number in parentheses may appear next to the service-policy output name and the class-map name. The number is for Cisco internal use only and can be disregarded.

#### Traffic Shaping show policy-map interface Command Example

The following sample output from the **show policy-map interface** command (shown below) displays the statistics for the serial 3/2 interface. Traffic shaping has been enabled on this interface, and an average rate of 20 percent of the bandwidth has been specified.

```
Router# show policy-map interface Serial3/2

Serial3/2

  Service-policy output: p1

    Class-map: c1 (match-all)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
```

```
Traffic Shaping
  Target/Average      Byte   Sustain    Excess      Interval  Increment  Adapt
  Rate              Limit  bits/int  bits/int    (ms)     (bytes)   Active
   20 %                        10 (ms)    20 (ms)
  201500/201500       1952   7808       7808        38         976       -

  Queue     Packets   Bytes     Packets   Bytes     Shaping
  Depth                         Delayed   Delayed   Active
  0         0         0         0         0         no
```

Table 12 describes the significant fields shown in the display.

***Table 12 show policy-map interface Field Descriptions—Configured for Percentage-Based Policing and Shaping (with Traffic Shaping Enabled)[1]***

| Field | Description |
|---|---|
| Service-policy output | Name of the output service policy applied to the specified interface or VC. |
| Class-map | Class of traffic being displayed. Output is displayed for each configured class in the policy. The choice for implementing class matches (for example, match-all or match-any) can also appear next to the traffic class. |
| packets, bytes | Number of packets (also shown in bytes) identified as belonging to the class of traffic being displayed. |
| offered rate | Rate, in kbps, of packets coming in to the class.<br>**Note** If the packets are compressed over an outgoing interface, the improved packet rate achieved by packet compression is not reflected in the offered rate. Also, if the packets are classified *before* they enter a combination of tunnels (for example, a generic routing encapsulation (GRE) tunnel and an IP Security (IPSec) tunnel), the offered rate does not include all the extra overhead associated with tunnel encapsulation in general. Depending on the configuration, the offered rate may include no overhead, may include the overhead for only *one* tunnel encapsulation, or may include the overhead for *all* tunnel encapsulations. In most of the GRE and IPSec tunnel configurations, the offered rate includes the overhead for GRE tunnel encapsulation only. |
| drop rate | Rate, in kbps, at which packets are dropped from the class. The drop rate is calculated by subtracting the number of successfully transmitted packets from the offered rate. |
| Match | Match criteria specified for the class of traffic. Choices include criteria such as the Layer 3 packet length, IP precedence, IP DSCP value, MPLS experimental value, access groups, and quality of service (QoS) groups. For more information about the variety of match criteria options that are available, refer to the chapter “Configuring the Modular Quality of Service Command-Line Interface” in the *Cisco IOS Quality of Service Solutions Configuration Guide*, Release 12.2. |
| Traffic Shaping | Indicates that traffic shaping based on a percentage of bandwidth has been enabled. |
| Target /Average Rate | Rate (percentage) used for shaping traffic and the number of packets meeting that rate. |

*Table 12 show policy-map interface Field Descriptions—Configured for Percentage-Based Policing and Shaping (with Traffic Shaping Enabled)[1] (continued)*

| Field | Description |
|---|---|
| Byte Limit | Maximum number of bytes that can be transmitted per interval. Calculated as follows:<br>((Bc+Be) /8 ) x 1 |
| Sustain bits/int | Committed burst (Bc) rate. |
| Excess bits/int | Excess burst (Be) rate. |
| Interval (ms) | Time interval value in milliseconds (ms). |
| Increment (bytes) | Number of credits (in bytes) received in the token bucket of the traffic shaper during each time interval. |
| Adapt Active | Indicates whether adaptive shaping is enabled. |
| Queue Depth | Current queue depth of the traffic shaper. |
| Packets | Total number of packets that have entered the traffic shaper system. |
| Bytes | Total number of bytes that have entered the traffic shaper system. |
| Packets Delayed | Total number of packets delayed in the queue of the traffic shaper before being transmitted. |
| Bytes Delayed | Total number of bytes delayed in the queue of the traffic shaper before being transmitted. |
| Shaping Active | Indicates whether the traffic shaper is active. For example, if a traffic shaper is active, and the traffic being sent exceeds the traffic shaping rate, a “yes” appears in this field. |

1. A number in parentheses may appear next to the service-policy output name, class-map name, and match criteria information. The number is for Cisco internal use only and can be disregarded.

### Packet Classification Based on Layer 3 Packet Length show policy-map interface Command Example

The following sample output from the **show policy-map interface** command displays the packet statistics for the Ethernet4/1 interface, to which a service policy called “mypolicy” is attached. The Layer 3 packet length has been specified as a match criterion for the traffic in the class called “class1”.

```
Router# show policy-map interface Ethernet4/1

 Ethernet4/1

  Service-policy input: mypolicy

    Class-map: class1 (match-all)
       500 packets, 125000 bytes
       5 minute offered rate 4000 bps, drop rate 0 bps
       Match: packet length min 100 max 300
       QoS Set
         qos-group 20
           Packets marked 500
```

Table 13 describes the significant fields shown in the display.

***Table 13 show policy-map interface Field Descriptions—Configured for Packet Classification Based on Layer 3 Packet Length[1]***

| Field | Description |
|---|---|
| Service-policy input | Name of the input service policy applied to the specified interface or VC. |
| Class-map | Class of traffic being displayed. Output is displayed for each configured class in the policy. The choice for implementing class matches (for example, match-all or match-any) can also appear next to the traffic class. |
| packets, bytes | Number of packets (also shown in bytes) identified as belonging to the class of traffic being displayed. |
| offered rate | Rate, in kbps, of packets coming in to the class.<br>**Note** If the packets are compressed over an outgoing interface, the improved packet rate achieved by packet compression is not reflected in the offered rate. Also, if the packets are classified *before* they enter a combination of tunnels (for example, a generic routing encapsulation (GRE) tunnel and an IP Security (IPSec) tunnel), the offered rate does not include all the extra overhead associated with tunnel encapsulation in general. Depending on the configuration, the offered rate may include no overhead, may include the overhead for only *one* tunnel encapsulation, or may include the overhead for *all* tunnel encapsulations. In most of the GRE and IPSec tunnel configurations, the offered rate includes the overhead for GRE tunnel encapsulation only. |
| drop rate | Rate, in kbps, at which packets are dropped from the class. The drop rate is calculated by subtracting the number of successfully transmitted packets from the offered rate. |
| Match | Match criteria specified for the class of traffic. Choices include criteria such as the Layer 3 packet length, IP precedence, IP DSCP value, MPLS experimental value, access groups, and QoS groups. |
| QoS Set, qos-group, Packets marked | Indicates that class-based packet marking based on the QoS group has been configured. Includes the qos-group number and the number of packets marked. |

1. A number in parentheses may appear next to the service-policy input name, class-map name, and match criteria information. The number is for Cisco internal use only and can be disregarded.

### Enhanced Packet Marking show policy-map interface Command Example

The following sample output of the **show policy-map interface** command shows the service policies attached to a FastEthernet subinterface. In this example, a service policy called “policy1” has been attached. In “policy1”, a table map called “table-map1” has been configured. The values in “table-map1” will be used to map the precedence values to the corresponding class of service (CoS) values.

```
Router# show policy-map interface

 FastEthernet1/0.1

  Service-policy input: policy1

    Class-map: class-default (match-any)
      0 packets, 0 bytes
```

```
    5 minute offered rate 0 bps, drop rate 0 bps
    Match: any
    QoS Set
      precedence cos table table-map1
        Packets marked 0
```

Table 14 describes the fields shown in the display.

***Table 14 show policy-map interface Field Descriptions—Configured for Enhanced Packet Marking [1]***

| Field | Description |
|---|---|
| Service-policy input | Name of the input service policy applied to the specified interface or VC. |
| Class-map | Class of traffic being displayed. Output is displayed for each configured class in the policy. The choice for implementing class matches (for example, match-all or match-any) can also appear next to the traffic class. |
| packets, bytes | Number of the packets (also shown in bytes) identified as belonging to the class of traffic being displayed. |
| offered rate | Rate, in kbps, of the packets coming into the class. |
| Match | Match criteria specified for the class of traffic. Choices include criteria such as Precedence, IP differentiated services code point (DSCP) value, Multiprotocol Label Switching (MPLS) experimental value, access groups, and quality of service (QoS) group (set). For more information about the variety of match criteria options that are available, refer to the "Configuring the Modular Quality of Service Command-Line Interface" section in the *Cisco IOS Quality of Service Solutions Configuration Guide*. |
| QoS Set | Indicates that QoS group (set) has been configured for the particular class. |
| precedence cos table table-map1 | Indicates that a table map (called "table-map1") has been used to determine the precedence value. The precedence value will be set according to the CoS value defined in the table map. |
| Packets marked | Total number of packets marked for the particular class. |

1. A number in parentheses may appear next to the service-policy input name and the class-map name. The number is for Cisco internal use only and can be disregarded.

### Traffic Policing show policy-map interface Command Example

The following is sample output from the **show policy-map interface** command. This sample displays the statistics for the serial 2/0 interface on which traffic policing has been enabled. The committed (conform) burst (bc) and excess (peak) burst (be) are specified in milliseconds (ms).

```
Router# show policy-map interface serial2/0

 Serial2/0

  Service-policy output: policy1 (1050)

    Class-map: class1 (match-all) (1051/1)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: ip precedence 0  (1052)
      police:
          cir 20 % bc 300 ms
          cir 409500 bps, bc 15360 bytes
          pir 40 % be 400 ms
```

```
        pir 819000 bps, be 40960 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) (1054/0)
    0 packets, 0 bytes
    5 minute offered rate 0 bps, drop rate 0 bps
    Match: any  (1055)
      0 packets, 0 bytes
      5 minute rate 0 bps
```

In this example, the CIR and PIR are displayed in bps, and both the committed burst (bc) and excess burst (be) are displayed in bits.

The CIR, PIR bc, and be are calculated on the basis of the formulas described below.

#### Formula for Calculating the CIR

When calculating the CIR, the following formula is used:

- CIR percentage specified (as shown in the output from the **show policy-map** command) * bandwidth (BW) of the interface (as shown in the output from the **show interfaces** command) = total bits per second

According to the output from the **show interfaces** command for the serial 2/0 interface, the interface has a bandwidth (BW) of 2048 kbps.

```
Router # show interfaces serial2/0

Serial2/0 is administratively down, line protocol is down
  Hardware is M4T
  MTU 1500 bytes, BW 2048 Kbit, DLY 20000 usec, rely 255/255, load 1/255
```

The following values are used for calculating the CIR:

20 % * 2048 kbps = 409600 bps

#### Formula for Calculating the PIR

When calculating the PIR, the following formula is used:

- PIR percentage specified (as shown in the output from the **show policy-map** command) * bandwidth (BW) of the interface (as shown in the output from the **show interfaces** command) = total bits per second

According to the output from the **show interfaces** command for the serial 2/0 interface, the interface has a bandwidth (BW) of 2048 kbps.

```
Router # show interfaces serial2/0

Serial2/0 is administratively down, line protocol is down
  Hardware is M4T
  MTU 1500 bytes, BW 2048 Kbit, DLY 20000 usec, rely 255/255, load 1/255
```

The following values are used for calculating the PIR:

40 % * 2048 kbps = 819200 bps

**Note** Discrepancies between this total and the total shown in the output from the **show policy-map interface** command can be attributed to a rounding calculation or to differences associated with the specific interface configuration.

#### Formula for Calculating the Committed Burst (bc)

When calculating the bc, the following formula is used:

- The bc in milliseconds (as shown in the **show policy-map** command) * the CIR in bits per seconds = total number bytes

The following values are used for calculating the bc:

300 ms * 409600 bps = 15360 bytes

#### Formula for Calculating the Excess Burst (be)

When calculating the bc and the be, the following formula is used:

- The be in milliseconds (as shown in the **show policy-map** command) * the PIR in bits per seconds = total number bytes

The following values are used for calculating the be:

400 ms * 819200 bps = 40960 bytes

Table 15 describes the significant fields shown in the display.

***Table 15 show policy-map interface Field Descriptions***

| Field | Description |
|---|---|
| Service-policy output | Name of the output service policy applied to the specified interface or VC. |
| Class-map | Class of traffic being displayed. Output is displayed for each configured class in the policy. The choice for implementing class matches (for example, match-all or match-any) can also appear next to the traffic class. |
| packets and bytes | Number of packets (also shown in bytes) identified as belonging to the class of traffic being displayed. |
| offered rate | Rate, in kbps, of packets coming in to the class. |
| drop rate | Rate, in kbps, at which packets are dropped from the class. The drop rate is calculated by subtracting the number of successfully transmitted packets from the offered rate. |
| Match | Match criteria specified for the class of traffic. Choices include criteria such as the Layer 3 packet length, IP precedence, IP differentiated services code point (DSCP) value, Multiprotocol Label Switching (MPLS) experimental value, access groups, and quality of service (QoS) groups. For more information about the variety of match criteria options that are available, refer to the "Configuring the Modular Quality of Service Command-Line Interface" chapter of the *Cisco IOS Quality of Service Solutions Configuration Guide*. |
| police | Indicates that traffic policing has been enabled. Display includes the CIR, PIR (in both a percentage of bandwidth and in bps) and the bc and be in bytes and milliseconds. Also displays the optional conform, exceed, and violate actions, if any, and the statistics associated with these optional actions. |

### Bandwidth Estimation show policy-map interface Command Example

The following sample output from the **show policy-map interface** command displays statistics for the FastEthernet 0/1 interface on which bandwidth estimates for quality of service (QoS) targets have been generated.

The Bandwidth Estimation section indicates that bandwidth estimates for QoS targets have been defined. These targets include the packet loss rate, the packet delay rate, and the timeframe in milliseconds. Confidence refers to the drop-one-in value (as a percentage) of the targets. Corvil Bandwidth means the bandwidth estimate in kilobits per second.

When no drop or delay targets are specified, “none specified, falling back to drop no more than one packet in 500” appears in the output.

```
Router# show policy-map interface FastEthernet0/1

 FastEthernet0/1

  Service-policy output: my-policy

    Class-map: icmp (match-all)
      199 packets, 22686 bytes
      30 second offered rate 0 bps, drop rate 0 bps
      Match: access-group 101
      Bandwidth Estimation:
        Quality-of-Service targets:
          drop no more than one packet in 1000 (Packet loss < 0.10%)
          delay no more than one packet in 100 by 40 (or more) milliseconds
            (Confidence: 99.0000%)
        Corvil Bandwidth: 1 kbits/sec

    Class-map: class-default (match-any)
      112 packets, 14227 bytes
      30 second offered rate 0 bps, drop rate 0 bps
      Match: any
      Bandwidth Estimation:
        Quality-of-Service targets:
          <none specified, falling back to drop no more than one packet in 500
        Corvil Bandwidth: 1 kbits/sec
```

### Shaping with HQF Enabled show policy-map interface Command Example

The following sample output from the **show policy-map interface** command shows that shaping is active (as seen in the queue depth field) with HQF enabled on the serial 4/3 interface. All traffic is classified to the class-default queue.

```
Router# show policy-map interface serial4/3

 Serial4/3

  Service-policy output: shape

    Class-map: class-default (match-any)
      2203 packets, 404709 bytes
      30 second offered rate 74000 bps, drop rate 14000 bps
      Match: any
      Queueing
      queue limit 64 packets
      (queue depth/total drops/no-buffer drops) 64/354/0
      (pkts output/bytes output) 1836/337280
      shape (average) cir 128000, bc 1000, be 1000
      target shape rate 128000
        lower bound cir 0,  adapt to fecn 0
```

```
Service-policy : LLQ

  queue stats for all priority classes:

    queue limit 64 packets
    (queue depth/total drops/no-buffer drops) 0/0/0
    (pkts output/bytes output) 0/0

  Class-map: c1 (match-all)
    0 packets, 0 bytes
    30 second offered rate 0 bps, drop rate 0 bps
    Match: ip precedence 1
    Priority: 32 kbps, burst bytes 1500, b/w exceed drops: 0

  Class-map: class-default (match-any)
    2190 packets, 404540 bytes
    30 second offered rate 74000 bps, drop rate 14000 bps
    Match: any

    queue limit 64 packets
    (queue depth/total drops/no-buffer drops) 63/417/0
    (pkts output/bytes output) 2094/386300
```

## Related Commands

| Command | Description |
|---|---|
| **compression header ip** | Configures RTP or TCP IP header compression for a specific class. |
| **drop** | Configures a traffic class to discard packets belonging to a specific class. |
| **match fr-dlci** | Specifies the Frame Relay DLCI number as a match criterion in a class map. |
| **match packet length (class-map)** | Specifies the length of the Layer 3 packet in the IP header as a match criterion in a class map. |
| **police** | Configures traffic policing. |
| **police (percent)** | Configures traffic policing on the basis of a percentage of bandwidth available on an interface. |
| **police (two rates)** | Configures traffic policing using two rates, the CIR and the PIR. |
| **policy-map** | Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy. |
| **random-detect ecn** | Enables ECN. |
| **shape (percent)** | Specifies average or peak rate traffic shaping on the basis of a percentage of bandwidth available on an interface. |
| **show frame-relay pvc** | Displays statistics about PVCs for Frame Relay interfaces. |
| **show interfaces** | Displays statistics for all interfaces configured on a router or access server. |
| **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 class** | Displays the configuration for the specified class of the specified policy map. |
| **show table-map** | Displays the configuration of a specified table map or of all table maps. |
| **table-map (value mapping)** | Creates and configures a mapping table for mapping and converting one packet-marking value to another. |