QoS: Tunnel Marking for L2TPv3 Tunnels

First Published: May 7, 2004
Last Updated: February 28, 2006

The QoS: Tunnel Marking for Layer 2 Tunnel Protocol Version 3 (L2TPv3) Tunnels feature introduces the capability to define and control the quality of service (QoS) for incoming customer traffic on the provider edge (PE) router in a service provider network.

History for the QoS: Tunnel Marking for L2TPv3 Tunnels Feature

Release	Modification
12.0(28)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

Prerequisites for QoS: Tunnel Marking for L2TPv3 Tunnels

- Cisco Express Forwarding (CEF) must be configured on the interface before L2TPv3 tunnel marking can be used.

For information on CEF switching, consult the "Cisco Express Forwarding" section of the *Cisco IOS Switching Services Configuration Guide*.

- Determine the topology and interfaces that need to be configured to mark incoming traffic.

Restrictions for QoS: Tunnel Marking for L2TPv3 Tunnels

- L2TPv3 tunnel marking is supported in input policy-maps only and should not be configured for output policy-maps.
- L2TPv3 tunnel marking is not supported on generic routing encapsulation (GRE) tunnel interfaces.
- It is possible to configure L2TPv3 tunnel marking and the **ip tos** command at the same time. However, Modular Quality of Service (QoS) Command-Line Interface (CLI) (MQC) (L2TPv3) tunnel marking has higher priority over IP ToS commands, meaning that tunnel marking always rewrites the IP header of the tunnel packet and overwrites the values set by **ip tos** commands. The priority of enforcement is as follows when these commands are used simultaneously:
  1. **set ip dscp tunnel** or **set ip precedence tunnel** (L2TPv3 tunnel marking)
  2. **ip tos reflect**
  3. **ip tos** *tos-value*

Note This is designed behavior. We recommend that you configure only L2TPv3 tunnel marking and reconfigure any peers configured with the **ip tos** command to use L2TPv3 tunnel marking.

Information About QoS: Tunnel Marking for L2TPv3 Tunnels

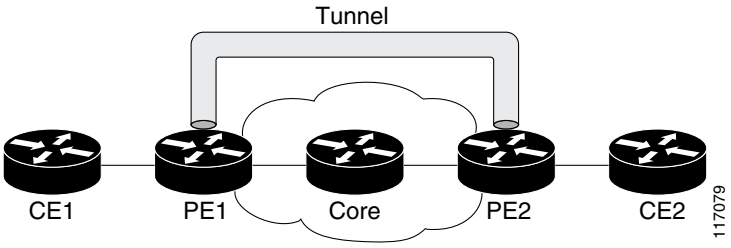
L2TPv3 Tunnel Marking Overview

The QoS: Tunnel Marking for L2TPv3 Tunnels feature allows you to define and control QoS for incoming customer traffic on the PE router in a service provider (SP) network. This feature lets you set (mark) either the IP precedence value or the differentiated services code point (DSCP) in the header of an L2TPv3 tunneled packet. L2TPv3 tunnel marking can be implemented by using a QoS marking command, such as **set ip** {**dscp** | **precedence**} [**tunnel**], and it can also be implemented in QoS traffic

policing. This feature simplifies administrative overhead previously required to control customer bandwidth by allowing you to mark the L2TPv3 tunnel header on the incoming interface on the PE routers.

Figure 1 shows traffic being received from CE1 through PE1's incoming interface on which tunnel marking occurs. The traffic is encapsulated (tunneled) and the tunnel header is marked on PE1. The marked packets travel (tunnel) through the core and are decapsulated automatically on PE2's exit interface. This feature is designed to simplify classifying CE traffic and is configured only in the service provider network. This process is transparent to the customer sites. CE1 and CE2 simply exist as a single network.

Figure 1 Sample Tunnel Marking Topology



Defining Class and Policy Maps for L2TPv3 Tunnel Marking Using the MQC

To configure the tunnel marking for L2TPv3 tunnels, you must define a traffic class, configure a policy map, and then attach that policy map to the appropriate interface. These three tasks can be accomplished by using the MQC.

For information on the MQC, defining class and policy maps, consult the Modular Quality of Service Command-Line Interface section of the *Cisco IOS Quality of Service Solutions Configuration Guide*.

Configuring L2TPv3 Tunnel Marking

L2TPv3 tunnel marking is configured with the **set ip precedence tunnel** or **set ip dscp tunnel** command on PE routers that carry incoming traffic from customer sites. L2TPv3 tunnel marking allows you to mark the header of a L2TPv3 tunnel by setting a DSCP value from 0 to 63 or an IP precedence value from 0 to 7 to control L2TPv3 tunnel traffic bandwidth and priority.

L2TPv3 traffic can also be marked under traffic policing with the **set-dscp-tunnel-transmit** and the **set-prec-tunnel-transmit** commands. The tunnel marking value is from 0 to 63 for the **set-dscp-tunnel-transmit** command and from 0 to 7 for the **set-prec-tunnel-transmit** command. Under traffic policing, tunnel marking can be applied with “conform” and “exceed” action statements, allowing you to automatically apply a different value for traffic that does not conform to the expected traffic rate.

After the tunnel header is marked, L2TPv3 traffic is carried through the tunnel and across the service provider network. This traffic is decapsulated on the interface of the PE router that carries the outgoing traffic to the other customer site. The configuration of L2TPv3 tunnel marking is transparent to customer sites. All internal configuration is preserved.

It is important to distinguish between the **set ip precedence** and **set ip dscp** commands and the **set ip precedence tunnel** and **set ip dscp tunnel** commands.

- The **set ip precedence** and **set ip dscp** commands are used to set the IP precedence or DSCP values in the header of an IP packet.

- The **set ip precedence tunnel** or **set ip dscp tunnel** commands are used set (mark) the IP precedence or DSCP value in the tunnel header that encapsulates the Layer 2 traffic.

Benefits of L2TPv3 Tunnel Marking

L2TPv3 Tunnel Marking Simplifies Customer Bandwidth Control at the Service Provider Site

L2TPv3 tunnel marking provides a simple mechanism to control the bandwidth of customer L2TPv3 traffic. This feature is configured entirely within the service provider network and only on interfaces that carry incoming traffic on the PE routers.

L2TPv3 Tunnel Marking Requires No Changes to Customer Configurations

The configuration of this feature is transparent to the customer sites and requires no configuration changes and has no impact on customer configurations.

L2TPv3 Definition

L2TPv3 is an Internet Engineering Task Force (IETF) Layer 2 Tunneling Protocol Extensions (l2tpext) working group draft that provides several enhancements to L2TP for the capability to tunnel any Layer 2 payload over L2TP. Specifically, L2TPv3 defines the L2TP protocol for tunneling Layer 2 payloads over an IP core network using Layer 2 virtual private networks (VPNs).

For information about L2TPv3, refer to the *Layer 2 Tunnel Protocol Version 3* Cisco IOS Release 12.0(25)S feature module.

How to Configure QoS: Tunnel Marking for L2TPv3 Tunnels

The QoS: Tunnel Marking for L2TPv3 Tunnels feature introduces the capability for a service provider to define and control customer traffic bandwidth and priority on the interfaces of PE routers that carry incoming traffic. This section contains the following procedures.

- Configuring a Class Map, page 4 (required)
- Creating a Policy Map, page 6 (required)
- Attaching the Policy Map to an Interface or a VC, page 8 (required)
- Verifying the Configuration, page 10 (optional)

Configuring a Class Map

To configure a class map, perform the following task.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **class-map** [**match-all** | **match-any**] *class-map-name*
4. **match** *l2tpv3-match-criteria*

5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**class-map** [**match-all** | **match-any**] *class-map-name* **Example:** `Router(config)# class-map MATCH_FRDE`	Specifies the name of the class map to be created and enters class-map configuration mode. The class map defines the criteria to use to differentiate the traffic. For example, you can use the class map to differentiate voice traffic from data traffic, based on a series of match criteria defined using the **match** command. • Enter class map name. **Note** If the **match-all** or **match-any** keyword is not specified, traffic must match all the match criteria to be classified as part of the traffic class.
Step 4	**match** *l2tpv3-match-criteria* **Example:** `Router(config-cmap)# match fr-de`	Enables packet matching based on the specified class. You can enter one of three following **match** commands to define L2TPv3 match criteria tunnel marking: • **match atm clp** • **match cos** • **match fr-de** **Note** This is an example of one match criterion that you can configure with a **match** command. Other criteria include matching on the IP precedence, access-group, or protocol. Enter the **match** command for the criterion you want to specify. For more information about specifying match criteria using the MQC, refer to the "Configuring the Modular Quality of Service Command-Line Interface" chapter of the *Cisco IOS Quality of Service Solutions Configuration Guide*.
Step 5	**exit** **Example:** `Router(config-cmap)# exit`	(Optional) Exits class-map configuration mode and enters global configuration mode.

Creating a Policy Map

To create a policy map and configure it to set either the precedence or the DSCP value in the header of a L2TPv3 tunneled packet, perform the following tasks.

L2TPv3 Tunnel Marking and Traffic Policing

Traffic policing 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). If you use traffic policing in your network, you can also implement the L2TPv3 tunnel marking feature with the **set-dscp-tunnel-transmit** or **set-prec-tunnel-transmit** traffic policing commands in policy-map class configuration mode. Under traffic policing, tunnel marking can be applied with "conform" and "exceed" action statements, allowing you to apply a different value automatically for traffic that does not conform to the expected traffic rate.

L2TPv3 Tunnel Marking Values

The range of the tunnel marking values for the **set ip dscp tunnel** and **set-dscp-tunnel-transmit** commands is from 0 to 63; and the range of values for the **set ip precedence tunnel** and **set-prec-tunnel-transmit** commands is from 0 to 7.

Restrictions

It is possible to configure L2TPv3 tunnel marking and the **ip tos** command at the same time. However, MQC (L2TPv3) tunnel marking has higher priority over IP ToS commands, meaning that tunnel marking will always rewrite the IP header of the tunnel packet, overwriting the values set by **ip tos** commands. The order of enforcement is as follows when these commands are used simultaneously:

1. **set ip dscp tunnel** or **set ip precedence tunnel** (L2TPv3 tunnel marking)
2. **ip tos reflect**
3. **ip tos** *tos-value*

Note This is designed behavior. We recommend that you configure only L2TPv3 tunnel marking and reconfigure any peers, configured with the **ip tos** command, to use L2TPv3 tunnel marking.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map** *policy-map-name*
4. **class** {*class-name* | **class-default**}
5. **set ip dscp tunnel** *dscp-value*

   or

   set ip precedence tunnel *precedence-value*

   or

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

6. **exit**
7. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**policy-map** *policy-map-name* **Example:** `Router(config)# policy-map TUNNEL_MARKING`	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. • Enter the policy map name.
Step 4	**class** {*class-name* | **class-default**} **Example:** `Router(config-pmap)# class MATCH_FRDE`	Specifies the name of the class whose policy you want to create or change or specifies the default class (commonly known as the class-default class) before you configure its policy. Also enters policy-map class mode. • Enter the class name or enter the **class-default** keyword.
Step 5	**set ip dscp tunnel** *dscp-value* **Example:** `Router(config-pmap-c)# set ip dscp tunnel 3`	Sets or marks the differentiated services code point (DSCP) value in the tunnel header of a Layer 2 Tunnel Protocol Version 3 (L2TPv3) tunneled packet on the ingress interface. The tunnel marking value is a number from 0 to 63 when configuring DSCP. • Enter the tunnel value.
	or **set ip precedence tunnel** *precedence-value* **Example:** `Router(config-pmap-c)# set ip precedence tunnel 3`	Sets or marks the IP precedence value in the tunnel header of a Layer 2 Tunnel Protocol Version 3 (L2TPv3) tunneled packet on the ingress interface. The tunnel marking value is a number from 0 to 7 when configuring IP precedence. • Enter the tunnel value.

	Command or Action	Purpose
	or **police** *bps* [*burst-normal*] [*burst-max*] **conform-action** *action* **exceed-action** *action* [**violate-action** *action*] **Example:** `Router(config-pmap-c)# police 8000 conform-action set-dscp-tunnel-transmit 4 exceed-action set-dscp-tunnel-transmit 0` or `Router(config-pmap-c)# police 8000 conform-action set-prec-tunnel-transmit 4 exceed-action set-prec-tunnel-transmit 0`	Configures traffic policing on the basis of the bits per second (bps) specified and the actions specified. If you use traffic policing in your network, you can implement the L2TPv3 tunnel marking feature with the **set-dscp-tunnel-transmit** or **set-prec-tunnel-transmit** traffic policing commands instead of the **set ip dscp tunnel** or the **set ip precedence tunnel** commands shown in Step 5. The tunnel marking value for the traffic policing commands is from 0 to 63 when using **set-dscp-tunnel-transmit** and from 0 to 7 when using **set-prec-tunnel-transmit**. • Enter the bps, any optional burst sizes, and the desired conform and exceed actions. • Enter the **set-dscp-tunnel-transmit** or **set-prec-tunnel-transmit** commands after the **conform-action** keyword. **Note** This is an example of one QoS feature you can configure at this step. Other QoS features include Weighted Random Early Detection (WRED), Weighted Fair Queueing (WFQ), and traffic shaping. Enter the command for the specific QoS feature you want to configure. For more information about QoS features, refer to *Cisco IOS Quality of Service Solutions Configuration Guide*, Release 12.3.
Step 6	**exit** **Example:** `Router(config-pmap-c)# exit`	(Optional) Exits policy-map class configuration mode and enters policy-map configuration mode.
Step 7	**exit** **Example:** `Router(config-pmap)# exit`	(Optional) Exits policy-map configuration mode and enters global configuration mode.

Attaching the Policy Map to an Interface or a VC

To attach the policy map to an interface or a virtual circuit (VC), perform the following task.

Restrictions

Policy maps can be attached to main interfaces, subinterfaces, or ATM permanent virtual circuits (PVCs). Policy maps are attached to interfaces by using the **service-policy** command and specifying either the **input** or **output** keyword s to indicate the direction of the interface. This feature is supported only on ingress interfaces with the **input** keyword and should not be configured on egress interfaces with the **output** keyword.

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** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* [*name-tag*] **Example:** `Router(config)# interface serial 0`	Configures the interface type specified and enters interface configuration mode. • Enter interface type.
Step 4	**pvc** [*name*] *vpi*/*vci* [**ilmi** | **qsaal** | **smds**] **Example:** `Router(config-if)# pvc cisco 0/16 ilmi`	Creates or assigns a name to an ATM PVC, specifies the encapsulation type on an ATM PVC, and enters ATM virtual circuit configuration mode.
Step 5	**service-policy** {**input** | **output**} *policy-map-name* **Example:** `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. • 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. • Enter the **input** keyword followed by the policy map name. **Note** For this feature, only the incoming interface configured with the **input** keyword is supported.
Step 6	**exit** **Example:** `Router(config-if)# exit`	(Optional) Exits interface configuration mode.

Verifying the Configuration

To verify that the feature is configured as intended and that either the IP precedence or DSCP value is set as expected, complete the following steps.

SUMMARY STEPS

1. **enable**
2. **show policy-map interface** *interface-name*

   and/or
3. **show policy-map** *policy-map*
4. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show policy-map interface** *interface-name* **Example:** `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. • Enter the interface name.
and/or		
Step 3	**show policy-map** *policy-map*	Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps. • Enter a policy map name.
Step 4	**exit** **Example:** `Router# exit`	(Optional) Exits privileged EXEC 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, you find that the configuration is not correct or the feature is not functioning as expected, perform these operations.

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.

Configuration Examples for QoS: Tunnel Marking L2TPv3 Tunnels

This section provides the following configuration examples:

- Configuring Tunnel Marking on L2TPv3 Tunnels: Example, page 11
- Verifying the Tunnel Marking on L2TPv3 Tunnels Configuration: Example, page 12

Configuring Tunnel Marking on L2TPv3 Tunnels: Example

The following is an example of a L2TPv3 tunnel marking configuration. In this sample, a class map called “MATCH_FRDE” has been configured to match traffic based on the Frame Relay DE bit.

```
Router> enable
Router# configure terminal
Router(config)# class-map MATCH_FRDE
Router(config-cmap)# match fr-de
Router(config-cmap)# exit
```

In this part of the example configuration, a policy map called “TUNNEL_MARKING” has been created and the **set ip dscp tunnel** command has been configured in the policy map. You could use the **set ip precedence tunnel** command instead of the **set ip dscp tunnel** command if you do not use DSCP in your network.

```
Router(config)# policy-map TUNNEL_MARKING
Router(config-pmap)# class MATCH_FRDE
Router(config-pmap-c)# set ip dscp tunnel 3
Router(config-pmap-c)# end
```

Note This next part of the example configuration is not required to configure this feature if you use the **set ip dscp tunnel** or **set ip precedence tunnel** commands to enable L2TPv3 tunnel marking. This example shows how L2TPv3 tunnel marking can be enabled under traffic policing.

In this part of the example configuration, the policy map called “TUNNEL_MARKING” has been created and traffic policing has also been configured by using the **police** command and specifying the appropriate policing actions. The **set-dscp-tunnel-transmit** command can be used instead of the **set-prec-tunnel-transmit** if you use DSCP in your network.

```
Router(config)# policy-map TUNNEL_MARKING
Router(config-pmap)# class class-default
Router(config-pmap-c)# police 8000 conform-action set-prec-tunnel-transmit 4 exceed-action
set-prec-tunnel-transmit 0
Router(config-pmap-c)# end
```

In the final part of the example configuration, the policy map is attached to serial interface 0 in the inbound (input) direction by specifying the **input** keyword of the **service-policy** command.

```
Router(config)# interface serial 0
Router(config-if)# service-policy input TUNNEL_MARKING
Router(config-if)# end
```

Verifying the Tunnel Marking on L2TPv3 Tunnels Configuration: Example

This section contains sample output from the **show policy-map interface** command and the **show policy-map** command. The output from these commands can be used to verify and monitor the feature configuration in your network.

The following is sample output from the **show policy-map interface** command. In this sample output, the character string “ip dscp tunnel 3” indicates that the tunnel marking on L2TPv3 feature has been configured to set the DSCP in the header of an L2TPv3 tunneled packet.

```
Router# show policy-map interface

 Seria0

  Service-policy input: tunnel

    Class-map: frde (match-all)
      0 packets, 0 bytes
      30 second offered rate 0 bps, drop rate 0 bps
      Match: fr-de
      QoS Set
        ip dscp tunnel 3
          Packets marked 0

    Class-map: class-default (match-any)
      13736 packets, 1714682 bytes
      30 second offered rate 0 bps, drop rate 0 bps
      Match: any
        13736 packets, 1714682 bytes
        30 second rate 0 bps
```

The following is sample output from the **show policy-map** command. In this sample output, the character string “ip precedence tunnel 4” indicates that the tunnel marking on L2TPv3 feature has been configured to set the IP precedence in the header of an L2TPv3 tunneled packet.

```
Router# show policy-map

Policy Map TUNNEL_MARKING
    Class MATCH_FRDE
      set ip precedence tunnel 4
```

Additional References

The following sections provide references related to the QoS: Tunnel Marking for L2TPv3 Tunnels 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
MQC	"Configuring the Modular Quality of Service Command-Line Interface" chapter in *Cisco IOS Quality of Service Solutions Configuration Guide*
L2TPv3	*Layer 2 Tunnel Protocol Version 3* Cisco IOS Release 12.0(25)S feature module
DSCP	"Implementing DiffServ for End-to-End Quality of Service Overview" chapter in *Cisco IOS Quality of Service Configuration Guide*

Standards

Standards	Title
None	—

MIBs

MIBs	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
None	—

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 12.3 command reference publications.

New Commands

- **match atm clp**
- **match fr-de**
- **set ip dscp tunnel**
- **set ip precedence tunnel**

Modified Commands

- **match cos**
- **police**
- **police (two rates)**
- **show policy-map**
- **show policy-map interface**

match atm clp

To specify the ATM cell loss priority (CLP) bit as a match criterion in a class map, use the **match atm clp** command in class-map configuration mode. To remove a previously specified ATM CLP bit as a match criterion, use the **no** form of this command.

match atm clp

no match atm clp

Syntax Description

This command has no keywords or arguments.

Defaults

No default behavior

Command Modes

Class-map configuration

Command History

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

Examples

In the following example, a class map called "MATCH_ATM_CLP" has been created to match traffic based on the ATM CLP bit:

```
Router(config)# class-map MATCH_ATM_CLP
Router(config-cmap)# match atm clp
Router(config-cmap)# end
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class.
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
show class-map	Displays all class maps and their matching criteria.
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.

match cos

To match a packet based on a Layer 2 class of service (CoS) marking, use the **match cos** command in class-map configuration mode. To remove a specific Layer 2 CoS/Inter-Switch Link (ISL) marking, use the **no** form of this command.

match cos *cos-value* [*cos-value* [*cos-value* [*cos-value*]]]

no match cos *cos-value* [*cos-value* [*cos-value* [*cos-value*]]]

Syntax Description

cos-value	Specific IEEE 802.1Q/ISL CoS value. The *cos-value* is from 0 to 7; up to four CoS values can be specified in one **match cos** statement.

Defaults

No match criteria are specified.

Command Modes

Class-map configuration

Command History

Release	Modification
12.1(5)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Examples

In the following example, the CoS-values of 1, 2, and 3 are successful match criteria for the interface that contains the classification policy called cos:

```
Router(config)# class-map cos
Router(config-cmap)# match cos 1 2 3
```

In the following example, classes called voice and video-n-data are created to classify traffic based on the CoS values. QoS treatment is then given to the appropriate packets (in this case, the QoS treatment is priority 64 and bandwidth 512) in the CoS-based-treatment policy map.

```
Router(config)# class-map voice
Router(config-cmap)# match cos 7

Router(config)# class-map video-n-data
Router(config-cmap)# match cos 5

Router(config)# policy-map cos-based-treatment
Router(config-pmap)# class voice
Router(config-pmap-c)# priority 64
Router(config-pmap-c)# exit
Router(config-pmap)# class video-n-data
Router(config-pmap-c)# bandwidth 512
Router(config-pmap-c)# exit
Router(config-pmap)# exit
```

```
Router(config)# interface fastethernet0/0.1
Router(config-if)# service-policy output cos-based-treatment
```

The service policy configured in this section is attached to all packets leaving Fast Ethernet interface 0/0.1. The service policy can be attached to any interface that supports service policies.

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class.
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
service-policy	Attaches a policy map to an input interface or VC, or an output interface or VC, to be used as the service policy for that interface or VC.
set cos	Sets the Layer 2 CoS value of an outgoing packet.
show class-map	Displays all class maps and their matching criteria.

match fr-de

To match packets with the Frame Relay discard eligibility (DE) bit set, use the **match fr-de** command in class-map configuration mode. To remove the match criteria, use the **no** form of this command.

match fr-de

no match fr-de

Syntax Description

This command has no arguments or keywords.

Command Default

Packets are not matched with the DE bit set.

Command Modes

Class-map configuration

Command History

Release	Modification
12.0(25)S	This command was introduced for the Cisco 7500 series router.
12.0(26)S	This command was implemented on the Cisco 7200 series router.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Examples

The following example creates a class called match-fr-de and matches packets with the Frame Relay DE bit set.

```
Router(config)# class-map match-fr-de
Router(config-cmap)# match fr-de
Router(config)# exit
```

Related Commands

Command	Description
set fr-de	Changes the DE bit setting in the address field of a Frame Relay frame to 1 for all traffic leaving an interface.

set ip dscp tunnel

To set the differentiated services code point (DSCP) value in the tunnel header of a Layer 2 Tunnel Protocol Version 3 (L2TPv3) tunneled packet for tunnel marking, use the **set ip dscp tunnel** command in policy-map class configuration mode. To disable this functionality, use the **no** form of this command.

set ip dscp tunnel *dscp-value*

no set ip dscp tunnel *dscp-value*

Syntax Description

dscp-value	A number from 0 to 63 that identifies the tunnel header value. The following reserved keywords can be specified instead of numeric values: • **EF** (expedited forwarding) • **AF11** (assured forwarding class AF11)

Defaults

The DSCP value is not set.

Command Modes

Policy-map class configuration

Command History

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

Usage Guidelines

It is possible to configure L2TPv3 tunnel marking and the **ip tos** command at the same time. However, Modular Quality of Service (QoS) Command-Line Interface (CLI) (MQC) (L2TPv3) tunnel marking has higher priority over IP ToS commands, meaning that tunnel marking always rewrites the IP header of the tunnel packet and overwrites the values set by **ip tos** commands. The order of enforcement is as follows when these commands are used simultaneously:

1. **set ip dscp tunnel** or **set ip precedence tunnel** (L2TPv3 tunnel marking)
2. **ip tos reflect**
3. **ip tos** *tos-value*

This is designed behavior. We recommend that you configure only L2TPv3 tunnel marking and reconfigure any peers configured with the **ip tos** command to use L2TPv3 tunnel marking.

Examples

The following example shows the **set ip dscp tunnel** command used in a tunnel marking for L2TPv3 tunnels configuration. In this example, a class map called "class-cl" has been configured to match traffic based on the Frame Relay discard eligible (DE) bit. Also, policy map called "policy1" has been created within which the **set ip dscp tunnel** command has been configured.

```
Router> enable
Router# configure terminal
Router(config)# class-map class-c1
Router(config-cmap)# match fr-de
Router(config-cmap)# exit
Router(config)# policy-map policy1
Router(config-pmap)# class tunnel
Router(config-pmap-c)# set ip dscp tunnel 5
Router(config-pmap-c)# end
```

Note The policy map must still be attached to an interface or ATM PVC using the **service-policy** command. For more information about attaching a policy map to an interface or ATM PVC, refer to the "Modular Quality of Service Command-Line Interface Overview" chapter of the *Cisco IOS Quality of Service Solutions Configuration Guide*.

Related Commands

Command	Description
ip tos	Specifies the ToS level for IP traffic.
set ip precedence tunnel	Sets the precedence value in the header of an L2TPv3 tunneled packet.

set ip precedence tunnel

To set the precedence value in the header of a Layer 2 Tunnel Protocol Version 3 (L2TPv3) tunneled packet for tunnel marking, use the **set ip precedence tunnel** command in policy-map class configuration mode. To disable this functionality, use the **no** form of this command.

set ip precedence tunnel *precedence-value*

no set ip precedence tunnel *precedence-value*

Syntax Description

precedence-value	A number from 0 to 63 that identifies the tunnel header value.

Defaults

The precedence value is not set.

Command Modes

Policy-map class configuration

Command History

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

Usage Guidelines

It is possible to configure L2TPv3 tunnel marking and the **ip tos** command at the same time. However, Modular Quality of Service (QoS) Command-Line Interface (CLI) (MQC) (L2TPv3) tunnel marking has higher priority over IP ToS commands, meaning that tunnel marking always rewrites the IP header of the tunnel packet and overwrites the values set by **ip tos** commands. The order of enforcement is as follows when these commands are used simultaneously:

1. **set ip dscp tunnel** or **set ip precedence tunnel** (L2TPv3 tunnel marking)
2. **ip tos reflect**
3. **ip tos** *tos-value*

This is designed behavior. We recommend that you configure only L2TPv3 tunnel marking and reconfigure any peers configured with the **ip tos** command to use L2TPv3 tunnel marking.

Examples

The following example shows the **set ip precedence tunnel** command used in a tunnel marking for L2TPv3 tunnels configuration. In this example, a class map called “class-cl” has been configured to match traffic based on the Frame Relay discard eligible (DE) bit. Also, policy map called “policy1” has been created within which the **set ip precedence tunnel** command has been configured.

```
Router> enable
Router# configure terminal
Router(config)# class-map MATCH_FRDE
Router(config-cmap)# match fr-de
Router(config-cmap)# exit
Router(config)# policy-map policy1
Router(config-pmap)# class tunnel
```

```
Router(config-pmap-c)# set ip precedence tunnel 7
Router(config-pmap-c)# end
```

Note The policy map must still be attached to an interface or ATM PVC using the **service-policy** command. For more information about attaching a policy map to an interface or ATM PVC, refer to the "Modular Quality of Service Command-Line Interface Overview" chapter of the *Cisco IOS Quality of Service Solutions Configuration Guide*.

Related Commands

Command	Description
ip tos	Specifies the ToS level for IP traffic in the TN3270 server.
set ip dscp tunnel	Sets the DSCP value in the header of an L2TPv3 tunneled packet.

police

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

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

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

Syntax Description

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

Defaults Disabled

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

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

Command History

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

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

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

Specifying Multiple Actions

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

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

Using the Police Command with the Traffic Policing Feature

The **police** command can be used with the Traffic Policing feature. The Traffic Policing feature works with a token bucket algorithm. Two types of token bucket algorithms are in Cisco IOS Release 12.1(5)T: a single-token bucket algorithm and a two-token bucket algorithm. A single-token bucket system is used when the **violate-action** option is not specified, and a two-token bucket system is used when the **violate-action** option is specified.

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

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

Token Bucket Algorithm with One Token Bucket

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

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

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

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

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

Token Bucket Algorithm with Two Token Buckets

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

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

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

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

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

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

  The token arrival rate is calculated as follows:

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

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

Examples

Token Bucket Algorithm with One Token Bucket Example

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

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

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

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

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

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

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

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

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

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

Token Bucket Algorithm with Two Token Buckets Example

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Conforming to the MPLS EXP Value Example

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

```
Router(config)# policy-map input-IP-dscp
Router(config-pmap)# class dscp24
Router(config-pmap-c)# police 8000 1500 1000
Router(config-pmap-c)# conform-action set-mpls-experimental-imposition-transmit 5
Router(config-pmap-c)# exceed-action set-mpls-experimental-imposition-transmit 3
Router(config-pmap-c)# violate-action drop
```

Related Commands

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

police (two rates)

To configure traffic policing using two rates, the committed information rate (CIR) and the peak information rate (PIR), use the **police** command in policy-map configuration mode. To remove two-rate traffic policing from the configuration, use the **no** form of this command.

police cir *cir* [**bc** *conform-burst*] **pir** *pir* [**be** *peak-burst*] [**conform-action** *action* [**exceed-action** *action* [**violate-action** *action*]]]

no police cir *cir* [**bc** *conform-burst*] **pir** *pir* [**be** *peak-burst*] [**conform-action** *action* [**exceed-action** *action* [**violate-action** *action*]]]

Syntax Description

cir	Committed information rate (CIR) at which the first token bucket is updated.
cir	Specifies the CIR value in bits per second. The value is a number from 8000 to 200000,000.
bc	(Optional) Conform burst (bc) size used by the first token bucket for policing.
conform-burst	(Optional) Specifies the bc value in bytes. The value is a number from 1000 to 51200,000.
pir	Peak information rate (PIR) at which the second token bucket is updated.
pir	Specifies the PIR value in bits per second. The value is a number from 8000 to 200000000.
be	(Optional) Peak burst (be) size used by the second token bucket for policing.
peak-burst	(Optional) Specifies the peak burst (be) size in bytes. The size varies according to the interface and platform in use.
conform-action	(Optional) Action to take on packets that conform to the CIR and PIR.
exceed-action	(Optional) Action to take on packets that conform to the PIR but not the CIR.
violate-action	(Optional) Action to take on packets exceed the PIR.
action	(Optional) Action to take on packets. Specify one of the following keywords: • **drop**—Drops the packet. • **set-clp-transmit**—Sets the ATM Cell Loss Priority (CLP) bit from 0 to 1 on the ATM cell and sends the packet with the ATM CLP bit set to 1. • **set-dscp-transmit** *new-dscp*—Sets the IP differentiated services code point (DSCP) value and sends the packet with the new IP DSCP value setting. • **set-frde-transmit**—Sets the Frame Relay discard eligible (DE) bit from 0 to 1 on the Frame Relay frame and sends the packet with the DE bit set to 1. • **set-mpls-exp-transmit**—Sets the Multiprotocol Label Switching (MPLS) experimental bits from 0 to 7 and sends the packet with the new MPLS experimental bit value setting. • **set-prec-transmit** *new-prec*—Sets the IP precedence and sends the packet with the new IP precedence value setting. • **set-qos-transmit** *new-qos*—Sets the quality of service (QoS) group value and sends the packet with the new QoS group value setting. • **transmit**—Sends the packet with no alteration.

Defaults Disabled

Command Modes Policy-map configuration

Command History

Release	Modification
12.0(5)XE	The **police** command was introduced.
12.1(1)E	This command was integrated into Cisco IOS Release 12.1(1)E.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T. The **violate-action** keyword was added.
12.2(2)T	The following keywords for the *action* argument were added: • **set-clp-transmit** • **set-frde-transmi**t • **set-mpls-exp-transmit**
12.2(4)T	This command expanded for the Two-Rate policing feature. The **cir** and **pir** keywords were added to accommodate two-rate traffic policing.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines Two-rate traffic policing uses two token buckets—Tc and Tp—for policing traffic at two independent rates. 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 two-rate policer. 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 two-rate policer. The Tp token bucket can contain up to the peak burst (Be) value.

Updating Token Buckets

The following scenario illustrates how the token buckets are updated:

A packet of B bytes arrives at time t. The last packet arrived at time t1. The CIR and the PIR token buckets at time t are represented by Tc(t) and Tp(t), respectively. Using these values and in this scenario, the token buckets are updated as follows:

Tc(t) = min(CIR * (t-t1) + Tc(t1), Bc)

Tp(t) = min(PIR * (t-t1) + Tp(t1), Be)

Marking Traffic

The two-rate policer marks packets as either conforming, exceeding, or violating a specified rate. The following points (using a packet of B bytes) illustrate how a packet is marked:

- If B > Tp(t), the packet is marked as violating the specified rate.
- If B > Tc(t), the packet is marked as exceeding the specified rate, and the Tp(t) token bucket is updated as Tp(t) = Tp(t) – B.

Otherwise, the packet is marked as conforming to the specified rate, and both token buckets—Tc(t) and Tp(t)—are updated as follows:

Tp(t) = Tp(t) – B

Tc(t) = Tc(t) – B

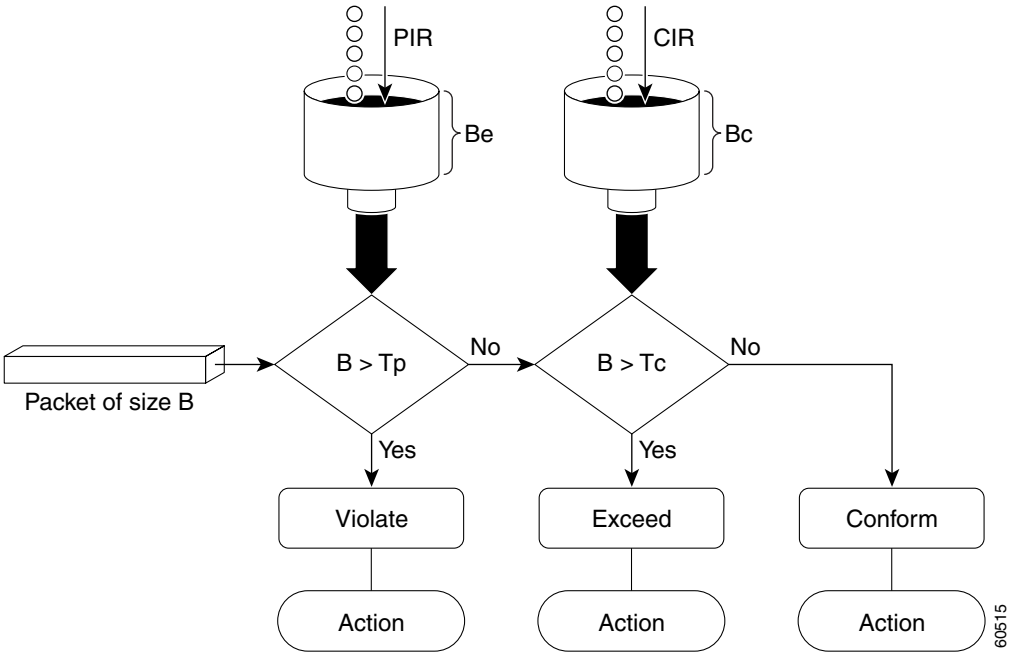
For example, if the CIR is 100 kbps, the PIR is 200 kbps, and a data stream with a rate of 250 kbps arrives at the two-rate policer, the packet would be marked as follows:

- 100 kbps would be marked as conforming to the rate
- 100 kbps would be marked as exceeding the rate
- 50 kbps would be marked as violating the rate

Marking Packets and Assigning Actions Flowchart

The flowchart in Figure 2 illustrates how the two-rate policer marks packets and assigns a corresponding action (that is, violate, exceed, or conform) to the packet.

Figure 2 Marking Packets and Assigning Actions with the Two-Rate Policer



Examples

In the following example, two-rate traffic policing is configured on a class to limit traffic to an average committed rate of 500 kbps and a peak rate of 1 Mbps:

```
Router(config)# class-map police
Router(config-cmap)# match access-group 101
Router(config-cmap)# policy-map policy1
Router(config-pmap)# class police
Router(config-pmap-c)# police cir 500000 bc 10000 pir 1000000 be 10000 conform-action
transmit exceed-action set-prec-transmit 2 violate-action drop
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface serial3/0
Router(config-if)# service-policy output policy1
Router(config-if)# end
Router# show policy-map policy1

 Policy Map policy1
  Class police
   police cir 500000 conform-burst 10000 pir 1000000 peak-burst 10000 conform-action
transmit exceed-action set-prec-transmit 2 violate-action drop
```

Traffic marked as conforming to the average committed rate (500 kbps) will be sent as is. Traffic marked as exceeding 500 kbps, but not exceeding 1 Mbps, will be marked with IP Precedence 2 and then sent. All traffic marked as exceeding 1 Mbps will be dropped. The burst parameters are set to 10000 bytes.

In the following example, 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 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 to the rate will be sent as is, and packets marked as exceeding the rate will be marked with IP Precedence 2 and then sent. Packets marked as violating the rate are dropped.

Related Commands

Command	Description
police	Configures traffic policing.
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
service-policy	Attaches a policy map to an input interface or an output interface to be used as the service policy for that interface.
show policy-map	Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps.
show policy-map interface	Displays the 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

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 1 describes the significant fields shown in the display.

Table 1 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. 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. 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. 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. 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. For the WRED — Explicit Congestion Notification (ECN) feature, the command displays ECN marking information
12.2(13)T	The following modifications were made: • This command was modified for the Percentage-Based Policing and Shaping feature. • This command was modified for the Class-Based RTP and TCP Header Compression feature. • 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. • This command was modified to display the Frame Relay DLCI number as a criterion for matching traffic inside a class map. • This command was modified to display Layer 3 packet length as a criterion for matching traffic inside a class map. • 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 2 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 2 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 2 describes significant fields commonly shown in the displays. The fields in the table are grouped according to the relevant QoS feature.

Table 2 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. **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 2 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. **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: ((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 2 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 3 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 3 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 3 describes the significant fields shown in the display when aggregate WRED is configured for an ATM shared port adapter.

Table 3 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. **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 4 describes the significant fields shown in the display. Significant fields that are not described in Table 4 are described in Table 2, "show policy-map interface Field Descriptions."

Table 4 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 5 describes the significant fields shown in the display.

Table 5 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 6 describes the significant fields shown in the display.

Table 6 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 7 describes the significant fields shown in the display.

Table 7 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. **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 7 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 8 describes the significant fields shown in the display.

Table 8 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 8 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. **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 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 9 describes the significant fields shown in the display.

Table 9 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. **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 9 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 10 describes the significant fields shown in the display.

Table 10 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. **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 11 describes the significant fields shown in the display.

Table 11 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. **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 11 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: ((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 12 describes the significant fields shown in the display.

Table 12 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. **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 13 describes the fields shown in the display.

Table 13 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 14 describes the significant fields shown in the display.

Table 14 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.