



Byte-Based Weighted Random Early Detection

First Published: August 26, 2003

Last Updated: February 28, 2006

This feature module explains how to enable byte-based Weighted Random Early Detection (WRED).

History for the Byte-Based Weighted Random Early Detection Feature

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

Finding Support Information for Platforms and Cisco IOS Software Images

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

Contents

- [Restrictions for Byte-Based WRED, page 2](#)
- [Information About Byte-Based WRED, page 2](#)
- [How to Configure Byte-Based WRED, page 2](#)
- [Configuration Examples for Byte-Based WRED, page 5](#)
- [Additional References, page 6](#)
- [Command Reference, page 8](#)



Corporate Headquarters:

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

© 2003–2006 Cisco Systems, Inc. All rights reserved.

Restrictions for Byte-Based WRED

- WRED is only useful when the bulk of the traffic is TCP/IP traffic. With TCP, dropped packets indicate congestion, so the packet source will reduce its transmission rate. With other protocols, packet sources may not respond or may resend dropped packets at the same rate. Thus, dropping packets does not decrease congestion.
- You cannot configure both packet-based WRED and byte-based WRED in the same policy.
- You cannot configure byte-based WRED on a class in which the queue-limit is configured in milliseconds or packets.

Information About Byte-Based WRED

This feature extends the functionality of WRED. In previous releases, you specified the WRED actions based on the number of packets. With the Byte-Based WRED, you can specify WRED actions based on the number of bytes. For more information about WRED, see the following documents:

- Weighted Random Early Detection overview in the *Cisco IOS Quality of Service Solutions Configuration Guide*, Release 12.2

Configuring Weighted Random Early Detection section of the *Cisco IOS Quality of Service Solutions Configuration Guide*, Release 12.3

How to Configure Byte-Based WRED

The following sections describe how to configure byte-based WRED:

- [Configuring Byte-Based WRED, page 2](#)
- [Verifying the Configuration, page 4](#)

Configuring Byte-Based WRED

Use the following steps to enable byte-based WRED.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **class-map** *class-map-name*
4. **match ip precedence** *ip-precedence-value*
5. **exit**
6. **policy-map** *policy-name*
7. **class** *class-name*
8. **random-detect**
9. **random-detect precedence** *precedence min-threshold bytes max-threshold bytes max-probability-denominator*

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	class-map <i>class-map-name</i> Example: Router(config)# class-map c1	Specifies the user-defined name of the traffic class. Names can be a maximum of 40 alphanumeric characters.
Step 4	match ip precedence <i>ip-precedence-value</i> Example: Router(config-cmap)# match ip precedence 1	Specifies up to eight IP Precedence values used as match criteria.
Step 5	exit Example: Router(config-cmap)# exit	Exits from class-map configuration mode.
Step 6	policy-map <i>policy-name</i> Example: Router(config)# policy-map p1	Specifies the name of the traffic policy to configure. Names can be a maximum of 40 alphanumeric characters.
Step 7	class <i>class-name</i> Example: Router(config-pmap)# class c1	Specifies the name of a predefined traffic class, which was configured with the class-map command, used to classify traffic to the traffic policy.
Step 8	random-detect Example: Router(config-pmap-c)# random-detect	Enables WRED.
Step 9	random-detect precedence <i>precedence</i> <i>min-threshold bytes</i> <i>max-threshold bytes</i> <i>mark-prob-denominator</i> Example: Router(config-pmap-c)# random-detect precedence 1 2000 bytes 3000 bytes 200	Configures the parameters for bytes with a specific IP precedence.

Verifying the Configuration

To verify that byte-based WRED is correctly configured, issue the **show policy-map interface** or **show policy-map** command.

[Example 1](#) shows the output for the **show policy-map** command for a service policy called pol1 that is configured for byte-based WRED.

Example 1 *show policy-map Command Output for Byte-Based WRED*

```
Router# show policy-map

Policy Map pol1
  Class class c1
    Bandwidth 10 (%)
      exponential weight 9
      class min-threshold(bytes) max-threshold(bytes) mark-probability
      -----
      0          -                -                1/10
      1      20000            30000            1/10
      2          -                -                1/10
      3          -                -                1/10
      4          -                -                1/10
      5          -                -                1/10
      6          -                -                1/10
      7          -                -                1/10
      rsvp      -                -                1/10
```

[Example 2](#) shows the output for the **show policy-map interface** command for an interface that is configured for byte-based WRED.

Example 2 *show policy-map interface Command Output for Byte-Based WRED*

```
Router# show policy-map interface serial3/1

Service-policy output: pol
Class-map: silver (match-all)
  366 packets, 87840 bytes
  30 second offered rate 15000 bps, drop rate 300 bps
  Match: ip precedence 1
  Queueing
    Output Queue: Conversation 266
    Bandwidth 10 (%)
    (pkts matched/bytes matched) 363/87120
    depth/total drops/no-buffer drops) 147/38/0
    exponential weight: 9
    mean queue depth: 25920
```

class	Transmitted pkts/bytes	Random drop pkts/bytes	Tail drop pkts/bytes	Minimum thresh (bytes)	Maximum thresh (bytes)	Mark prob
0	0/0	0/0	0/0	20000	40000	1/10
1	328/78720	38/9120	0/0	22000	40000	1/10
2	0/0	0/0	0/0	24000	40000	1/10
3	0/0	0/0	0/0	26000	40000	1/10
4	0/0	0/0	0/0	28000	40000	1/10

Configuration Examples for Byte-Based WRED

The following example shows a service policy called wred-policy that sets up byte-based wred for a class called prec2 and for the default class. The policy is then applied to Ethernet interface 0/0/1.

```
policy wred-policy

  class prec2

    bandwidth 1000
    random-detect
    random-detect precedence 2 100 bytes 200 bytes 10

  class class-default

    random-detect
    random-detect precedence 4 150 bytes 300 bytes 15
    random-detect precedence 6 200 bytes 400 bytes 5

interface Ethernet0/0/1

  service-policy output wred-policy
```

The following example shows the byte-based WRED results for the service policy attached to interface Ethernet interface 0/0/1.

Router# **show policy-map interface**

```
Ethernet0/0/1

Service-policy output: wred-policy (1177)

Class-map: prec2 (match-all) (1178/10)
 0 packets, 0 bytes
 5 minute offered rate 0 bps, drop rate 0 bps
 Match: ip precedence 2 (1179)
 Queueing
 queue limit 62500 bytes
 (queue depth/total drops/no-buffer drops) 0/0/0
 (pkts queued/bytes queued) 0/0
 bandwidth 1000 (kbps)
 Exp-weight-constant: 9 (1/512)
 Mean queue depth: 0 bytes
```

class	Transmitted pkts/bytes	Random drop pkts/bytes	Tail drop pkts/bytes	Minimum thresh bytes	Maximum thresh bytes	Mark prob
0	0/0	0/0	0/0	15625	31250	1/10
1	0/0	0/0	0/0	17578	31250	1/10
2	0/0	0/0	0/0	100	200	1/10
3	0/0	0/0	0/0	21484	31250	1/10
4	0/0	0/0	0/0	23437	31250	1/10
5	0/0	0/0	0/0	25390	31250	1/10
6	0/0	0/0	0/0	27343	31250	1/10
7	0/0	0/0	0/0	29296	31250	1/10

```

Class-map: class-default (match-any) (1182/0)
 0 packets, 0 bytes
 5 minute offered rate 0 bps, drop rate 0 bps
 Match: any (1183)
 0 packets, 0 bytes
 5 minute rate 0 bps
```

```

queue limit 562500 bytes
(queue depth/total drops/no-buffer drops) 0/0/0
(pkts queued/bytes queued) 0/0
Exp-weight-constant: 9 (1/512)
Mean queue depth: 0 bytes

```

class	Transmitted pkts/bytes	Random drop pkts/bytes	Tail drop pkts/bytes	Minimum thresh bytes	Maximum thresh bytes	Mark prob
0	0/0	0/0	0/0	140625	281250	1/10
1	0/0	0/0	0/0	158203	281250	1/10
2	0/0	0/0	0/0	175781	281250	1/10
3	0/0	0/0	0/0	193359	281250	1/10
4	0/0	0/0	0/0	150	300	1/15
5	0/0	0/0	0/0	228515	281250	1/10
6	0/0	0/0	0/0	200	400	1/5
7	0/0	0/0	0/0	263671	281250	1/10

Additional References

The following sections provide references related to the Byte-Based Weighted Random Early Detection feature.

Related Documents

Related Topic	Document Title
Modular QoS CLI	Modular Quality of Service Command-Line Interface
CBWFQ and WRED	Class-Based Weighted Fair Queueing and Weighted Random Early Detection

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 modified commands. All other commands used with this feature are documented in the Cisco IOS Release 12.3 command reference publications.

Modified Commands

- [random-detect dscp](#)
- [random-detect precedence](#)
- [show policy-map](#)
- [show policy-map interface](#)

random-detect dscp

To change the minimum and maximum packet thresholds for the differentiated services code point (DSCP) value, use the **random-detect dscp** command in interface configuration mode. To return the minimum and maximum packet thresholds to the default for the DSCP value, use the **no** form of this command.

random-detect dscp *dscp-alue min-threshold max-threshold [max-probability-denominator]*

no random-detect dscp *dscp-value min-threshold max-threshold [max-probability-denominator]*

Syntax Description		
<i>dscp-value</i>		Specifies the DSCP value. The DSCP value can be a number from 0 to 63, or it can be one of the following keywords: ef , af11 , af12 , af13 , af21 , af22 , af23 , af31 , af32 , af33 , af41 , af42 , af43 , cs1 , cs2 , cs3 , cs4 , cs5 , or cs7 .
<i>min-threshold</i>		Minimum threshold in number of packets. The value range of this argument is from 1 to 4096. When the average queue length reaches the minimum threshold, Weighted Random Early Detection (WRED) randomly drops some packets with the specified DSCP value.
<i>max-threshold</i>		Maximum threshold in number of packets. The value range of this argument is from the value of the <i>min-threshold</i> argument to 4096. When the average queue length exceeds the maximum threshold, WRED drops all packets with the specified DSCP value.
<i>max-probability-denominator</i>		(Optional) Denominator for the fraction of packets dropped when the average queue depth is at the maximum threshold. For example, if the denominator is 512, 1 out of every 512 packets is dropped when the average queue is at the maximum threshold. The value range is from 1 to 65536. The default is 10; 1 out of every 10 packets is dropped at the maximum threshold.

Defaults	If WRED is using the DSCP value to calculate the drop probability of a packet, all entries of the DSCP table are initialized with the default settings shown in Table 1 in the “Usage Guidelines” section of this command.
----------	--

Command Modes	Interface 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.

Usage Guidelines

The **random-detect dscp** command allows you to specify the DSCP value. The DSCP value can be a number from 0 to 63, or it can be one of the following keywords: **ef**, **af11**, **af12**, **af13**, **af21**, **af22**, **af23**, **af31**, **af32**, **af33**, **af41**, **af42**, **af43**, **cs1**, **cs2**, **cs3**, **cs4**, **cs5**, or **cs7**.

This command must be used in conjunction with the **random-detect** (interface) command.

Additionally, the **random-detect dscp** command is available only if you specified the *dscp-based* argument when using the **random-detect** (interface) command.

[Table 1](#) lists the default settings used by the **random-detect dscp** command for the DSCP value specified. [Table 1](#) lists the DSCP value, and its corresponding minimum threshold, maximum threshold, and max probability. The last row of the table (the row labeled “default”) shows the default settings used for any DSCP value not specifically shown in the table.

Table 1 *random-detect dscp Default Settings*

DSCP (Precedence)	Minimum Threshold	Maximum Threshold	Max Probability
af11	32	40	1/10
af12	28	40	1/10
af13	24	40	1/10
af21	32	40	1/10
af22	28	40	1/10
af23	24	40	1/10
af31	32	40	1/10
af32	28	40	1/10
af33	24	40	1/10
af41	32	40	1/10
af42	28	40	1/10
af43	24	40	1/10
cs1	22	40	1/10
cs2	24	40	1/10
cs3	26	40	1/10
cs4	28	40	1/10
cs5	30	40	1/10
cs6	32	40	1/10
cs7	34	40	1/10
ef	36	40	1/10
rsvp	36	40	1/10
default	20	40	1/10

Examples

The following example enables WRED to use the DSCP value af22. The minimum threshold for DSCP value af22 is 28, the maximum threshold is 40, and the max probability is 10.

```
random-detect dscp af22 20 40 10
```

Related Commands	Command	Description
	random-detect (interface)	Enables WRED or DWRED.
	show queueing	Lists all or selected configured queueing strategies.
	show queueing interface	Displays the queueing statistics of an interface or VC.

random-detect precedence

To configure Weighted Random Early Detection (WRED) and distributed WRED (DWRED) parameters for a particular IP Precedence, use the **random-detect precedence** command in interface configuration mode. To configure WRED parameters for a particular IP Precedence for a class policy in a policy map, use the **random-detect precedence** command in policy-map class configuration mode. To return the values to the default for the precedence, use the **no** form of this command.

```
random-detect precedence {precedence | rsvp} min-threshold max-threshold
max-probability-denominator

no random-detect precedence {precedence | rsvp} min-threshold max-threshold
max-probability-denominator
```

Syntax Description

<i>precedence</i>	IP Precedence number. The value range is from 0 to 7. For Cisco 7000 series routers with an RSP7000 interface processor and Cisco 7500 series routers with a VIP2-40 interface processor (VIP2-50 interface processor strongly recommended), the precedence value range is from 0 to 7 only; see Table 2 in the “Usage Guidelines” section of this command.
rsvp	Indicates Resource Reservation Protocol (RSVP) traffic.
<i>min-threshold</i>	Minimum threshold in number of packets. The value range of this argument is from 1 to 4096. When the average queue length reaches the minimum threshold, WRED randomly drops some packets with the specified IP Precedence.
<i>max-threshold</i>	Maximum threshold in number of packets. The value range of this argument is from the value of the <i>min-threshold</i> argument to 4096. When the average queue length exceeds the maximum threshold, WRED drops all packets with the specified IP Precedence.
<i>max-probability-denominator</i>	Denominator for the fraction of packets dropped when the average queue depth is at the maximum threshold. For example, if the denominator is 512, 1 out of every 512 packets is dropped when the average queue is at the maximum threshold. The value range is from 1 to 65536. The default is 10; 1 out of every 10 packets is dropped at the maximum threshold.

Defaults

For all precedences, the *max-probability-denominator* default is 10, and the *max-threshold* is based on the output buffering capacity and the transmission speed for the interface.

The default *min-threshold* depends on the precedence. The *min-threshold* for IP Precedence 0 corresponds to half of the *max-threshold*. The values for the remaining precedences fall between half the *max-threshold* and the *max-threshold* at evenly spaced intervals. See [Table 2](#) in the “Usage Guidelines” section of this command for a list of the default minimum threshold values for each IP Precedence.

Command Modes

- Interface configuration when used on an interface
- Policy-map class configuration when used to specify class policy in a policy map

Command History

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

Usage Guidelines

WRED is a congestion avoidance mechanism that slows traffic by randomly dropping packets when congestion exists. DWRED is similar to WRED but uses the Versatile Interface Processor (VIP) instead of the Route Switch Processor (RSP).

When you configure the **random-detect** command on an interface, packets are given preferential treatment based on the IP Precedence of the packet. Use the **random-detect precedence** command to adjust the treatment for different precedences.

If you want WRED or DWRED to ignore the precedence when determining which packets to drop, enter this command with the same parameters for each precedence. Remember to use reasonable values for the minimum and maximum thresholds.

Note that if you use the **random-detect precedence** command to adjust the treatment for different precedences within class policy, you must ensure that WRED is not configured for the interface to which you attach that service policy.

Table 2 lists the default minimum threshold value for each IP Precedence.

Table 2 *Default WRED and DWRED Minimum Threshold Values*

IP Precedence	Minimum Threshold Value (Fraction of Maximum Threshold Value)	
	WRED	DWRED
0	9/18	8/16
1	10/18	9/16
2	11/18	10/16
3	12/18	11/16
4	13/18	12/16
5	14/18	13/16
6	15/18	14/16
7	16/18	15/16
RSVP	17/18	—

**Note**

The default WRED or DWRED parameter values are based on the best available data. We recommend that you do not change the parameters from their default values unless you have determined that your applications would benefit from the changed values.

The DWRED feature is supported only on Cisco 7000 series routers with an RSP7000 card and Cisco 7500 series routers with a VIP2-40 or greater interface processor. A VIP2-50 interface processor is strongly recommended when the aggregate line rate of the port adapters on the VIP is greater than DS3. A VIP2-50 interface processor is required for OC-3 rates.

To use DWRED, distributed Cisco Express Forwarding (dCEF) switching must first be enabled on the interface. For more information on dCEF, refer to the *Cisco IOS Switching Services Configuration Guide* and the *Cisco IOS Switching Services Command Reference*.

**Note**

The DWRED feature is not supported in a class policy.

Examples

The following example enables WRED on the interface and specifies parameters for the different IP Precedences:

```
interface Hssi0/0/0
description 45Mbps to R1
ip address 10.200.14.250 255.255.255.252
random-detect
random-detect precedence 0 32 256 100
random-detect precedence 1 64 256 100
random-detect precedence 2 96 256 100
random-detect precedence 3 120 256 100
random-detect precedence 4 140 256 100
random-detect precedence 5 170 256 100
random-detect precedence 6 290 256 100
random-detect precedence 7 210 256 100
random-detect precedence rsvp 230 256 100
```

The following example configures policy for a class called acl10 included in a policy map called policy10. Class acl101 has these characteristics: a minimum of 2000 kbps of bandwidth are expected to be delivered to this class in the event of congestion and a weight factor of 10 is used to calculate the average queue size. For congestion avoidance, WRED packet drop is used, not tail drop. IP Precedence is reset for levels 0 through 4.

```
policy-map policy10
class acl10
bandwidth 2000
random-detect
random-detect exponential-weighting-constant 10
random-detect precedence 0 32 256 100
random-detect precedence 1 64 256 100
random-detect precedence 2 96 256 100
random-detect precedence 3 120 256 100
random-detect precedence 4 140 256 100
```

Related Commands	Command	Description
	bandwidth (policy-map class)	Specifies or modifies the bandwidth allocated for a class belonging to a policy map.
	fair-queue (class-default)	Specifies the number of dynamic queues to be reserved for use by the class-default class as part of the default class policy.
	random-detect dscp	Changes the minimum and maximum packet thresholds for the DSCP value.
	random-detect (per VC)	Enables per-VC WRED or per-VC DWRED.
	random-detect exponential-weighting-constant	Configures the WRED and DWRED exponential weight factor for the average queue size calculation.
	random-detect flow count	Sets the flow count for flow-based WRED.
	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.
	show queue	Displays the contents of packets inside a queue for a particular interface or VC.
	show queueing	Lists all or selected configured queueing strategies.

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 3 describes the significant fields shown in the display.

Table 3 *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]


```

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.
<i>interface-name</i>		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.
<i>vpi</i>		(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 <i>vpi</i> and <i>vci</i> arguments cannot both be set to 0; if one is 0, the other cannot be 0.
<i>vci</i>		(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 <i>vpi</i> and <i>vci</i> 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.
<i>dlci</i>		(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.

<i>slot</i>	(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.
<i>/subslot</i>	(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.
<i>/port</i>	(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.
<i>.subinterface</i>	(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	<p>The command was modified for the Policer Enhancement — Multiple Actions feature and the WRED — Explicit Congestion Notification (ECN) feature.</p> <p>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.</p> <p>For the WRED — Explicit Congestion Notification (ECN) feature, the command displays ECN marking information</p>
12.2(13)T	<p>The following modifications were made:</p> <ul style="list-style-type: none"> • 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 4](#) 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
```

show policy-map interface

```

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 pkts/bytes	Random drop pkts/bytes	Tail drop pkts/bytes	Minimum thresh	Maximum thresh	Mark 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 4](#) 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 4 describes significant fields commonly shown in the displays. The fields in the table are grouped according to the relevant QoS feature.

Table 4 *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 <i>before</i> 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 <i>one</i> tunnel encapsulation, or may include the overhead for <i>all</i> 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 <i>Cisco IOS Quality of Service Solutions Configuration Guide</i> .
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 4 *show policy-map interface Field Descriptions¹ (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 <i>after</i> 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: $((Bc+Be) / 8) \times 1$
Sustain bits/int	Committed burst (Bc) rate.
Excess bits/int	Excess burst (Be) rate.
Interval (ms)	Time interval value in milliseconds (ms).

Table 4 *show policy-map interface Field Descriptions¹ (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 5](#) 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
```


Table 5 describes the significant fields shown in the display when aggregate WRED is configured for an ATM shared port adapter.

Table 5 *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 <i>after</i> 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
```

show policy-map interface

```

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
  BECN  0      1434    162991  26      2704   yes
  Voice Adaptive Shaping active, time left 29 secs

```

Table 6 describes the significant fields shown in the display. Significant fields that are not described in Table 6 are described in Table 4, “show policy-map interface Field Descriptions.”

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

Table 7 *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 serial13/2

Serial13/2: 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 8 describes the significant fields shown in the display.

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

Table 9 *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	<p>Number of packets (also shown in bytes) passed through WRED and not dropped by WRED.</p> <p>Note If there is insufficient memory in the buffer to accommodate the packet, the packet can be dropped <i>after</i> 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.</p>
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 9 *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 10](#) describes the significant fields shown in the display.

Table 10 *show policy-map interface Field Descriptions—Configured for Class-Based RTP and TCP Header Compression¹*

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 10 *show policy-map interface Field Descriptions—Configured for Class-Based RTP and TCP Header Compression¹ (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 <i>before</i> 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 <i>one</i> tunnel encapsulation, or may include the overhead for <i>all</i> 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 11 describes the significant fields shown in the display.

Table 11 *show policy-map interface Field Descriptions—Configured for MQC Unconditional Packet Discard¹*

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 <i>before</i> 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 <i>one</i> tunnel encapsulation, or may include the overhead for <i>all</i> 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 11 *show policy-map interface Field Descriptions—Configured for MQC Unconditional Packet Discard¹ (continued)*

Field	Description
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 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 <i>Cisco IOS Quality of Service Solutions Configuration Guide</i> .
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 12 describes the significant fields shown in the display.

Table 12 *show policy-map interface Field Descriptions—Configured for Percentage-Based Policing and Shaping¹*

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 <i>before</i> 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 <i>one</i> tunnel encapsulation, or may include the overhead for <i>all</i> 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		Byte	Sustain	Excess	Interval	Increment	Adapt
Target/Average		Limit	bits/int	bits/int	(ms)	(bytes)	Active
Rate			10 (ms)	20 (ms)			
20 %							
201500/201500		1952	7808	7808	38	976	-
Queue	Packets	Bytes	Packets	Bytes	Shaping		
Depth			Delayed	Delayed	Active		
0	0	0	0	0	no		

Table 13 describes the significant fields shown in the display.

Table 13 *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 <i>before</i> 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 <i>one</i> tunnel encapsulation, or may include the overhead for <i>all</i> 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 <i>Cisco IOS Quality of Service Solutions Configuration Guide</i> , 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 13 *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: $((Bc+Be) / 8) \times 1$
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 14 describes the significant fields shown in the display.

Table 14 *show policy-map interface Field Descriptions—Configured for Packet Classification Based on Layer 3 Packet Length¹*

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 <i>before</i> 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 <i>one</i> tunnel encapsulation, or may include the overhead for <i>all</i> 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
```

show policy-map interface

```

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

```

Table 15 describes the fields shown in the display.

Table 15 *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 <i>Cisco IOS Quality of Service Solutions Configuration Guide</i> .
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:

$$20 \% * 2048 \text{ kbps} = 409600 \text{ bps}$$

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:

$$40 \% * 2048 \text{ kbps} = 819200 \text{ bps}$$

**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:

$$300 \text{ ms} * 409600 \text{ bps} = 15360 \text{ bytes}$$

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:

$$400 \text{ ms} * 819200 \text{ bps} = 40960 \text{ bytes}$$

[Table 16](#) describes the significant fields shown in the display.

Table 16 *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 <i>Cisco IOS Quality of Service Solutions Configuration Guide</i> .
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.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2003–2006 Cisco Systems, Inc. All rights reserved.

show policy-map interface