



Quality of Service Solutions Command Reference, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)

First Published: January 11, 2013

Last Modified: January 11, 2013

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883



CONTENTS

CHAPTER 1

A through M 1

- auto discovery qos 2
- auto qos 4
- auto qos voip 6
- bandwidth (policy-map class) 9
- bandwidth remaining ratio 19
- class (policy-map) 24
- class-map 31
- dscp 38
- match class-map 41
- match cos 44
- match protocol 47
- match qos-group 61
- mls qos (global configuration mode) 64
- mls qos (interface configuration mode) 66

CHAPTER 2

P through V 67

- policy-map 68
- priority-group 75
- priority level 78
- priority-list default 80
- priority-list interface 82
- priority-list protocol 84
- priority-list queue-limit 89
- service-policy 91
- set cos 101
- set qos-group 105
- show auto discovery qos 109

show auto qos	113
show policy-map	118
show policy-map class	134
show policy-map interface	136
show queue	185
show queueing	191
show queueing interface	198
vbr-nrt	203



A through M

- [auto discovery qos, page 2](#)
- [auto qos, page 4](#)
- [auto qos voip, page 6](#)
- [bandwidth \(policy-map class\), page 9](#)
- [bandwidth remaining ratio, page 19](#)
- [class \(policy-map\), page 24](#)
- [class-map, page 31](#)
- [dscp, page 38](#)
- [match class-map, page 41](#)
- [match cos, page 44](#)
- [match protocol, page 47](#)
- [match qos-group, page 61](#)
- [mls qos \(global configuration mode\), page 64](#)
- [mls qos \(interface configuration mode\), page 66](#)

auto discovery qos

To begin discovering and collecting data for configuring the AutoQoS for the Enterprise feature, use the **autodiscoveryqos** command in interface configuration mode. To stop discovering and collecting data, use the **no** form of this command.

auto discovery qos [trust]

no auto discovery qos

Syntax Description

trust	<p>(Optional) Indicates that the differentiated services code point (DSCP) markings of a packet are trust (that is, relied on) for classification of the voice, video, and data traffic.</p> <p>If the optional trust keyword is not specified, the voice, video, and data traffic is classified using network-based application recognition (NBAR), and the packets are marked with the appropriate DSCP value.</p>
--------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Command Default

No data collection is performed.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.3(11)T	The trust mode was modified to classify packets by DSCP value rather than by protocol type.

Usage Guidelines

The **autodiscoveryqos** command initiates the Auto-Discovery (data collection) phase of the AutoQoS for the Enterprise feature. This command invokes NBAR protocol discovery to collect data and analyze the traffic at the egress direction of the interface.

The **noautodiscoveryqos** command terminates the Auto-Discovery phase and removes any data collection reports generated.

The **trust** keyword is used for the trusted model based on the specified DSCP marking. For more information, see the “Trusted Boundary” section of the *AutoQoS for the Enterprise* feature module, Cisco IOS Release 12.3(7)T.

Examples

The following is a sample configuration showing the Auto-Discovery (data collection) phase of the AutoQoS for the Enterprise feature enabled on a serial2/1/1 subinterface.

```
Router> enable
Router# configure terminal
Router(config)# interface serial2/1.1
Router(config-if)# frame-relay interface-dlci 58
Router(config-if)# auto discovery qos
Router(config-if)# end
```

Related Commands

Command	Description
auto qos	Installs the QoS class maps and policy maps created by the AutoQoS for the Enterprise feature.
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.
show auto qos	Displays the interface configurations, policy maps, and class maps created by AutoQoS on a specific interface or all interfaces.

auto qos

To install the quality-of-service (QoS) class maps and policy maps created by the AutoQoS for the Enterprise feature, use the **auto qos** command in interface configuration mode. To remove the QoS policies, use the **no** form of this command.

auto qos

no auto qos

Syntax Description

This command has no arguments or keywords.

Command Default

No QoS policies are installed.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

The class maps and policy maps are created from the templates that are automatically generated by the AutoQoS for the Enterprise feature. These templates (and the resulting class maps and policy maps) are generated on the basis of the data collected during the Auto-Discovery phase of the AutoQoS for the Enterprise feature. For more information about the Auto-Discovery phase, see the “Configuration Phases” section of the *AutoQoS for the Enterprise* feature module, Cisco IOS Release 12.3(7)T.

The **noautoqos** command removes any AutoQoS-generated class maps and policy maps installed on the interface.

The **autoqos** command is not supported on gigabit interfaces.

Examples

The following is a sample configuration showing the AutoQoS for the Enterprise feature enabled on a serial2/1/1 subinterface. In this configuration, the AutoQoS class maps and policy maps will be installed on the serial2/1 interface.

```
Router> enable
Router# configure terminal
Router(config)# interface serial2/1
Router(config-if)# frame-relay interface-dlci 58
Router(config-if)# auto qos
Router(config-if)# end
```


Related Commands

Command	Description
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.
show auto qos	Displays the interface configurations, policy maps, and class maps created by AutoQoS on a specific interface or all interfaces.

auto qos voip

To configure the AutoQoS--VoIP feature on an interface, use the **autoqosvoip** command in interface configuration mode or Frame Relay DLCI configuration mode. To remove the AutoQoS--VoIP feature from an interface, use the **no** form of this command.

auto qos voip [trust] [fr-atm]

no auto qos voip [trust] [fr-atm]

Syntax Description

trust	(Optional) Indicates that the differentiated services code point (DSCP) markings of a packet are trusted (relied on) for classification of the voice traffic. If the optional trust keyword is not specified, the voice traffic is classified using network-based application recognition (NBAR), and the packets are marked with the appropriate DSCP value.
fr-atm	(Optional) Enables the AutoQoS--VoIP feature for Frame-Relay-to-ATM links. This option is available on the Frame Relay data-link connection identifiers (DLCIs) for Frame-Relay-to-ATM interworking only.

Command Default

Default mode is disabled.

Command Modes

Interface configuration (config-if) Frame Relay DLCI configuration (for use with Frame Relay DLCIs) (config-fr-dlci)

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

To enable the AutoQoS--VoIP feature for Frame-Relay-to-ATM interworking, the **fr-atm** keyword must be configured explicitly. However, the **fr-atm** keyword affects low-speed DLCIs *only*. It does not affect high-speed DLCIs.

**Note**

DLCIs with link speeds lower than or equal to 768 kbps are considered low-speed DLCIs; DLCIs with link speeds higher than 768 kbps are considered high-speed DLCIs.

Depending on whether the **trust** keyword has been configured for this command, the AutoQoS--VoIP feature automatically creates one of the following two policy maps:

- “AutoQoS-Policy-Trust” (created if the **trust** keyword is configured)
- “AutoQoS-Policy-UnTrust” (created if the **trust** keyword is *not* configured)

Both of these policy maps are designed to handle the Voice over IP (VoIP) traffic on an interface or a permanent virtual circuit (PVC) and can be modified to suit the quality of service (QoS) requirements of the network. To modify these policy maps, use the appropriate Cisco IOS command.

These policy maps should not be attached to an interface or PVC by using the **service-policy** command. If the policy maps are attached in this manner, the AutoQoS--VoIP feature (that is, the policy maps, class maps, and access control lists [ACLs]) will not be removed properly when the **noautoqosvoip** command is configured.

For low-speed Frame Relay DLCIs that are interconnected with ATM PVCs in the same network, the **fr-atm** keyword must be explicitly configured in the **autoqosvoip** command to configure the AutoQoS--VoIP feature properly. That is, the command must be configured as **autoqosvoipfr-atm**.

For low-speed Frame Relay DLCIs that are configured with Frame-Relay-to-ATM, Multilink PPP (MLP) over Frame Relay (MLPoFR) is configured automatically. The subinterface must have an IP address. When MLPoFR is configured, this IP address is removed and put on the MLP bundle. The AutoQoS--VoIP feature must also be configured on the ATM side by using the **autoqosvoip** command.

The **autoqosvoip** command is not supported on subinterfaces or gigabit interfaces.

The **autoqosvoip** command is available for Frame Relay DLCIs.

Disabling AutoQoS--VoIP

The **noautoqosvoip** command disables the AutoQoS--VoIP feature and removes the configurations associated with the feature.

When the **noautoqosvoip** command is used, the **no** forms of the individual commands originally generated by the AutoQoS--VoIP feature are configured. With the use of individual **no** forms of the commands, the system defaults are reinstated. The **no** forms of the commands will be applied just as if the user had entered the commands individually. As the configuration reinstating the default setting is applied, any messages resulting from the processing of the commands are displayed.

**Note**

If you delete a subinterface or PVC (either ATM or Frame Relay PVCs) without configuring the **noautoqosvoip** command, the AutoQoS--VoIP feature will not be removed properly.

Examples

The following example shows the AutoQoS--VoIP feature configured on serial point-to-point subinterface 4/1.2. In this example, both the **trust** and **fr-atm** keywords are configured.

```
Router> enable
Router# configure terminal
Router(config)# interface serial4/1.2 point-to-point
Router(config-if)# bandwidth 100
Router(config-if)# ip address 192.168.0.0 255.255.255.0
```

```
Router(config-if)# frame-relay interface-dlci 102  
Router(config-fr-dlci)# auto qos voip trust fr-atm  
Router(config-fr-dlci)# end  
Router(config-if#
```

```
exit
```

Related Commands

Command	Description
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.
show auto qos	Displays the configurations created by the AutoQoS--VoIP feature on a specific interface or all interfaces.

bandwidth (policy-map class)

To specify or modify the bandwidth allocated for a class belonging to a policy map, or to enable ATM overhead accounting, use the **bandwidth** command in QoS policy-map class configuration mode. To remove the bandwidth specified for a class or disable ATM overhead accounting, use the **no** form of this command.

bandwidth {*kbps*| [**remaining**] **percent** *percentage*} [**account** {**qinq**| **dot1q**} **aal5** *subscriber-encapsulation*]
no bandwidth

Cisco 10000 Series Router (PRE3)

bandwidth {*kbps*| [**remaining**] **percent** *percentage*} **account** {**qinq**| **dot1q**} {**aal5**| **aal3**}
*subscriber-encapsulation***user-defined** *offset* [**atm**]
no bandwidth

Syntax Description

<i>kbps</i>	Amount of bandwidth, in kilobits per second (kbps), to be assigned to the class. The amount of bandwidth varies according to the interface and platform in use. The value must be between 1 and 2,000,000 kbps.
remaining	(Optional) Specifies that the percentage of guaranteed bandwidth is based on a relative percent of available bandwidth.
percent <i>percentage</i>	Specifies the percentage of guaranteed bandwidth based on an absolute percent of available bandwidth to be set aside for the priority class or on a relative percent of available bandwidth. The valid range is 1 to 100.
account	(Optional) Enables ATM overhead accounting.
qinq	(Optional) Specifies queue-in-queue encapsulation as the broadband aggregation system (BRAS) to digital subscriber line access multiplexer (DSLAM) encapsulation type for ATM overhead accounting.
dot1q	(Optional) Specifies IEEE 802.1Q VLAN encapsulation as the BRAS-DSLAM encapsulation type for ATM overhead accounting.
aal5	(Optional) Specifies ATM Adaptation Layer 5 and the encapsulation type at the subscriber line for ATM overhead accounting. AAL5 supports connection-oriented variable bit rate (VBR) services. See the “Usage Guidelines” section for valid encapsulation types.

<i>subscriber-encapsulation</i>	The subscriber line encapsulation type. See the “Usage Guidelines” section for valid encapsulation types.
aal3	Specifies the ATM Adaptation Layer 5 that supports both connectionless and connection-oriented links. You must specify either aal3 or aal5 .
user-defined <i>offset</i>	Specifies the offset size that the router uses when calculating ATM overhead. Valid values are from –127 to 127 bytes; 0 is not a valid value. Note The router configures the offset size if you do not specify the user-defined <i>offset</i> option.
atm	Applies ATM cell tax in the ATM overhead calculation. Note Configuring both the <i>offset</i> and atm options adjusts the packet size to the offset size and then adds ATM cell tax.

Command Default

No bandwidth is specified.
ATM overhead accounting is disabled.

Command Modes

QoS policy-map class configuration (config-pmap-c)

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 and implemented on Versatile Interface Processor (VIP)-enabled Cisco 7500 series routers.
12.0(7)T	This command was modified. The percent keyword was added.
12.0(17)SL	This command was integrated into Cisco IOS Release 12.0(17)SL and implemented on Cisco 10000 series routers.
12.0(22)S	This command was modified. Support for the percent keyword was added on Cisco 10000 series routers.
12.0(23)SX	This command was modified. Support for the remaining percent keyword was added on Cisco 10000 series routers.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T and implemented on VIP-enabled Cisco 7500 series routers.

Release	Modification
12.2(2)T	This command was modified. The remaining percent keyword was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB and implemented on Cisco 10000 series routers.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.0(17)SL and implemented on the PRE3 for the Cisco 10000 series router, and was enhanced for ATM overhead accounting on the Cisco 10000 series router for the PRE3.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(31)SB6	This command was modified to specify an offset size when calculating ATM overhead and implemented on the Cisco 10000 series router for the PRE3.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC and implemented on Cisco 7600 series routers.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB and implemented on Cisco 7300 series routers.
12.4(20)T	This command was modified. Support was added for hierarchical queueing framework (HQF) using the modular quality of service (QoS) CLI (MQC).
15.1(1)T	This command was modified. The allowed values for the <i>kbps</i> argument were changed. The value must be from 8 to 2000000.
15.2(1)T	This command was modified. The allowed values for the offset argument and kbps arguments were changed.

Usage Guidelines

Configuring a Policy Map

Use the **bandwidth** command when you configure a policy map for a class defined by the **class-map** command. The **bandwidth** command specifies the bandwidth for traffic in that class. Class-based weighted fair queueing (CBWFQ) derives the weight for packets belonging to the class from the bandwidth allocated to the class. CBWFQ then uses the weight to ensure that the queue for the class is serviced fairly.

Configuring Strict Priority with Bandwidth

You can configure only one class with strict priority. Other classes cannot have priority or bandwidth configuration. To configure minimum bandwidth for another class, use the **bandwidth remaining percent** command.

Specifying Bandwidth as a Percentage for All Supported Platforms Except the Cisco 10000 Series Routers

Besides specifying the amount of bandwidth in kilobits per second (kbps), you can specify bandwidth as a percentage of either the available bandwidth or the total bandwidth. During periods of congestion, the classes are serviced in proportion to their configured bandwidth percentages. The bandwidth percentage is based on the interface bandwidth. Available bandwidth is equal to the interface bandwidth minus the sum of all bandwidths reserved by the Resource Reservation Protocol (RSVP) feature, the IP RTP Priority feature, and the low latency queueing (LLQ) feature.

**Note**

It is important to remember that when the **bandwidth remaining percent** command is configured, hard bandwidth guarantees may not be provided and only relative bandwidths are assured. That is, class bandwidths are always proportional to the specified percentages of the interface bandwidth. When the link bandwidth is fixed, class bandwidth guarantees are in proportion to the configured percentages. If the link bandwidth is unknown or variable, the router cannot compute class bandwidth guarantees in kbps.

Specifying Bandwidth as a Percentage for the Cisco 10000 Series Routers

Besides specifying the amount of bandwidth in kilobits per second (kbps), you can specify bandwidth as a percentage of either the available bandwidth or the total bandwidth. During periods of congestion, the classes are serviced in proportion to their configured bandwidth percentages. The minimum bandwidth percentage is based on the nearest parent shape rate.

**Note**

It is important to remember that when the **bandwidth remaining percent** command is configured, hard bandwidth guarantees may not be provided and only relative bandwidths are assured. That is, class bandwidths are always proportional to the specified percentages of the interface bandwidth. When the link bandwidth is fixed, class bandwidth guarantees are in proportion to the configured percentages. If the link bandwidth is unknown or variable, the router cannot compute class bandwidth guarantees in kbps.

The router converts the specified bandwidth to the nearest multiple of 1/255 (ESR-PRE1) or 1/65535 (ESR-PRE2) of the interface speed. Use the **show policy-map interface** command to display the actual bandwidth.

Restrictions for All Supported Platforms

The following restrictions apply to the **bandwidth** command:

- The amount of bandwidth configured should be large enough to also accommodate Layer 2 overhead.
- A policy map can have all the class bandwidths specified in either kbps or percentage, but not both, in the same class. However, the unit for the **priority** command in the priority class can be different from the bandwidth unit of the nonpriority class.
- When the **bandwidth percent** command is configured, and a policy map containing class policy configurations is attached to the interface to stipulate the service policy for that interface, available bandwidth is assessed. If a policy map cannot be attached to a particular interface because of insufficient interface bandwidth, the policy is removed from all interfaces to which it was successfully attached. This restriction does not apply to the **bandwidth remaining percent** command.

**Note**

With CSCsy73939, if the **bandwidth percent** command results in a bandwidth value that is lower than the valid range then the policy map specifying this value cannot be attached to an interface, and the router displays the following error message: "service-policy output parent Configured Percent results in out of range kbps. Allowed range is *min-value-max-value*. The present CIR value is *n*."

For more information on bandwidth allocation, see the "Congestion Management Overview" module in the *Cisco IOS Quality of Service Solutions Configuration Guide*.

Note that when the policy map containing class policy configurations is attached to the interface to stipulate the service policy for that interface, available bandwidth is assessed. If a policy map cannot be attached to a particular interface because of insufficient interface bandwidth, then the policy is removed from all interfaces to which it was successfully attached.

Modular QoS CLI Queue Limits

The **bandwidth** command can be used with MQC to specify the bandwidth for a particular class. When used with MQC, the **bandwidth** command uses a default queue limit for the class. This queue limit can be modified using the **queue-limit** command, thereby overriding the default set by the **bandwidth** command.

**Note**

To meet the minimum bandwidth guarantees required by interfaces, modify the default queue limit of high-speed interfaces by using the **queue-limit** command.

Cisco 10000 Series Router

The Cisco 10000 series routers supports the **bandwidth** command on outbound interfaces only. They do not support this command on inbound interfaces.

On the PRE2, you specify a bandwidth value and a unit for the bandwidth value. Valid values for the bandwidth are from 1 to 2488320000. The units are bps, kbps, mbps, and gbps. The default unit is kbps. For example, the following commands configure a bandwidth of 10000 bps and 10000 kbps on the PRE2:

```
bandwidth 10000 bps
bandwidth 10000
```

On the PRE3, you specify only a bandwidth value. Because the unit is always kbps, the PRE3 does not support the unit argument. Valid values are from 1 to 2000000. For example, the following command configures a bandwidth of 128,000 kbps on the PRE3:

```
bandwidth 128000
```

The PRE3 accepts the PRE2 **bandwidth** command only if the command is used without the unit argument. The PRE3 rejects the PRE2 **bandwidth** command if the specified bandwidth is outside the valid PRE3 bandwidth value range (1 to 2000000).

Besides specifying the amount of bandwidth in kilobits per second (kbps), you can specify bandwidth as a percentage of either the available bandwidth or the total bandwidth. During periods of congestion, the classes are serviced in proportion to their configured bandwidth percentages. The bandwidth percentage is based on the interface bandwidth. However, in a hierarchical policy the minimum bandwidth percentage is based on the nearest parent shape rate.

**Note**

When the **bandwidth remaining percent** command is configured, hard bandwidth guarantees may not be provided and only relative bandwidths are assured. Class bandwidths are always proportional to the specified percentages of the interface bandwidth. When the link bandwidth is fixed, class bandwidth guarantees are in proportion to the configured percentages. If the link bandwidth is unknown or variable, the router cannot compute class bandwidth guarantees in kbps.

The router converts the specified bandwidth to the nearest multiple of 1/255 (PRE1) or 1/65535 (PRE2, PRE3) of the interface speed. Use the **show policy-map interface** command to display the actual bandwidth.

Overhead Accounting for ATM (Cisco 10000 Series Router)

When configuring ATM overhead accounting, you must specify the BRAS-DSLAM, DSLAM-CPE, and subscriber line encapsulation types. The router supports the following subscriber line encapsulation types:

- mux-1483routed
- mux-dot1q-rbe
- snap-pppoa
- mux-rbe
- snap-1483routed
- snap-dot1q-rbe
- mux-pppoa
- snap-rbe

The router calculates the offset size unless you specify the **user-defined offset** option.

For hierarchical policies, configure ATM overhead accounting in the following ways:

- Enabled on parent--If you enable ATM overhead accounting on a parent policy, you are not required to enable accounting on the child policy.
- Enabled on child and parent--If you enable ATM overhead accounting on a child policy, then you must enable ATM overhead accounting on the parent policy.

The encapsulation types must match for the child and parent policies.

The user-defined offset values must match for the child and parent policies.

Examples**Examples**

In the following example, the policy map named VLAN guarantees 30 percent of the bandwidth to the class named Customer1 and 60 percent of the bandwidth to the class named Customer2. If you apply the VLAN policy map to a 1-Mbps link, 300 kbps (30 percent of 1 Mbps) is guaranteed to class Customer1 and 600 kbps (60 percent of 1 Mbps) is guaranteed to class Customer2, with 100 kbps remaining for the class-default class. If the class-default class does not need additional bandwidth, the unused 100 kbps is available for use by class Customer1 and class Customer2. If both classes need the bandwidth, they share it in proportion to the configured rates. In this example, the sharing ratio is 30:60 or 1:2:

```
router(config)# policy-map VLAN
```

```

router(config-pmap)# class Customer1
router(config-pmap-c)# bandwidth percent 30
router(config-pmap-c)# exit
router(config-pmap)# class Customer2
router(config-pmap-c)# bandwidth percent 60

```

Examples

The following example shows how to create a policy map with two classes, shows how bandwidth is guaranteed when only CBWFQ is configured, and shows how to attach the policy to serial interface 3/2/1:

```

Router(config)# policy-map policy1
Router(config-pmap)# class class1
Router(config-pmap-c)# bandwidth percent 50
Router(config-pmap-c)# exit
Router(config-pmap)# class class2
Router(config-pmap-c)# bandwidth percent 25
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface serial3/2/1
Router(config-if)# service output policy1
Router(config-if)# end

```

The following output from the **show policy-map** command shows the configuration for the policy map named policy1:

```

Router# show policy-map policy1

Policy Map policy1
  Class class1
    Weighted Fair Queuing
      Bandwidth 50 (%) Max Threshold 64 (packets)
  Class class2
    Weighted Fair Queuing
      Bandwidth 25 (%) Max Threshold 64 (packets)

```

The output from the **show policy-map interface** command shows that 50 percent of the interface bandwidth is guaranteed for the class named class1, and 25 percent is guaranteed for the class named class2. The output displays the amount of bandwidth as both a percentage and a number of kbps.

```

Router# show policy-map interface serial3/2

Serial3/2
Service-policy output:policy1
Class-map:class1 (match-all)
  0 packets, 0 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
  Match:none
  Weighted Fair Queuing
    Output Queue:Conversation 265
    Bandwidth 50 (%)
    Bandwidth 772 (kbps) Max Threshold 64 (packets)
    (pkts matched/bytes matched) 0/0
    (depth/total drops/no-buffer drops) 0/0/0
  Class-map:class2 (match-all)
    0 packets, 0 bytes
    5 minute offered rate 0 bps, drop rate 0 bps
    Match:none
    Weighted Fair Queuing
      Output Queue:Conversation 266
      Bandwidth 25 (%)
      Bandwidth 386 (kbps) Max Threshold 64 (packets)
      (pkts matched/bytes matched) 0/0
      (depth/total drops/no-buffer drops) 0/0/0
  Class-map:class-default (match-any)
    0 packets, 0 bytes
    5 minute offered rate 0 bps, drop rate 0 bps
    Match:any

```

In this example, serial interface 3/2 has a total bandwidth of 1544 kbps. During periods of congestion, 50 percent (or 772 kbps) of the bandwidth is guaranteed to the class named class1, and 25 percent (or 386 kbps) of the link bandwidth is guaranteed to the class named class2.

Examples

In the following example, the interface has a total bandwidth of 1544 kbps. During periods of congestion, 50 percent (or 772 kbps) of the bandwidth is guaranteed to the class named class1, and 25 percent (or 386 kbps) of the link bandwidth is guaranteed to the class named class2.

The following sample output from the **show policy-map** command shows the configuration of a policy map named p1:

```
Router# show policy-map p1
Policy Map p1
Class voice
  Weighted Fair Queuing
  Strict Priority
  Bandwidth 500 (kbps) Burst 12500 (Bytes)
Class class1
  Weighted Fair Queuing
  Bandwidth remaining 50 (%) Max Threshold 64 (packets)
Class class2
  Weighted Fair Queuing
  Bandwidth remaining 25 (%) Max Threshold 64 (packets)
```

The following output from the **show policy-map interface** command on serial interface 3/2 shows that 500 kbps of bandwidth is guaranteed for the class named voice1. The classes named class1 and class2 receive 50 percent and 25 percent of the remaining bandwidth, respectively. Any unallocated bandwidth is divided proportionally among class1, class2, and any best-effort traffic classes.



Note

In this sample output (unlike many of the others earlier in this section) the bandwidth is displayed only as a percentage for class 1 and class 2. Bandwidth expressed as a number of kbps is not displayed because the **percent** keyword was used with the **bandwidth remaining** command. The **bandwidth remaining percent** command allows you to allocate bandwidth as a relative percentage of the total bandwidth available on the interface.

```
Router# show policy-map interface serial13/2

Serial3/2
Service-policy output:p1
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 Queuing
  Strict Priority
  Output Queue:Conversation 264
  Bandwidth 500 (kbps) Burst 12500 (Bytes)
  (pkts matched/bytes matched) 0/0
  (total drops/bytes drops) 0/0
Class-map:class1 (match-all)
  0 packets, 0 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
  Match:none
  Weighted Fair Queuing
  Output Queue:Conversation 265
  Bandwidth remaining 50 (%) Max Threshold 64 (packets)
  (pkts matched/bytes matched) 0/0
  (depth/total drops/no-buffer drops) 0/0/0
Class-map:class2 (match-all)
  0 packets, 0 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
```

```

Match:none
Weighted Fair Queuing
  Output Queue:Conversation 266
  Bandwidth remaining 25 (%) Max Threshold 64 (packets)
  (pkts matched/bytes matched) 0/0
  (depth/total drops/no-buffer drops) 0/0/0
Class-map:class-default (match-any)
  0 packets, 0 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
Match:any

```

Examples

When a parent policy has ATM overhead accounting enabled, you are not required to enable ATM overhead accounting on a child traffic class that does not contain the **bandwidth** or **shape** command. In the following configuration example, ATM overhead accounting is enabled for bandwidth on the gaming and class-default class of the child policy map named subscriber_classes and on the class-default class of the parent policy map named subscriber_line. The voip and video classes do not have ATM overhead accounting explicitly enabled; these priority queues have overhead accounting implicitly enabled because ATM overhead accounting is enabled on the parent policy. Notice that the features in the parent and child policies use the same encapsulation type.

```

Router(config)# policy-map subscriber_classes
Router(config-pmap)# class voip
Router(config-pmap-c)# priority level 1
Router(config-pmap-c)# police 8000
Router(config-pmap-c)# exit
Router(config-pmap)# class video
Router(config-pmap-c)# priority level 2
Router(config-pmap-c)# police 20
Router(config-pmap-c)# exit
Router(config-pmap)# class gaming
Router(config-pmap-c)# bandwidth remaining percent 80 account aal5 snap-rbe-dot1q
Router(config-pmap-c)# exit
Router(config-pmap)# class class-default
Router(config-pmap-c)# bandwidth remaining percent 20 account aal5 snap-rbe-dot1q
Router(config-pmap-c)# policy-map subscriber_line
Router(config-pmap-c)# exit
Router(config-pmap)# class class-default
Router(config-pmap-c)# bandwidth remaining ratio 10 account aal5 snap-rbe-dot1q
Router(config-pmap-c)# shape average 512 account aal5 snap-rbe-dot1q
Router(config-pmap-c)# service policy subscriber_classes

```

In the following example, the router uses 20 overhead bytes and ATM cell tax in calculating ATM overhead. The child and parent policies contain the required matching offset values. The parent policy is attached to virtual template 1.

```

Router(config)# policy-map child
Router(config-pmap)# class class1
Router(config-pmap-c)# bandwidth 500 account user-defined 20 atm
Router(config-pmap-c)# exit
Router(config-pmap)# class class2
Router(config-pmap-c)# shape average 30000 account user-defined 20 atm
Router(config-pmap-c)# exit
Router(config)# exit
Router(config)#

```

Related Commands

Command	Description
class (policy-map)	Specifies the name of the class whose policy you want to create or change, and the default class (commonly known as the class-default class) before you configure its policy.

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class.
max-reserved-bandwidth	Changes the percent of interface bandwidth allocated for CBWFQ, LLQ, and IP RTP Priority.
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
priority	Specifies the priority of a class of traffic belonging to a policy map.
queue-limit	Specifies or modifies the maximum number of packets the queue can hold for a class policy configured in a policy map.
random-detect (interface)	Enables WRED or DWRED.
random-detect exponential-weighting- constant	Configures the WRED and DWRED exponential weight factor for the average queue size calculation.
random-detect precedence	Configures WRED and DWRED parameters for a particular IP precedence.
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.

bandwidth remaining ratio

To specify a bandwidth-remaining ratio for class-level or subinterface-level queues to be used during congestion to determine the amount of excess bandwidth (unused by priority traffic) to allocate to nonpriority queues, use the **bandwidthremainingratio** command in policy-map class configuration mode. To remove the bandwidth-remaining ratio, use the **no** form of this command.

bandwidth remaining ratio *ratio*

no bandwidth remaining ratio *ratio*

bandwidth remaining ratio *ratio* [**account** {**qinq**|**dot1q**} [**aal5**] {*subscriber-encapsulation*|**user-defined offset**}]

no bandwidth remaining ratio *ratio* [**account** {**qinq**|**dot1q**} [**aal5**] {*subscriber-encapsulation*|**user-defined offset**}]

bandwidth remaining ratio *ratio*

no bandwidth remaining ratio *ratio*

Syntax Description

<i>ratio</i>	Relative weight of this subinterface or class queue with respect to other subinterfaces or class queues. Valid values are from 1 to 1000. At the subinterface level, the default value is platform dependent. At the class queue level, the default is 1.
Cisco 7300 Series Router, Cisco 7600 Series Router, and Cisco 10000 Series Router	
<i>ratio</i>	Relative weight of this subinterface or class queue with respect to other subinterfaces or class queues. Note For the Cisco 7300 series router and 7600 series router, valid values are from 1 to 10000, and the default value is 1. Note For the Cisco 10000 series router, valid values are from 1 to 1000, and the default is 1.
account	(Optional) Enables ATM overhead accounting.
qinq	(Optional) Specifies queue-in-queue encapsulation as the Broadband Remote Access Server - Digital Subscriber Line Access Multiplexer (BRAS-DSLAM) encapsulation type.
dot1q	(Optional) Specifies IEEE 802.1Q VLAN encapsulation as the BRAS-DSLAM encapsulation type.

aal5	(Optional) Specifies the ATM adaptation layer 5 that supports connection-oriented variable bit rate (VBR) services.
<i>subscriber-encapsulation</i>	(Optional) Specifies the encapsulation type at the subscriber line. Encapsulation type varies according to subscriber line.
user-defined <i>offset</i>	<p>(Optional) Specifies the offset size, in bytes, that the router uses when calculating the ATM overhead.</p> <p>Note For the Cisco 7300 series router and 7600 series router, valid values are from -48 to +48.</p> <p>Note For the Cisco 10000 series router, valid values are from -63 to +63.</p>
Cisco ASR 1000 Series Routers	
<i>ratio</i>	Relative weight of this subinterface or class queue with respect to other subinterfaces or class queues. Valid values are from 1 to 1000. At the subinterface level and class-queue level, the default is 1.

For most platforms, the default bandwidth ratio is 1.

Command Default

When you use default bandwidth-remaining ratios at the subinterface level, the Cisco 10000 series router distinguishes between interface types. At the subinterface level, the default bandwidth-remaining ratio is 1 for VLAN subinterfaces and Frame Relay Data Link Connection Identifiers (DLCI). For ATM subinterfaces, the router computes the default bandwidth-remaining ratio based on the subinterface speed.

When you use default bandwidth-remaining ratios at the class level, the Cisco 10000 series router makes no distinction between interface types. At the class level, the default bandwidth-remaining ratio is 1.

Command Modes

Policy-map class (config-pmap-c)

Command History

Release	Modification
12.2(31)SB2	This command was introduced. This command was implemented on the Cisco 10000 series router for the PRE3.
12.2(33)SRC	This command was modified. It was implemented on the Cisco 7600 series routers. Additional keywords and arguments were added to support ATM overhead accounting (optional) on the Cisco 7600 series router and the Cisco 10000 series router for the PRE3.

Release	Modification
12.2(33)SB	This command was modified. Support for the Cisco 7300 series routers was added. The additional keyword and arguments associated with ATM overhead accounting were also supported.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

Cisco 10000 Series Router

The scheduler uses the ratio specified in the **bandwidthremainingratio** command to determine the amount of excess bandwidth (unused by priority traffic) to allocate to a class-level queue or a subinterface-level queue during periods of congestion. The scheduler allocates the unused bandwidth relative to other queues or subinterfaces.

The **bandwidthremainingratio** command cannot coexist with another **bandwidth** command in different traffic classes of the same policy map. For example, the following configuration is not valid and causes an error message to display:

```
policy-map Prec1
  class precedence_0
    bandwidth remaining ratio 10
  class precedence_2
    bandwidth 1000
```

For the PRE2, the **bandwidthremainingratio** command can coexist with another **bandwidth** command in the same class of a policy map. On the PRE3, the **bandwidthremainingratio** command cannot coexist with another **bandwidth** command in the same class. For example, the following configuration is not valid on the PRE3 and causes an error message to display:

```
policy-map Prec1
  class precedence_0
    bandwidth 1000
    bandwidth remaining ratio 10
```

In a hierarchical policy map in which the parent policy has only the class-default class defined with a child queuing policy applied, the router accepts only the **bandwidthremainingratio** form of the **bandwidth** command in the class-default class.

The **bandwidthremainingratio** command cannot coexist with the **priority** command in the same class. For example, the following configuration is not valid and causes an error message to display:

```
policy-map Prec1
  class precedence_1
    priority
    police percent 30
    bandwidth remaining ratio 10
```

All of the queues for which the **bandwidthremainingratio** command is not specified receive the platform-specified minimum bandwidth-remaining ratio. The router determines the minimum committed information rate (CIR) based on the configuration.

ATM Overhead Accounting (Optional)

The **bandwidthremainingratio** command can also be used to enable ATM overhead accounting. To enable ATM overhead accounting, use the **account** keyword and the subsequent keywords and arguments as documented in the Syntax Description table.

Cisco 7200 Series Routers

The **bandwidthremainingratio** command is not supported on the Cisco 7200 series routers. If you have upgraded from Cisco IOS Release 12.2(33)SRD to Cisco IOS Release 12.2(33)SRE, you may see parser errors when you run this command. You can use the **bandwidthremainingpercent** command in place of the **bandwidthremainingratio** command on Cisco 7200 series routers to achieve the same functionality.

Examples

Examples

The following example shows how to configure a bandwidth-remaining ratio on an ATM subinterface. In the example, the router guarantees a peak cell rate of 50 Mbps for the variable bit rate nonreal-time (VBR-nrt) PVC 0/200. During periods of congestion, the subinterface receives a share of excess bandwidth (unused by priority traffic) based on the bandwidth-remaining ratio of 10, relative to the other subinterfaces configured on the physical interface.

```
policy-map Child
  class precedence_0
    bandwidth 10000
  class precedence_1
    shape average 100000
    bandwidth 100
  !
policy-map Parent
  class class-default
    bandwidth remaining ratio 10
    shape average 20000000
    service-policy Child
  !
interface ATM2/0/3.200 point-to-point
  ip address 10.20.1.1 255.255.255.0
  pvc 0/200
  protocol ip 10.20.1.2
  vbr-nrt 50000
  encapsulation aal5snap
  service-policy output Parent
```

The following example shows how to configure bandwidth remaining ratios for individual class queues. Some of the classes configured have bandwidth guarantees and a bandwidth-remaining ratio explicitly specified. When congestion occurs within a subinterface level, the class queues receive excess bandwidth (unused by priority traffic) based on their class-level bandwidth-remaining ratios: 20, 30, 120, and 100, respectively, for the precedence_0, precedence_1, precedence_2, and precedence_5 classes. Normally, the precedence_3 class (without a defined ratio) would receive bandwidth based on the bandwidth-remaining ratio of the class-default class defined in the Child policy. However, in the example, the Child policy does not define a class-default bandwidth remaining ratio. Therefore, the router uses a ratio of 1 to allocate excess bandwidth to precedence_3 traffic.

```
policy-map Child
  class precedence_0
    shape average 100000
    bandwidth remaining ratio 20
  class precedence_1
    shape 10000
    bandwidth remaining ratio 30
  class precedence_2
    shape average 200000
    bandwidth remaining ratio 120
  class precedence_3
    set ip precedence 3
  class precedence_5
    set ip precedence 5
    bandwidth remaining ratio 100
policy-map Parent
  class class-default
    bandwidth remaining ratio 10
  service-policy Child
```

```

!
interface GigabitEthernet 2/0/1.10
 encapsulation dot1q 10
 service-policy output Parent

```

Examples

The following example shows how to configure overhead accounting by using the optional **account** keyword and associated keywords and arguments:

```

policy-map subscriber_line
 class class-default
  bandwidth remaining ratio 10 account dot1q aal5 snap-rbe-dot1q
  shape average 512 account dot1q
 aal5 snap-rbe-dot1q
 service-policy subscriber_classes

```

Related Commands

Command	Description
bandwidth remaining percent	Specifies a bandwidth-remaining percentage for class-level or subinterface-level queues to be used during congestion to determine the amount of excess bandwidth (unused by priority traffic) to allocate to nonpriority queues.
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.

class (policy-map)

To specify the name of the class whose policy you want to create or change or to specify the default class (commonly known as the class-default class) before you configure its policy, use the **class** command in policy-map configuration mode. To remove a class from the policy map, use the **no** form of this command.

class {*class-name*| **class-default** [**fragment** *fragment-class-name*]} [**insert-before** *class-name*]
[**service-fragment** *fragment-class-name*]

no class {*class-name*| **class-default**}

Syntax Description

<i>class-name</i>	Name of the class to be configured or whose policy is to be modified. The class name is used for both the class map and to configure a policy for the class in the policy map.
class-default	Specifies the default class so that you can configure or modify its policy.
fragment <i>f</i> <i>ragment-class-name</i>	(Optional) Specifies the default traffic class as a fragment, and names the fragment traffic class.
insert-before <i>class-name</i>	(Optional) Adds a class map between any two existing class maps. Inserting a new class map between two existing class map provides more flexibility when modifying existing policy map configurations. Without this option, the class map is appended to the end of the policy map. This keyword is supported only on flexible packet matching (FPM) policies.
service-fragment <i>fragment-class-name</i>	(Optional) Specifies that the class is classifying a collection of fragments. The fragments being classified by this class must all share the same <i>fragment-class-name</i> .

Command Default

No class is specified.

Command Modes

Policy-map configuration (config-pmap)

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(14)SX	Support for this command was introduced on Cisco 7600 routers.
12.2(17d)SXB	This command was implemented on the Cisco 7600 router and integrated into Cisco IOS Release 12.2(17d)SXB.
12.2(18)SXE	The class-default keyword was added to the Cisco 7600 router.
12.4(4)T	The insert-before <i>class-name</i> option was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(31)SB2	This command was introduced on the PRE3 for the Cisco 10000 series router.
12.2(18)ZY	The insert-before <i>class-name</i> option was integrated into Cisco IOS Release 12.2(18)ZY on the Catalyst 6500 series of switches equipped with the Programmable Intelligent Services Accelerator (PISA).
Cisco IOS XE Release 2.1	This command was implemented on Cisco ASR 1000 series routers. The fragment <i>fragment-class-name</i> and <i>service-fragment</i> <i>fragment-class-name</i> options were introduced.

Usage Guidelines**Policy Map Configuration Mode**

Within a policy map, the **class**(policy-map)command can be used to specify the name of the class whose policy you want to create or change. First, the policy map must be identified.

To identify the policy map (and enter the required policy-map configuration mode), use the **policy-map** command before you use the **class**(policy-map)command. After you specify a policy map, you can configure policy for new classes or modify the policy for any existing classes in that policy map.

Class Characteristics

The class name that you specify in the policy map ties the characteristics for that class--that is, its policy--to the class map and its match criteria, as configured using the **class-map** command.

When you configure policy for a class and specify its bandwidth and attach the policy map to an interface, class-based weighted fair queueing (CBWFQ) determines if the bandwidth requirement of the class can be satisfied. If so, CBWFQ allocates a queue for the bandwidth requirement.

When a class is removed, available bandwidth for the interface is incremented by the amount previously allocated to the class.

The maximum number of classes that you can configure for a router--and, therefore, within a policy map--is 64.

Predefined Default Class

The **class-default** keyword is used to specify the predefined default class called class-default. The class-default class is the class to which traffic is directed if that traffic does not match any of the match criteria in the configured class maps.

Tail Drop or WRED

You can define a class policy to use either tail drop by using the **queue-limit** command or Weighted Random Early Detection (WRED) by using the **random-detect** command. When using either tail drop or WRED, note the following points:

- The **queue-limit** and **random-detect** commands cannot be used in the same class policy, but they can be used in two class policies in the same policy map.
- You can configure the **bandwidth** command when either the **queue-limit** command or the **random-detect** command is configured in a class policy. The **bandwidth** command specifies the amount of bandwidth allocated for the class.
- For the predefined default class, you can configure the **fair-queue** (class-default) command. The **fair-queue** command specifies the number of dynamic queues for the default class. The **fair-queue** command can be used in the same class policy as either the **queue-limit** command or the **random-detect** command. It cannot be used with the **bandwidth** command.

Fragments

A default traffic class is marked as a fragment within a policy map class statement using the **fragment** keyword. Multiple fragments can then be classified collectively in a separate policy map that is created using the **service-fragment** keyword. When fragments are used, default traffic classes marked as fragments have QoS applied separately from the non-default traffic classes.

When using fragments, note the following guidelines:

- Only default traffic classes can be marked as fragments.
- The **fragment**/*fragment-class-name* option within a default class statement marks that default class as a fragment.
- The **service-fragment**/*fragment-class-name* option when defining a class in a policy map is used to specify a class of traffic within the Modular QoS CLI that contains all fragments sharing the same *fragment-class-name*.
- Fragments can only be used within the same physical interface. Policy maps with fragments sharing the same *fragment-class-name* on different interfaces cannot be classified collectively using a class with the **service-fragment**/*fragment-class-name* option.

Cisco 10000 Series Router

The PRE2 allows you to configure 31 class queues in a policy map.

In a policy map, the PRE3 allows you to configure one priority level 1 queue, plus one priority level 2 queue, plus 12 class queues, plus one default queue.

Cisco ASR 1000 Series Routers

The maximum number of classes that you can configure for a Cisco ASR 1000 Series Router--and, therefore, within a policy map--is 8.

Examples

The following example shows how to configure three class policies included in the policy map called policy1. Class1 specifies policy for traffic that matches access control list 136. Class2 specifies policy for traffic on interface ethernet101. The third class is the default class to which packets that do not satisfy configured match criteria are directed:

```
! The following commands create class-maps class1 and class2
! and define their match criteria:
class-map class1
  match access-group 136
class-map class2
  match input-interface ethernet101
! The following commands create the policy map, which is defined to contain policy
! specification for class1, class2, and the default class:
policy-map policy1
Router(config)# policy-map policy1
Router(config-pmap)# class class1
Router(config-pmap-c)# bandwidth 2000
Router(config-pmap-c)# queue-limit 40
Router(config-pmap)# class class2
Router(config-pmap-c)# bandwidth 3000
Router(config-pmap-c)# random-detect
Router(config-pmap-c)# random-detect exponential-weighting-constant 10
Router(config-pmap)# class class-default
Router(config-pmap-c)# fair-queue 16
Router(config-pmap-c)# queue-limit 20
```

- Class1--A minimum of 2000 kbps of bandwidth is expected to be delivered to this class in the event of congestion, and the queue reserved for this class can enqueue 40 packets before tail drop is enacted to handle additional packets.
- Class2--A minimum of 3000 kbps of bandwidth is 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.
- The default class--16 dynamic queues are reserved for traffic that does not meet the match criteria of other classes whose policy is defined by the policy map called policy1, and a maximum of 20 packets per queue is enqueued before tail drop is enacted to handle additional packets.



Note

When the policy map that contains these classes is attached to the interface to stipulate the service policy for that interface, available bandwidth is assessed, taking into account all class policies and Resource Reservation Protocol (RSVP), if configured.

The following example shows how to configure policy for the default class included in the policy map called policy8. The default class has these characteristics: 20 dynamic queues are available for traffic that does not meet the match criteria of other classes whose policy is defined by the policy map called policy8, and a weight factor of 14 is used to calculate the average queue size. For congestion avoidance, WRED packet drop is used, not tail drop:

```
Router(config)# policy-map policy8
Router(config-pmap)# class class-default
Router(config-pmap-c)# fair-queue 20
Router(config-pmap-c)# random-detect exponential-weighting-constant 14
```

The following example shows how to configure policy for a class called `acl136` included in the policy map called `policy1`. Class `acl136` has these characteristics: a minimum of 2000 kbps of bandwidth is expected to be delivered to this class in the event of congestion, and the queue reserved for this class can enqueue 40 packets before tail drop is enacted to handle additional packets. Note that when the policy map that contains this class is attached to the interface to stipulate the service policy for that interface, available bandwidth is assessed, taking into account all class policies and RSVP, if configured:

```
Router(config)# policy-map policy1
Router(config-pmap)# class acl136
Router(config-pmap-c)# bandwidth 2000
Router(config-pmap-c)# queue-limit 40
```

The following example shows how to configure policy for a class called `int101` included in the policy map called `policy8`. Class `int101` has these characteristics: a minimum of 3000 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. Note that when the policy map that contains this class is attached to the interface to stipulate the service policy for that interface, available bandwidth is assessed:

```
Router(config)# policy-map policy8
Router(config-pmap)# class int101
Router(config-pmap-c)# bandwidth 3000
Router(config-pmap-c)# random-detect exponential-weighting-constant 10
```

The following example shows how to configure policy for the **class-default** default class included in the policy map called `policy1`. The **class-default** default class has these characteristics: 10 hashed queues for traffic that does not meet the match criteria of other classes whose policy is defined by the policy map called `policy1`; and a maximum of 20 packets per queue before tail drop is enacted to handle additional enqueued packets:

```
Router(config)# policy-map policy1
Router(config-pmap)# class class-default
Router(config-pmap-c)# fair-queue
Router(config-pmap-c)# queue-limit 20
```

The following example shows how to configure policy for the **class-default** default class included in the policy map called `policy8`. The **class-default** default class has these characteristics: 20 hashed queues for traffic that does not meet the match criteria of other classes whose policy is defined by the policy map called `policy8`; and a weight factor of 14 is used to calculate the average queue size. For congestion avoidance, WRED packet drop is used, not tail drop:

```
Router(config)# policy-map policy8
Router(config-pmap)# class class-default
Router(config-pmap-c)# fair-queue 20
Router(config-pmap-c)# random-detect exponential-weighting-constant 14
```

The following example shows how to configure FPM for blaster packets. The class map contains the following match criteria: TCP port 135, 4444 or UDP port 69; and pattern 0x0030 at 3 bytes from start of IP header:

```
load protocol disk2:ip.phdf
load protocol disk2:tcp.phdf
load protocol disk2:udp.phdf
class-map type stack match-all ip-tcp
  match field ip protocol eq 0x6 next tcp
class-map type stack match-all ip-udp
  match field ip protocol eq 0x11 next udp
class-map type access-control match-all blaster1
  match field tcp dest-port eq 135
  match start 13-start offset 3 size 2 eq 0x0030
class-map type access-control match-all blaster2
  match field tcp dest-port eq 4444
Router(config-cmap)# match start 13-start offset 3 size 2 eq 0x0030
class-map type access-control match-all blaster3
```



```

match field udp dest-port eq 69
match start 13-start offset 3 size 2 eq 0x0030
policy-map type access-control fpm-tcp-policy
  class blaster1
  drop
  class blaster2
  drop
policy-map type access-control fpm-udp-policy
  class blaster3
  drop
policy-map type access-control fpm-policy
  class ip-tcp
  service-policy fpm-tcp-policy
  class ip-udp
  service-policy fpm-udp-policy
interface gigabitEthernet 0/1
  service-policy type access-control input fpm-policy

```

The following example shows how to create a fragment class of traffic to classify the default traffic class named BestEffort. All default traffic from the policy maps named subscriber1 and subscriber2 is part of the fragment default traffic class named BestEffort. This default traffic is then shaped collectively by creating a class called data that uses the **service-fragment** keyword and the **shape** command:

Note the following about this example:

- The *class-name* for each fragment default traffic class is “BestEffort.”
- The *class-name* of “BestEffort” is also used to define the class where the **service-fragment** keyword is entered. This class applies a shaping policy to all traffic forwarded using the fragment default traffic classes named “BestEffort.”

```

policy-map subscriber1
class voice
set cos 5
priority level 1
class video
set cos 4
priority level 2
class class-default fragment BestEffort
shape average 200
bandwidth remaining ratio 10
policy-map subscriber 2
class voice
set cos 5
priority level 1
class video
set cos 4
priority level 2
class class-default fragment BestEffort
shape average 200
bandwidth remaining ratio 10
policy-map input_policy
class class-default
set dscp default
policy-map main-interface
class data service-fragment BestEffort
shape average 400
interface portchannel1.1001
encapsulation dot1q 1001 service-policy output subscriber1
service-policy input input_policy
interface portchannel1.1002
encapsulation dot1q 1002
service-policy output subscriber2
service-policy input input_policy
interface gigabitEthernet 0/1
description member-link1
port channel 1
service-policy output main-interface
interface gigabitEthernet 0/2

```

```

description member-link2
port channel 1
service-policy output main-interface

```

Related Commands

Command	Description
bandwidth (policy-map class)	Specifies or modifies the bandwidth allocated for a class belonging to a policy map.
class-map	Creates a class map to be used for matching packets to a specified class.
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.
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
queue-limit	Specifies or modifies the maximum number of packets the queue can hold for a class policy configured in a policy map.
random-detect (interface)	Enables WRED or DWRED.
random-detect exponential-weighting-constant	Configures the WRED and DWRED exponential weight factor for the average queue size calculation.
random-detect precedence	Configures WRED and DWRED parameters for a particular IP Precedence.

class-map

To create a class map to be used for matching packets to a specified class and to enter QoS class-map configuration mode, use the **class-map** command in global configuration mode. To remove an existing class map from a device, use the **no** form of this command.

Cisco 2600, 3660, 3845, 6500, 7200, 7401, and 7500 Series Routers

class-map [**type** {**stack**| **access-control**| **port-filter**| **queue-threshold**| **logging** *log-class*}] [**match-all**| **match-any**] *class-map-name*

no class-map [**type** {**stack**| **access-control**| **port-filter**| **queue-threshold**| **logging** *log-class*}] [**match-all**| **match-any**] *class-map-name*

Cisco 7600 Series Routers

class-map *class-map-name* [**match-all**| **match-any**]

no class-map *class-map-name* [**match-all**| **match-any**]

Cisco Performance Monitor in Cisco IOS Release 15.1(3)T and 12.2(58)SE

class-map *class-map-name*

no class-map *class-map-name*

Syntax Description

type	(Optional) Specifies the class-map type.
stack	<p>(Optional) Enables the flexible packet matching (FPM) functionality to determine the protocol stack to examine.</p> <p>When you use the load protocol command to load protocol header description files (PHDFs) on the device, a stack of protocol headers can be defined so that the filter can determine which headers are present and in what order.</p>
access-control	<p>(Optional) Determines the pattern to look for in the configured protocol stack.</p> <p>Note You must specify a stack class map (by using the type stack keywords) before specifying an access-control class map (by using the type access-control keywords).</p>
port-filter	(Optional) Creates a port-filter class map that enables the TCP or UDP port policing of control plane packets. When this keyword is enabled, the command filters the traffic that is destined to specific ports on the control-plane host subinterface.

queue-threshold	(Optional) Enables queue thresholding, which limits the total number of packets for a specified protocol allowed in the control plane IP input queue. The queue-thresholding applies only to the control-plane host subinterface.
logging <i>log-class</i>	(Optional) Enables the logging of packet traffic on the control plane. The value for the <i>log-class</i> argument is the name of the log class.
match-all	(Optional) Determines how packets are evaluated when multiple match criteria exist. Matches statements under this class map based on the logical AND function. A packet must match all statements to be accepted. If you do not specify the match-all or match-any keyword, the default keyword used is match-all .
match-any	(Optional) Determines how packets are evaluated when multiple match criteria exist. Matches statements under this class map based on the logical OR function. A packet must match any of the match statements to be accepted. If you do not specify the match-any or match-all keyword, the default keyword is used match-all .
<i>class-map-name</i>	<p>Name of the class for the class map. The class name is used for both the class map and to configure a policy for the class in the policy map.</p> <p>Note You can enter the value for the <i>class-map-name</i> argument within quotation marks. The software does not accept spaces in a class map name entered without quotation marks.</p>

Command Default A class map is not configured.

Command Modes Global configuration (config)

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.

Release	Modification
12.1(1)E	This command was integrated into Cisco IOS Release 12.1(1)E.
12.2(14)SX	This command was integrated into Cisco IOS Release 12.2(14)SX and implemented on Cisco 7600 series routers.
12.2(17d)SXB	This command was integrated into Cisco IOS Release 12.2(17d)SXB and implemented on Cisco 7600 series routers.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(4)T	This command was modified. The stack and access-control keywords were added to support FPM. The port-filter and queue-threshold keywords were added to support control-plane protection.
12.4(6)T	This command was modified. The logging <i>log-class</i> keyword and argument pair was added to support control-plane packet logging.
12.2(18)ZY	This command was modified. The stack and access-control keywords were integrated into Cisco IOS Release 12.2(18)ZY on Catalyst 6500 series switches equipped with the programmable intelligent services accelerator (PISA).
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1 and implemented on Cisco ASR 1000 Series Aggregation Services Routers.
15.1(3)T	This command was integrated into Cisco IOS Release 15.1(3)T for Cisco Performance Monitor with the <i>class-map-name</i> argument as the only syntax element available.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE for Cisco Performance Monitor with the <i>class-map-name</i> argument.
12.2(33)SCF	This command was integrated into Cisco IOS Release 12.2(33)SCF.
15.2(3)T	This command was modified. The software does not accept spaces in a class map name entered without quotation marks.
15.1(2)SNG	This command was integrated into Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

Cisco Performance Monitor in Cisco IOS Release 15.1(3)T and 12.2(58)SE

Only the *class-map-name* argument is available.

Cisco 2600, 3660, 3845, 6500, 7200, 7401, 7500, and ASR 1000 Series Routers

Use the **class-map** command to specify the class that you will create or modify to meet the class-map match criteria. This command enters QoS class-map configuration mode in which you can enter one or more **match**

commands to configure the match criteria for this class. Packets that arrive at either the input interface or the output interface (determined by how the **service-policy** command is configured) are checked against the match criteria that are configured for a class map to determine if packets belong to that class.

When configuring a class map, you can use one or more **match** commands to specify the match criteria. For example, you can use the **match access-group** command, the **match protocol** command, or the **match input-interface** command. The **match** commands vary according to the Cisco software release. For more information about match criteria and **match** commands, see the “Modular Quality of Service Command-Line Interface (CLI) (MQC)” chapter of the *Cisco IOS Quality of Service Solutions Configuration Guide*.

Cisco 7600 Series Routers

Apply the **class-map** command and commands available in QoS class-map configuration mode on a per-interface basis to define packet classification, marking, aggregating, and flow policing as part of a globally named service policy.

You can attach a service policy to an EtherChannel. Do not attach a service policy to a port that is a member of an EtherChannel.

When a device is in QoS class-map configuration mode, the following configuration commands are available:

- **description**—Specifies the description for a class-map configuration.
- **exit**—Exits from QoS class-map configuration mode.
- **match**—Configures classification criteria.
- **no**—Removes a match statement from a class map.

The following commands appear in the CLI help but are not supported on LAN interfaces or WAN interfaces on Optical Service Modules (OSMs):

- **destination-address mac** *mac-address*
- **input-interface** {*interface-type interface-number* | **null** *number* | **vlan** *vlan-id*}
- **protocol** *link-type*
- **source-address mac** *mac-address*

OSMs are not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 32.

Policy Feature Card (PFC) QoS does not support the following commands:

- **destination-address mac** *mac-address*
- **input-interface** {*interface-type interface-number* | **null** *number* | **vlan** *vlan-id*}
- **protocol** *link-type*
- **qos-group** *group-value*
- **source-address mac** *mac-address*

If you enter these commands, PFC QoS does not detect unsupported keywords until you attach a policy map to an interface. When you try to attach the policy map to an interface, an error message is generated. For additional information, see the *Cisco 7600 Series Router Cisco IOS Software Configuration Guide* and Cisco IOS command references.

After configuring the class-map name and the device you can enter the **match access-group** and **match ip dscp** commands in QoS class-map configuration mode. The syntax for these commands is as follows:

match [**access-group** {*acl-index* | *acl-name*} | **ip dscp** | **precedence**] *value*

See the table below for a description of **match** command keywords.

Table 1: match command Syntax Description

Optional command	Description
access-group <i>acl-index</i> <i>acl-name</i>	(Optional) Specifies the access list index or access list names. Valid access list index values are from 1 to 2699.
access-group <i>acl-name</i>	(Optional) Specifies the named access list.
ip dscp <i>value1 value2 ... value8</i>	(Optional) Specifies IP differentiated services code point (DSCP) values to match. Valid values are from 0 to 63. You can enter up to eight DSCP values separated by spaces.
ip precedence <i>value1 value2 ... value8</i>	(Optional) Specifies the IP precedence values to match. Valid values are from 0 to 7. You can enter up to eight precedence values separated by spaces.

Examples

The following example shows how to specify class101 as the name of a class and define a class map for this class. The class named class101 specifies policy for the traffic that matches ACL 101.

```
Device(config)# class-map class101
Device(config-cmap)# match access-group 101
Device(config-cmap)# end
```

The following example shows how to define FPM traffic classes for slammer and UDP packets. The match criteria defined within class maps are for slammer and UDP packets with an IP length that does not exceed 404 (0x194) bytes, UDP port 1434 (0x59A), and pattern 0x4011010 at 224 bytes from the start of the IP header.

```
Device(config)# load protocol disk2:ip.phdf
Device(config)# load protocol disk2:udp.phdf
Device(config)# class-map type stack match-all ip-udp
Device(config-cmap)# description "match UDP over IP packets"
Device(config-cmap)# match field ip protocol eq 0x11 next udp
Device(config-cmap)# exit
Device(config)# class-map type access-control match-all slammer
Device(config-cmap)# description "match on slammer packets"
Device(config-cmap)# match field udp dest-port eq 0x59A
Device(config-cmap)# match field ip length eq 0x194
Device(config-cmap)# match start 13-start offset 224 size 4 eq 0x 4011010
Device(config-cmap)# end
```

The following example shows how to configure a port-filter policy to drop all traffic that is destined to closed or "nonlistening" ports except Simple Network Management Protocol (SNMP):

```
Device(config)# class-map type port-filter pf-class
Device(config-cmap)# match not port udp 123
Device(config-cmap)# match closed-ports
```

```

Device(config-cmap)# exit
Device(config)# policy-map type port-filter pf-policy
Device(config-pmap)# class pf-class
Device(config-pmap-c)# drop
Device(config-pmap-c)# end

```

The following example shows how to configure a class map named ipp5 and enter a match statement for IP precedence 5:

```

Device(config)# class-map ipp5
Device(config-cmap)# match ip precedence 5

```

Examples

The following example shows how to set up a class map and match traffic classes for the 802.1p domain with packet class of service (CoS) values:

```

Device> enable
Device# configure terminal
Device(config)# class-map cos1
Device(config-cmap)# match cos 0
Device(config-pmap-c)# end

```

Examples

The following example shows how to set up a class map and match traffic classes for the Multiprotocol Label Switching (MPLS) domain with packet experimental (EXP) values:

```

Device> enable
Device# configure terminal
Device(config)# class-map exp7
Device(config-cmap)# match mpls experimental topmost 2
Device(config-pmap-c)# end

```

Related Commands

Command	Description
description	Specifies the description for a class map or policy map configuration.
drop	Configures the traffic class to discard packets belonging to a specific class map.
class (policy-map)	Specifies the name of the class whose policy you want to create or change, and the default class before you configure its policy.
load protocol	Loads a PHDF onto a router.
match (class-map)	Configures the match criteria for a class map on the basis of port filter or protocol queue policies.
match access-group	Configures the match criteria for a class map on the basis of the specified ACL.
match input-interface	Configures a class map to use the specified input interface as a match criterion.

Command	Description
match ip dscp	Identifies one or more DSCP, AF, and CS value as a match criterion.
match mpls experimental	Configures a class map to use the specified EXP field value as a match criterion.
match protocol	Configures the match criteria for a class map on the basis of the specified protocol.
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
protocol	Configures a timer and authentication method for a control interface.
qos-group	Associates a QoS group value for a class map.
service-policy	Attaches a policy map to an input interface or VC or to an output interface or VC to be used as the service policy for that interface or VC.
show class-map	Displays class map information.
show policy-map interface	Displays statistics and configurations of input and output policies that are attached to an interface.
source-address	Configures the source-address control on a port.

dscp

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

dscp *dscp-value min-threshold max-threshold* [*mark-probability-denominator*]

no dscp *dscp-value min-threshold max-threshold* [*mark-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 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>mark-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, one 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; one out of every ten packets is dropped at the maximum threshold.

Command Default

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 the table in the “Usage Guidelines” section.

Command Modes

Random-detect-group configuration

Command History

Release	Modification
12.1(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command must be used in conjunction with the **random-detect-group** command.

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

The table below lists the DSCP default settings used by the **dscp** command. The table below lists the DSCP value, and its corresponding minimum threshold, maximum threshold, and mark 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 2: dscp Default Settings

DSCP (Precedence)	Minimum Threshold	Maximum Threshold	Mark 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

DSCP (Precedence)	Minimum Threshold	Maximum Threshold	Mark Probability
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 the DSCP value af22 is 28, the maximum threshold is 40, and the mark probability is 10.

```
Router> enable
Router# configure terminal
Router(config)# random-detect-group class1 dscp-based
Router(cfg-red-group)# dscp af22 28 40 10
Router(cfg-red-group)# end
```

Related Commands

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

match class-map

To use a traffic class as a classification policy, use the **match class-map** command in class-map or policy inline configuration mode. To remove a specific traffic class as a match criterion, use the **no** form of this command.

match class-map *class-map-name*

no match class-map *class-map-name*

Syntax Description

<i>class-map-name</i>	Name of the traffic class to use as a match criterion.
-----------------------	--------------------------------------------------------

Command Default

No match criteria are specified.

Command Modes

Class-map configuration (config-cmap)

Command History

Release	Modification
12.0(5)XE	This 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.
12.4(6)T	This command was enhanced to support Zone-Based Policy Firewall.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB	This command was implemented on the Cisco 10000 series.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 3.2S	This command was integrated into Cisco IOS XE Release 3.2S.

Usage Guidelines

The only method of including both match-any and match-all characteristics in a single traffic class is to use the **match class-map** command. To combine match-any and match-all characteristics into a single class, do one of the following:

- Create a traffic class with the match-any instruction and use a class configured with the match-all instruction as a match criterion (using the **match class-map** command).

- Create a traffic class with the match-all instruction and use a class configured with the match-any instruction as a match criterion (using the **match class-map** command).

You can also use the **match class-map** command to nest traffic classes within one another, saving users the overhead of re-creating a new traffic class when most of the information exists in a previously configured traffic class.

When packets are matched to a class map, a traffic rate is generated for these packets. In a zone-based firewall policy, only the first packet that creates a session matches the policy. Subsequent packets in this flow do not match the filters in the configured policy, but instead match the session directly. The statistics related to subsequent packets are shown as part of the 'inspect' action.

Examples

Examples

In the following example, the traffic class called class1 has the same characteristics as traffic class called class2, with the exception that traffic class class1 has added a destination address as a match criterion. Rather than configuring traffic class class1 line by line, you can enter the **match class-map class2** command. This command allows all of the characteristics in the traffic class called class2 to be included in the traffic class called class1, and you can simply add the new destination address match criterion without reconfiguring the entire traffic class.

```
Router(config)# class-map match-any class2
Router(config-cmap)# match protocol ip
Router(config-cmap)# match qos-group 3
Router(config-cmap)# match access-group 2
Router(config-cmap)# exit
Router(config)# class-map match-all class1
Router(config-cmap)# match class-map class2
Router(config-cmap)# match destination-address mac 1.1.1
Router(config-cmap)# exit
```

The following example shows how to combine the characteristics of two traffic classes, one with match-any and one with match-all characteristics, into one traffic class with the **match class-map** command. The result of traffic class called class4 requires a packet to match one of the following three match criteria to be considered a member of traffic class called class 4: IP protocol *and* QoS group 4, destination MAC address 1.1.1, or access group 2. Match criteria IP protocol *and* QoS group 4 are required in the definition of the traffic class named class3 and included as a possible match in the definition of the traffic class named class4 with the **match class-map class3** command.

In this example, only the traffic class called class4 is used with the service policy called policy1.

```
Router(config)# class-map match-all class3
Router(config-cmap)# match protocol ip
Router(config-cmap)# match qos-group 4
Router(config-cmap)# exit
Router(config)# class-map match-any class4
Router(config-cmap)# match class-map class3
Router(config-cmap)# match destination-address mac 1.1.1
Router(config-cmap)# match access-group 2
Router(config-cmap)# exit
Router(config)# policy-map policy1
Router(config-pmap)# class class4
Router(config-pmap-c)# police 8100 1500 2504 conform-action transmit exceed-action
set-qos-transmit 4
Router(config-pmap-c)# exit
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class.

match cos

To match a packet on the basis of a Layer 2 class of service (CoS)/Inter-Switch Link (ISL) marking, use the **matchcos** command in class-map configuration or policy inline configuration mode. To remove a specific Layer 2 CoS/ISL marking as a match criterion, 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

Supported Platforms Other Than the Cisco 10000 Series Routers	
<i>cos-value</i>	Specific IEEE 802.1Q/ISL CoS value. The <i>cos-value</i> is from 0 to 7; up to four CoS values, separated by a space, can be specified in one matchcos statement.
Cisco 10000 Series Routers	
<i>cos-value</i>	Specific packet CoS bit value. Specifies that the packet CoS bit value must match the specified CoS value. The <i>cos-value</i> is from 0 to 7; up to four CoS values, separated by a space, can be specified in one matchcos statement.

Command Default

Packets are not matched on the basis of a Layer 2 CoS/ISL marking.

Command Modes

Class-map configuration (config-cmap) Policy inline configuration (config-if-spolicy-inline)

Command History

Release	Modification
12.1(5)T	This command was introduced.
12.0(25)S	This command was integrated into Cisco IOS Release 12.0(25)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB and implemented on the Cisco 10000 series routers.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Release	Modification
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC and support for the Cisco 7600 series routers was added.
12.4(15)T2	This command was integrated into Cisco IOS Release 12.4(15)T2.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB and support for the Cisco 7300 series router was added.
15.1(3)T	This command was integrated into Cisco IOS Release 15.1(3)T for Cisco Performance Monitor. Support was added for policy inline configuration mode.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE for Cisco Performance Monitor.
12.2(33)SCF	This command was integrated into Cisco IOS Release 12.2(33)SCF.
3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.
15.1(2)SNG	This command was integrated into Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

This command can be used with both Flexible NetFlow and Performance Monitor. These products use different commands to enter the configuration mode in which you issue this command.

Cisco Performance Monitor in Cisco IOS Release 15.1(3)T and 12.2(58)SE

You must first enter the **service-policy type performance-monitor inline** command.

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 named cos:

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

In the following example, classes named 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 the CoS-based-treatment policy map (in this case, the QoS treatment is priority 64 and bandwidth 512). The service policy configured in this example 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.

```
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
```

Examples

The following example shows how to use the policy inline configuration mode to configure a service policy for Performance Monitor. The policy specifies that packets traversing Ethernet interface 0/0 that match the criteria of a CoS value of 2 will be monitored based on the parameters specified in the flow monitor configuration named **fm-2**:

```
Router(config)# interface ethernet 0/0
Router(config-if)# service-policy type performance-monitor inline input
Router(config-if-spolicy-inline)# match cos 2
Router(config-if-spolicy-inline)# flow monitor fm-2
Router(config-if-spolicy-inline)# exit
```

Examples

The following example shows how to match traffic classes for the 802.1p domain with packet CoS values:

```
Router> enable
Router# config terminal
Router(config)# class-map cos7
Router(config-cmap)# match cos 2
Router(config-cmap)# exit
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class.
service-policy type performance-monitor	Associates a Performance Monitor policy with an interface.
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 protocol

To configure the match criterion for a class map on the basis of a specified protocol, use the **match protocol** command in class-map configuration or policy inline configuration mode. To remove the protocol-based match criterion from the class map, use the **no** form of this command.

match protocol *protocol-name*

no match protocol *protocol-name*

Syntax Description

<i>protocol-name</i>	Name of the protocol (for example, bgp) used as a matching criterion. See the “Usage Guidelines” for a list of protocols supported by most routers.
----------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------

Command Default

No match criterion is configured.

Command Modes

Class-map configuration (config-cmap) Policy inline configuration (config-if-spolicy-inline)

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(13)E	This command was integrated into Cisco IOS Release 12.1(13)E and implemented on Catalyst 6000 family switches without FlexWAN modules.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(13)T	This command was modified to remove apollo , vines , and xns from the list of protocols used as matching criteria. These protocols were removed because Apollo Domain, Banyan VINES, and Xerox Network Systems (XNS) were removed in this release. The IPv6 protocol was added to support matching on IPv6 packets.
12.0(28)S	This command was integrated into Cisco IOS Release 12.0(28)S for IPv6.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(17a)SX1	This command was integrated into Cisco IOS Release 12.2(17a)SX1.

Release	Modification
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE and implemented on the Supervisor Engine 720.
12.4(6)T	This command was modified. The Napster protocol was removed because it is no longer supported.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2 and implemented on the Cisco 10000 series routers.
12.2(18)ZY	This command was integrated into Cisco IOS Release 12.2(18)ZY. This command was modified to enhance Network-Based Application Recognition (NBAR) functionality on the Catalyst 6500 series switch that is equipped with the Supervisor 32/programmable intelligent services accelerator (PISA) engine.
12.4(15)XZ	This command was integrated into Cisco IOS Release 12.4(15)XZ.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T and implemented on the Cisco 1700, Cisco 1800, Cisco 2600, Cisco 2800, Cisco 3700, Cisco 3800, Cisco 7200, and Cisco 7300 series routers.
Cisco IOS XE Release 2.2	This command was integrated into Cisco IOS XE Release 2.2 and implemented on the Cisco ASR 1000 Series Routers.
Cisco IOS XE Release 3.1S	This command was modified. Support for more protocols was added.
15.1(3)T	This command was integrated into Cisco IOS Release 15.1(3)T for Cisco Performance Monitor. Support was added for policy inline configuration mode.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE for Cisco Performance Monitor.

Usage Guidelines

This command can be used with both Flexible NetFlow and Performance Monitor. These products use different commands to enter the configuration mode in which you issue this command.

Cisco Performance Monitor in Cisco IOS Release 15.1(3)T and 12.2(58)SE

You must first enter the **service-policytypeperformance-monitorinline** command.

Supported Platforms Other Than Cisco 7600 Routers and Cisco 10000 Series Routers

For class-based weighted fair queueing (CBWFQ), you define traffic classes based on match criteria protocols, access control lists (ACLs), input interfaces, quality of service (QoS) labels, and Experimental (EXP) field values. Packets satisfying the match criteria for a class constitute the traffic for that class.

The **matchprotocol** command specifies the name of a protocol to be used as the match criteria against which packets are checked to determine if they belong to the class specified by the class map.

The **matchprotocolipx** command matches packets in the output direction only.

To use the **matchprotocol** command, you must first enter the **class-map** command to specify the name of the class whose match criteria you want to establish. After you identify the class, you can use one of the following commands to configure its match criteria:

- **match access-group**
- **match input-interface**
- **match mpls experimental**

If you specify more than one command in a class map, only the last command entered applies. The last command overrides the previously entered commands.

To configure NBAR to match protocol types that are supported by NBAR traffic, use the **matchprotocol(NBAR)** command.

Cisco 7600 Series Routers

The **matchprotocol** command in QoS class-map configuration configures NBAR and sends all traffic on the port, both ingress and egress, to be processed in the software on the Multilayer Switch Feature Card 2 (MSFC2). For CBWFQ, you define traffic classes based on match criteria like protocols, ACLs, input interfaces, QoS labels, and Multiprotocol Label Switching (MPLS) EXP field values. Packets satisfying the match criteria for a class constitute the traffic for that class.

The **matchprotocol** command specifies the name of a protocol to be used as the match criteria against which packets are checked to determine if they belong to the class specified by the class map.

If you want to use the **matchprotocol** command, you must first enter the **class-map** command to specify the name of the class to which you want to establish the match criteria.

If you specify more than one command in a class map, only the last command entered applies. The last command overrides the previously entered commands.

This command can be used to match protocols that are known to the NBAR feature. For a list of protocols supported by NBAR, see the “Classification” part of the *Cisco IOS Quality of Service Solutions Configuration Guide*.

Cisco 10000 Series Routers

For CBWFQ, you define traffic classes based on match criteria including protocols, ACLs, input interfaces, QoS labels, and EXP field values. Packets satisfying the match criteria for a class constitute the traffic for that class.

The **matchprotocol** command specifies the name of a protocol to be used as the match criteria against which packets are checked to determine if they belong to the class specified by the class map.

The **matchprotocolipx** command matches packets in the output direction only.

To use the **matchprotocol** command, you must first enter the **class-map** command to specify the name of the class whose match criteria you want to establish.

If you are matching NBAR protocols, use the **matchprotocol(NBAR)** command.

Match Protocol Command Restrictions (Catalyst 6500 Series Switches Only)

Policy maps contain traffic classes. Traffic classes contain one or more **match** commands that can be used to match packets (and organize them into groups) on the basis of a protocol type or application. You can create as many traffic classes as needed.

Cisco IOS Release 12.2(18)ZY includes software intended for use on the Catalyst 6500 series switch that is equipped with a Supervisor 32/PISA engine. For this release and platform, note the following restrictions for using policy maps and **matchprotocol** commands:

- A single traffic class can be configured to match a maximum of 8 protocols or applications.
- Multiple traffic classes can be configured to match a cumulative maximum of 95 protocols or applications.

Supported Protocols

The table below lists the protocols supported by most routers. Some routers support a few additional protocols. For example, the Cisco 7600 router supports the AARP and DECnet protocols, while the Cisco 7200 router supports the directconnect and PPPOE protocols. For a complete list of supported protocols, see the online help for the **matchprotocol** command on the router that you are using.

Table 3: Supported Protocols

Protocol Name	Description
802-11-iapp	IEEE 802.11 Wireless Local Area Networks Working Group Internet Access Point Protocol
ace-svr	ACE Server/Propagation
aol	America-Online Instant Messenger
appleqt	Apple QuickTime
arp *	IP Address Resolution Protocol (ARP)
bgp	Border Gateway Protocol
biff	Biff mail notification
bootpc	Bootstrap Protocol Client
bootps	Bootstrap Protocol Server
bridge *	bridging
cddbp	CD Database Protocol
cdp *	Cisco Discovery Protocol
cifs	CIFS
cisco-fna	Cisco FNATIVE
cisco-net-mgmt	cisco-net-mgmt
cisco-svcs	Cisco license/perf/GDP/X.25/ident svcs

Protocol Name	Description
cisco-sys	Cisco SYSMANT
cisco-tdp	cisco-tdp
cisco-tna	Cisco TNATIVE
citrix	Citrix Systems Metaframe
citriximaclient	Citrix IMA Client
clns *	ISO Connectionless Network Service
clns_es *	ISO CLNS End System
clns_is *	ISO CLNS Intermediate System
clp	Cisco Line Protocol
cmns *	ISO Connection-Mode Network Service
cmp	Cluster Membership Protocol
compressedtcp *	Compressed TCP
creativepartnr	Creative Partner
creativeserver	Creative Server
cuseeme	CU-SeeMe desktop video conference
daytime	Daytime (RFC 867)
dbase	dBASE Unix
dbcontrol_agent	Oracle Database Control Agent
ddns-v3	Dynamic DNS Version 3
dhcp	Dynamic Host Configuration
dhcp-failover	DHCP Failover
directconnect	Direct Connect
discard	Discard port
dns	Domain Name Server lookup

Protocol Name	Description
dnsix	DNSIX Security Attribute Token Map
echo	Echo port
edonkey	eDonkey
egp	Exterior Gateway Protocol
eigrp	Enhanced Interior Gateway Routing Protocol
entrust-svc-handler	Entrust KM/Admin Service Handler
entrust-svcs	Entrust sps/aaas/aams
exec	Remote Process Execution
exchange	Microsoft RPC for Exchange
fasttrack	FastTrack Traffic (KaZaA, Morpheus, Grokster, and so on)
fcip-port	FCIP
finger	Finger
ftp	File Transfer Protocol
ftps	FTP over TLS/SSL
gdoi	Group Domain of Interpretation
giop	Oracle GIOP/SSL
gnutella	Gnutella Version 2 Traffic (BearShare, Shareeza, Morpheus, and so on)
gopher	Gopher
gre	Generic Routing Encapsulation
gtpv0	GPRS Tunneling Protocol Version 0
gtpv1	GPRS Tunneling Protocol Version 1
h225ras	H225 RAS over Unicast
h323	H323 Protocol

Protocol Name	Description
h323callsigalt	H323 Call Signal Alternate
hp-alarm-mgr	HP Performance data alarm manager
hp-collector	HP Performance data collector
hp-managed-node	HP Performance data managed node
hsrp	Hot Standby Router Protocol
http	Hypertext Transfer Protocol
https	Secure Hypertext Transfer Protocol
ica	ica (Citrix)
icabrowser	icabrowser (Citrix)
icmp	Internet Control Message Protocol
ident	Authentication Service
igmpv3lite	IGMP over UDP for SSM
imap	Internet Message Access Protocol
imap3	Interactive Mail Access Protocol 3
imaps	IMAP over TLS/SSL
ip *	IP (version 4)
ipass	IPASS
ipinip	IP in IP (encapsulation)
ipsec	IP Security Protocol (ESP/AH)
ipsec-msft	Microsoft IPsec NAT-T
ipv6 *	IP (version 6)
ipx	IPX
irc	Internet Relay Chat
irc-serv	IRC-SERV

Protocol Name	Description
ircs	IRC over TLS/SSL
ircu	IRCU
isakmp	ISAKMP
iscsi	iSCSI
iscsi-target	iSCSI port
kazaa2	Kazaa Version 2
kerberos	Kerberos
l2tp	Layer 2 Tunnel Protocol
ldap	Lightweight Directory Access Protocol
ldap-admin	LDAP admin server port
ldaps	LDAP over TLS/SSL
llc2 *	llc2
login	Remote login
lotusmtap	Lotus Mail Tracking Agent Protocol
lotusnote	Lotus Notes
mgcp	Media Gateway Control Protocol
microsoft-ds	Microsoft-DS
msexch-routing	Microsoft Exchange Routing
msnmsgr	MSN Instant Messenger
msrpc	Microsoft Remote Procedure Call
msrpc-smb-netbios	MSRPC over TCP port 445
ms-cluster-net	MS Cluster Net
ms-dotnetster	Microsoft .NETster Port
ms-sna	Microsoft SNA Server/Base

Protocol Name	Description
ms-sql	Microsoft SQL
ms-sql-m	Microsoft SQL Monitor
mysql	MySQL
n2h2server	N2H2 Filter Service Port
ncp	NCP (Novell)
net8-cman	Oracle Net8 Cman/Admin
netbios	Network Basic Input/Output System
netbios-dgm	NETBIOS Datagram Service
netbios-ns	NETBIOS Name Service
netbios-ssn	NETBIOS Session Service
netshow	Microsoft Netshow
netstat	Variant of systat
nfs	Network File System
nntp	Network News Transfer Protocol
novadigm	Novadigm Enterprise Desktop Manager (EDM)
ntp	Network Time Protocol
oem-agent	OEM Agent (Oracle)
oracle	Oracle
oracle-em-vp	Oracle EM/VP
oraclenames	Oracle Names
orasrv	Oracle SQL*Net v1/v2
ospf	Open Shortest Path First
pad *	Packet assembler/disassembler (PAD) links
pcanywhere	Symantec pcANYWHERE

Protocol Name	Description
pcanywheredata	pcANYWHEREdata
pcanywherestat	pcANYWHEREstat
pop3	Post Office Protocol
pop3s	POP3 over TLS/SSL
pppoe	Point-to-Point Protocol over Ethernet
pptp	Point-to-Point Tunneling Protocol
printer	Print spooler/ldp
pwdgen	Password Generator Protocol
qmtip	Quick Mail Transfer Protocol
radius	RADIUS & Accounting
rcmd	Berkeley Software Distribution (BSD) r-commands (rsh, rlogin, rexec)
rdb-dbs-disp	Oracle RDB
realmedia	RealNetwork's Realmedia Protocol
realsecure	ISS Real Secure Console Service Port
rip	Routing Information Protocol
router	Local Routing Process
rsrb *	Remote Source-Route Bridging
rsvd	RSVD
rsvp	Resource Reservation Protocol
rsvp-encap	RSVP ENCAPSULATION-1/2
rsvp_tunnel	RSVP Tunnel
rtc-pm-port	Oracle RTC-PM port
rtelnet	Remote Telnet Service
rtp	Real-Time Protocol

Protocol Name	Description
rtsp	Real-Time Streaming Protocol
r-winsock	remote-winsock
secure-ftp	FTP over Transport Layer Security/Secure Sockets Layer (TLS/SSL)
secure-http	Secured HTTP
secure-imap	Internet Message Access Protocol over TLS/SSL
secure-irc	Internet Relay Chat over TLS/SSL
secure-ldap	Lightweight Directory Access Protocol over TLS/SSL
secure-nntp	Network News Transfer Protocol over TLS/SSL
secure-pop3	Post Office Protocol over TLS/SSL
secure-telnet	Telnet over TLS/SSL
send	SEND
shell	Remote command
sip	Session Initiation Protocol
sip-tls	Session Initiation Protocol-Transport Layer Security
skinny	Skinny Client Control Protocol
sms	SMS RCINFO/XFER/CHAT
smtp	Simple Mail Transfer Protocol
snapshot	Snapshot routing support
snmp	Simple Network Protocol
snmptrap	SNMP Trap
socks	Sockets network proxy protocol (SOCKS)
sqlnet	Structured Query Language (SQL)*NET for Oracle
sqlserv	SQL Services
sqlsrv	SQL Service

Protocol Name	Description
sqlserver	Microsoft SQL Server
ssh	Secure shell
sshell	SSLshell
ssp	State Sync Protocol
streamwork	Xing Technology StreamWorks player
stun	cisco Serial Tunnel
sunrpc	Sun remote-procedure call (RPC)
syslog	System Logging Utility
syslog-conn	Reliable Syslog Service
tacacs	Login Host Protocol (TACACS)
tacacs-ds	TACACS-Database Service
tarantella	Tarantella
tcp	Transport Control Protocol
telnet	Telnet
telnets	Telnet over TLS/SSL
tftp	Trivial File Transfer Protocol
time	Time
timed	Time server
tr-rsrb	cisco RSRB
tto	Oracle TTC/SSL
udp	User Datagram Protocol
uucp	UUCPD/UUCP-RLOGIN
vdolive	VDOLive streaming video
vofr *	Voice over Frame Relay

Protocol Name	Description
vqp	VLAN Query Protocol
webster	Network Dictionary
who	Who's service
wins	Microsoft WINS
x11	X Window System
xdmcp	XDM Control Protocol
xwindows *	X-Windows remote access
ymsg	Yahoo! Instant Messenger

* This protocol is not supported on the Catalyst 6500 series switch that is equipped with a Supervisor 32/PISA engine.

Examples

The following example specifies a class map named ftp and configures the FTP protocol as a match criterion:

```
Router(config)# class-map ftp
Router(config-cmap)
#
  match protocol ftp
```

Cisco Performance Monitor in Cisco IOS Release 15.1(3)T and 12.2(58)SE

The following example shows how to use the policy inline configuration mode to configure a service policy for Performance Monitor. The policy specifies that packets traversing Ethernet interface 0/0 for the IP protocol will be monitored based on the parameters specified in the flow monitor configuration named **fm-2**:

```
Router(config)# interface ethernet 0/0
Router(config-if)# service-policy type performance-monitor inline input
Router(config-if-spolicy-inline)# match protocol ip
Router(config-if-spolicy-inline)# flow monitor fm-2
Router(config-if-spolicy-inline)# exit
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class.
service-policy type performance-monitor	Associates a Performance Monitor policy with an interface.
match access-group	Configures the match criteria for a class map based on the specified ACL.

Command	Description
match input-interface	Configures a class map to use the specified input interface as a match criterion.
match mpls experimental	Configures a class map to use the specified value of the experimental field as a match criterion.
match precedence	Identifies IP precedence values as match criteria.
match protocol (NBAR)	Configures NBAR to match traffic by a protocol type known to NBAR.
match qos-group	Configures a class map to use the specified EXP field value as a match criterion.

match qos-group

To identify a specific quality of service (QoS) group value as a match criterion, use the **match qos-group** command in class-map configuration or policy inline configuration mode. To remove a specific QoS group value from a class map, use the **no** form of this command.

match qos-group *qos-group-value*

no match qos-group *qos-group-value*

Syntax Description

<i>qos-group-value</i>	The exact value from 0 to 99 used to identify a QoS group value.
------------------------	------------------------------------------------------------------

Command Default

No match criterion is specified.

Command Modes

Class-map configuration (config-cmap) Policy inline configuration (config-if-spolicy-inline)

Command History

Release	Modification
11.1CC	This command was introduced.
12.0(5)XE	This command was integrated into Cisco IOS Release 12.0(5)XE.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB and implemented on the Cisco 10000 series routers.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1 and implemented on Cisco ASR 1000 Series Routers.
15.1(3)T	This command was integrated into Cisco IOS Release 15.1(3)T for Cisco Performance Monitor. Support was added for policy inline configuration mode.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE for Cisco Performance Monitor.

Usage Guidelines

This command can be used with both Flexible NetFlow and Performance Monitor. These products use different commands to enter the configuration mode in which you issue this command.

The **matchqos-group** command is used by the class map to identify a specific QoS group value marking on a packet. This command can also be used to convey the received Multiprotocol Label Switching (MPLS) experimental (EXP) field value to the output interface.

The *qos-group-value* argument is used as a marking only. The QoS group values have no mathematical significance. For instance, the *qos-group-value* of 2 is not greater than 1. The value simply indicates that a packet marked with the *qos-group-value* of 2 is different than a packet marked with the *qos-group-value* of 1. The treatment of these packets is defined by the user through the setting of QoS policies in QoS policy-map class configuration mode.

The QoS group value is local to the router, meaning that the QoS group value that is marked on a packet does not leave the router when the packet leaves the router. If you need a marking that resides in the packet, use IP precedence setting, IP differentiated services code point (DSCP) setting, or another method of packet marking.

This command can be used with the **random-detectdiscard-class-based** command.

Cisco Performance Monitor in Cisco IOS Release 15.1(3)T and 12.2(58)SE

You must first enter the **service-policytypeperformance-monitorinline** command.

Examples

The following example shows how to configure the service policy named priority50 and attach service policy priority50 to an interface. In this example, the class map named qosgroup5 will evaluate all packets entering Fast Ethernet interface 1/0/0 for a QoS group value of 5. If the incoming packet has been marked with the QoS group value of 5, the packet will be treated with a priority level of 50.

```
Router(config)#

class-map qosgroup5
Router(config-cmap)
#
  match qos-group 5
Router(config)#

exit
Router(config)#

policy-map priority50
Router(config-pmap)#

class qosgroup5
Router(config-pmap-c)#

priority 50
Router(config-pmap-c)#

exit
Router(config-pmap)#

exit
Router(config)#

interface fastethernet1/0/0
Router(config-if)#

service-policy output priority50
```

Examples

The following example shows how to use the policy inline configuration mode to configure a service policy for Performance Monitor. The policy specifies that packets traversing Ethernet interface 0/0 that match the criteria of a QoS value of 4 will be monitored based on the parameters specified in the flow monitor configuration named **fm-2**:

```
Router(config)# interface ethernet 0/0
Router(config-if)# service-policy type performance-monitor inline input
Router(config-if-spolicy-inline)# match qosgroup 4
Router(config-if-spolicy-inline)# flow monitor fm-2
Router(config-if-spolicy-inline)# exit
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class.
service-policy type performance-monitor	Associates a Performance Monitor policy with an interface.
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
random-detect discard-class-based	Bases WRED on the discard class value of a packet.
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 precedence	Specifies an IP precedence value for packets within a traffic class.
set qos-group	Sets a group ID that can be used later to classify packets.

mls qos (global configuration mode)

To enable the quality of service (QoS) functionality globally, use the **mls qos** command in global configuration mode. To disable the QoS functionality globally, use the **no** form of this command.

mls qos

no mls qos

Syntax Description This command has no arguments or keywords.

Command Default QoS is globally disabled.

Command Modes Global configuration

Command History	Release	Modification
	12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
	12.2(17d)SXB	This command was implemented on the Supervisor Engine 2 and integrated into Cisco IOS Release 12.2(17d)SXB.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

If you enable QoS globally, QoS is enabled on all interfaces with the exception of the interfaces where you disabled QoS. If you disable QoS globally, all traffic is passed in QoS pass-through mode.

In port-queueing mode, Policy Feature Card (PFC) QoS (marking and policing) is disabled, and packet type of service (ToS) and class of service (CoS) are not changed by the PFC. All queueing on rcv and xmt is based on a QoS tag in the incoming packet, which is based on the incoming CoS.

For 802.1Q or Inter-Switch Link (ISL)-encapsulated port links, queueing is based on the packet 802.1Q or ISL CoS.

For the router main interfaces or access ports, queueing is based on the configured per-port CoS (the default CoS is 0).

This command enables or disables ternary content addressable memory (TCAM) QoS on all interfaces that are set in the OFF state.

Examples This example shows how to enable QoS globally:

```
Router(config)# mls qos
Router(config)#
```

This example shows how to disable QoS globally on the Cisco 7600 series routers:

```
Router(config)# no mls qos
Router(config)#
```

Related Commands

Command	Description
mls qos (interface configuration mode)	Enables the QoS functionality on an interface.
show mls qos	Displays MLS QoS information.

mls qos (interface configuration mode)

To enable the quality of service (QoS) functionality on an interface, use the **mls qos** command in interface configuration command mode. To disable QoS functionality on an interface, use the **no** form of this command.

mls qos

no mls qos

Syntax Description This command has no arguments or keywords.

Command Default Enabled

Command Modes Interface configuration

Command History	Release	Modification
	12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is deprecated on Cisco 7600 series routers that are configured with a Supervisor Engine 2. Although the CLI allows you to configure PFC-based QoS on the WAN ports on the OC-12 ATM OSMs and on the WAN ports on the channelized OSMs, PFC-based QoS is not supported on the WAN ports on these OSMs.

If you disable QoS globally, it is also disabled on all interfaces.

This command enables or disables TCAM QoS (classification, marking, and policing) for the interface.

Examples This example shows how to enable QoS on an interface:

```
Router(config-if)# mls qos
```

Related Commands

Command	Description
mls qos (global configuration mode)	Enables the QoS functionality globally.
show mls qos	Displays MLS QoS information.



P through V

- [policy-map, page 68](#)
- [priority-group, page 75](#)
- [priority level, page 78](#)
- [priority-list default, page 80](#)
- [priority-list interface, page 82](#)
- [priority-list protocol, page 84](#)
- [priority-list queue-limit, page 89](#)
- [service-policy, page 91](#)
- [set cos, page 101](#)
- [set qos-group, page 105](#)
- [show auto discovery qos, page 109](#)
- [show auto qos, page 113](#)
- [show policy-map, page 118](#)
- [show policy-map class, page 134](#)
- [show policy-map interface, page 136](#)
- [show queue, page 185](#)
- [show queueing, page 191](#)
- [show queueing interface, page 198](#)
- [vbr-nrt, page 203](#)

policy-map

To enter policy-map configuration mode and create or modify a policy map that can be attached to one or more interfaces to specify a service policy, use the **policy-map** command in global configuration mode. To delete a policy map, use the **no** form of this command.

Supported Platforms Other Than Cisco 10000 and Cisco 7600 Series Routers

policy-map [**type** {**stack**|**access-control**|**port-filter**|**queue-threshold**|**logging** *log-policy*}] *policy-map-name*

no policy-map [**type** {**stack**|**access-control**|**port-filter**|**queue-threshold**|**logging** *log-policy*}]
policy-map-name

Cisco 10000 Series Router

policy-map [**type** {**control**|**service**}] *policy-map-name*

no policy-map [**type** {**control**|**service**}] *policy-map-name*

Cisco CMTS and 7600 Series Router

policy-map [**type** {**class-routing** **ipv4** **unicast** *unicast-name*|**control** *control-name*|**service** *service-name*}]
policy-map-name

no policy-map [**type** {**class-routing** **ipv4** **unicast** *unicast-name*|**control** *control-name*|**service** *service-name*}]
policy-map-name

Syntax Description

type	(Optional) Specifies the policy-map type.
stack	(Optional) Determines the exact pattern to look for in the protocol stack of interest.
access-control	(Optional) Enables the policy map for the flexible packet matching feature.
port-filter	(Optional) Enables the policy map for the port-filter feature.
queue-threshold	(Optional) Enables the policy map for the queue-threshold feature.
logging	(Optional) Enables the policy map for the control-plane packet logging feature.
<i>log-policy</i>	(Optional) Type of log policy for control-plane logging.
<i>policy-map-name</i>	Name of the policy map.
control	(Optional) Creates a control policy map.

<i>control-name</i>	Name of the control policy map.
service	(Optional) Creates a service policy map.
<i>service-name</i>	Name of the policy-map service.
class-routing	Configures the class-routing policy map.
ipv4	Configures the class-routing IPv4 policy map.
unicast	Configures the class-routing IPv4 unicast policy map.
<i>unicast-name</i>	Unicast policy-map name.

Command Default The policy map is not configured.

Command Modes Global configuration (config)

Command History	Release	Modification
	12.0(5)T	This command was introduced.
	12.4(4)T	This command was modified. The type and access-control keywords were added to support flexible packet matching. The port-filter and queue-threshold keywords were added to support control-plane protection.
	12.4(6)T	This command was modified. The logging keyword was added to support control-plane packet logging.
	12.2(31)SB	This command was modified. The control and service keywords were added to support the Cisco 10000 series router.
	12.2(18)ZY	This command was modified. <ul style="list-style-type: none"> • The type and access-control keywords were integrated into Cisco IOS Release 12.2(18)ZY on the Catalyst 6500 series switch that is equipped with the Supervisor 32/programmable intelligent services accelerator (PISA) engine. • The command was modified to enhance the Network-Based Application Recognition (NBAR) functionality on the Catalyst 6500 series switch that is equipped with the Supervisor 32/PISA engine.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Release	Modification
12.2(33)SRC	This command was modified. Support for this command was implemented on Cisco 7600 series routers.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1 and implemented on Cisco ASR 1000 series routers.
12.2(33)SCF	This command was integrated into Cisco IOS Release 12.2(33)SCF.

Usage Guidelines

Use the **policy-map** command to specify the name of the policy map to be created, added, or modified before you configure policies for classes whose match criteria are defined in a class map. The **policy-map** command enters policy-map configuration mode, in which you can configure or modify the class policies for a policy map.

You can configure class policies in a policy map only if the classes have match criteria defined for them. Use the **class-map** and **match** commands to configure match criteria for a class. Because you can configure a maximum of 64 class maps, a policy map cannot contain more than 64 class policies, except as noted for quality of service (QoS) class maps on Cisco 7600 systems.



Note

For QoS class maps on Cisco 7600 series routers, the limits are 1024 class maps and 256 classes in a policy map.

A policy map containing ATM set cell loss priority (CLP) bit QoS cannot be attached to PPP over X (PPPoX) sessions. The policy map is accepted only if you do not specify the **set atm-clp** command.

A single policy map can be attached to more than one interface concurrently. Except as noted, when you attempt to attach a policy map to an interface, the attempt is denied if the available bandwidth on the interface cannot accommodate the total bandwidth requested by class policies that make up the policy map. In such cases, if the policy map is already attached to other interfaces, the map is removed from those interfaces.



Note

This limitation does not apply on Cisco 7600 series routers that have session initiation protocol (SIP)-400 access-facing line cards.

Whenever you modify a class policy in an attached policy map, class-based weighted fair queuing (CBWFQ) is notified and the new classes are installed as part of the policy map in the CBWFQ system.



Note

Policy-map installation via subscriber-profile is not supported. If you configure an unsupported policy map and there are a large number of sessions, an equally large number of messages print on the console. For example, if there are 32,000 sessions, then 32,000 messages print on the console at 9,600 baud.

Class Queues (Cisco 10000 Series Routers Only)

The Performance Routing Engine (PRE)2 allows you to configure 31 class queues in a policy map.

In a policy map, the PRE3 allows you to configure one priority level 1 queue, one priority level 2 queue, 12 class queues, and one default queue.

Control Policies (Cisco 10000 Series Routers Only)

Control policies define the actions that your system will take in response to the specified events and conditions.

A control policy is made of one or more control policy rules. A control policy rule is an association of a control class and one or more actions. The control class defines the conditions that must be met before the actions are executed.

There are three steps involved in defining a control policy:

- 1 Using the **class-map type control** command, create one or more control class maps.
- 2 Using the **policy-map type control** command, create a control policy map.

A control policy map contains one or more control policy rules. A control policy rule associates a control class map with one or more actions. Actions are numbered and executed sequentially.

- 1 Using the **service-policy type control** command, apply the control policy map to a context.

Service Policies (Cisco 10000 Series Routers Only)

Service policy maps and service profiles contain a collection of traffic policies and other functions. Traffic policies determine which function is applied to which session traffic. A service policy map or service profile may also contain a network-forwarding policy, which is a specific type of traffic policy that determines how session data packets will be forwarded to the network.

Policy Map Restrictions (Catalyst 6500 Series Switches Only)

Cisco IOS Release 12.2(18)ZY includes software intended for use on the Catalyst 6500 series switch that is equipped with a Supervisor 32/PISA engine. This release and platform has the following restrictions for using policy maps and **match** commands:

- You cannot modify an existing policy map if the policy map is attached to an interface. To modify the policy map, remove the policy map from the interface by using the **no** form of the **service-policy** command.
- Policy maps contain traffic classes. Traffic classes contain one or more **match** commands that can be used to match packets (and organize them into groups) on the basis of a protocol type or application. You can create as many traffic classes as needed. However, the following restrictions apply:
 - A single traffic class can be configured to match a maximum of 8 protocols or applications.
 - Multiple traffic classes can be configured to match a cumulative maximum of 95 protocols or applications.

Examples

The following example shows how to create a policy map called “policy1” and configure two class policies included in that policy map. The class policy called “class1” specifies a policy for traffic that matches access control list (ACL) 136. The second class is the default class to which packets that do not satisfy the configured match criteria are directed.

```
! The following commands create class-map class1 and define its match criteria:
class-map class1
```

```

match access-group 136
! The following commands create the policy map, which is defined to contain policy
! specification for class1 and the default class:
policy-map policy1
class class1
  bandwidth 2000
  queue-limit 40
class class-default
  fair-queue 16
  queue-limit 20

```

The following example shows how to create a policy map called “policy9” and configure three class policies to belong to that map. Of these classes, two specify the policy for classes with class maps that specify match criteria based on either a numbered ACL or an interface name, and one specifies a policy for the default class called “class-default” to which packets that do not satisfy the configured match criteria are directed.

```

policy-map policy9

class acl136
  bandwidth 2000
  queue-limit 40

class ethernet101
  bandwidth 3000
  random-detect exponential-weighting-constant 10
class class-default
  fair-queue 10
  queue-limit 20

```

The following is an example of a modular QoS command-line interface (MQC) policy map configured to initiate the QoS service at the start of a session.

```

Router> enable
Router# configure terminal
Router(config)# policy-map type control TEST
Router(config-control-policymap)# class type control always event session-start
Router(config-control-policymap-class-control)# 1
  service-policy type service name QoS_Service
Router(config-control-policymap-class-control)# end

```

Examples

The following example shows the configuration of a control policy map named “rule4”. Control policy map rule4 contains one policy rule, which is the association of the control class named “class3” with the action to authorize subscribers using the network access server (NAS) port ID. The **service-policy type control** command is used to apply the control policy map globally.

```

class-map type control match-all class3
  match access-type pppoe
  match domain cisco.com
  available nas-port-id
!
policy-map type control rule4
  class type control class3
  authorize nas-port-id
!
service-policy type control rule4

```

The following example shows the configuration of a service policy map named “redirect-profile”:

```

policy-map type service redirect-profile
  class type traffic CLASS-ALL
  redirect to group redirect-sg

```

Examples

The following example shows how to define a policy map for the 802.1p domain:

```
enable
configure terminal
policy-map cos7
  class cos7
    set cos 2
  end
```

The following example shows how to define a policy map for the MPLS domain:

```
enable
configure terminal
policy-map exp7
  class exp7
    set mpls experimental topmost 2
  end
```

Related Commands

Command	Description
bandwidth (policy-map class)	Specifies or modifies the bandwidth allocated for a class belonging to a policy map.
class (policy-map)	Specifies the name of the class whose policy you want to create or change, and its default class before you configure its policy.
class class-default	Specifies the default class whose bandwidth is to be configured or modified.
class-map	Creates a class map to be used for matching packets to a specified class.
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.
match access-group	Configures the match criteria for a class map on the basis of the specified ACL.
queue-limit	Specifies or modifies the maximum number of packets that the queue can hold for a class policy configured in a policy map.
random-detect (interface)	Enables WRED or DWRED.
random-detect exponential-weighting-constant	Configures the WRED and DWRED exponential weight factor for the average queue size calculation.
random-detectservice-policy precedence	Configures WRED and DWRED parameters for a particular IP precedence.

Command	Description
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 atm-clp precedence	Sets the ATM CLP bit when a policy map is configured.

priority-group

**Note**

Effective with Cisco IOS Release 15.1(3)T, the **priority-group** command is hidden. Although this command is still available in Cisco IOS software, the CLI interactive Help does not display it if you attempt to view it by entering a question mark at the command line. This command will be completely removed in a future release, which means that you will need to use the appropriate replacement command (or sequence of commands). For more information (including a list of replacement commands), see the "Legacy QoS Command Deprecation" feature document in the *Cisco IOS Quality of Service Solutions Configuration Guide*.

To assign the specified priority list to an interface, use the **priority-group** command in interface configuration mode. To remove the specified priority group assignment, use the **no** form of this command.

priority-group *list-number*

no priority-group *list-number*

Syntax Description

<i>list-number</i>	Priority list number assigned to the interface. Any number from 1 to 16.
--------------------	--------------------------------------------------------------------------

Command Default

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)T	This command was modified. This command was hidden.

Usage Guidelines

Only one list can be assigned per interface. Priority output queueing provides a mechanism to prioritize packets sent on an interface.

Use the **show queueing** and **show interfaces** commands to display the current status of the output queues.

Examples

The following example causes packets for transmission on serial interface 0 to be classified by priority list 1:

```
interface serial 0
  priority-group 1
```

The following example shows how to establish queueing priorities based on the address of the serial link on a serial tunnel (STUN) connection. Note that you must use the **priority-group** interface configuration command to assign a priority group to an output interface.

```
stun peer-name 172.16.0.0
stun protocol-group 1 sdlc
!
interface serial 0
! Disable the ip address for interface serial 0:
no ip address
! Enable the interface for STUN:
encapsulation stun
!
stun group 2
stun route address 10 tcp 172.16.0.1 local-ack priority
!
! Assign priority group 1 to the input side of interface serial 0:
priority-group 1
! Assign a low priority to priority list 1 on serial link identified
! by group 2 and address A7:
priority-list 1 stun low address 2 A7
```

Related Commands

Command	Description
locaddr-priority-list	Maps LUs to queueing priorities as one of the steps to establishing queueing priorities based on LU addresses.
priority-list default	Assigns a priority queue for those packets that do not match any other rule in the priority list.
priority-list interface	Establishes queueing priorities on packets entering from a given interface.
priority-list protocol	Establishes queueing priorities based on the protocol type.
priority-list protocol ip tcp	Establishes BSTUN or STUN queueing priorities based on the TCP port.
priority-list protocol stun address	Establishes STUN queueing priorities based on the address of the serial link.
priority-list queue-limit	Specifies the maximum number of packets that can be waiting in each of the priority queues.
show interfaces	Displays statistics for all interfaces configured on the router or access server.

Command	Description
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.

priority level

To configure multiple priority queues, use the **priority level** command in policy-map class configuration mode. To remove a previously specified priority level for a class, use the **no** form of this command.

priority level *level*

no priority level *level*

Syntax Description

<i>level</i>	<p>Defines multiple levels of a strict priority service model. When you enable a traffic class with a specific level of priority service, the implication is a single priority queue associated with all traffic that is enabled with the specified level of priority service.</p> <p>Valid values are from 1 (high priority) to 4 (low priority). Default is 1. For Cisco ASR 1000 Series Routers and the Cisco ASR 903 Series Routers, valid values are from 1 (high priority) to 2 (low priority). Default is 1.</p>
--------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Command Default

The priority level has a default level of 1.

Command Modes

Policy-map class configuration (config-pmap-c)

Command History

Release	Modification
12.2(31)SB2	This command was introduced to provide multiple levels of strict priority queuing and implemented on the Cisco 10000 Series Router for the PRE3.
Cisco IOS XE Release 2.1	This command was implemented on Cisco ASR 1000 Series Routers.
Cisco IOS XE Release 3.7S	This command was implemented on Cisco ASR 903 Series Routers.

Usage Guidelines

The **bandwidth** and **priority level** commands cannot be used in the same class, within the same policy map. These commands can be used in the same policy map, however.

The **shape** and **priority level** commands cannot be used in the same class, within the same policy map. These commands can be used in the same policy map, however.

Within a policy map, you can give one or more classes priority status. The router associates a single priority queue with all of the traffic enabled with the same priority level and services the high-level priority queues until empty before servicing the next-level priority queues and non-priority queues.

You cannot specify the same priority level for two different classes in the same policy map.

You cannot specify the **priority** command and the **priority level** command for two different classes in the same policy map. For example, you cannot specify the **priority bandwidth** *kbps* or **priority percent** *percentage* command and the **priority level** command for different classes.

When the **priority level** command is configured with a specific level of priority service, the **queue-limit** and **random-detect** commands can be used only if a single class at that level of priority is configured.

You cannot configure the default queue as a priority queue at any priority level.

Cisco 10000 Series Router, Cisco ASR 1000 Series Router, and Cisco ASR 903 Series Router

The Cisco 10000 series router, the Cisco ASR 1000 Series Router, and the Cisco ASR 903 Series Router support two levels of priority service: level 1 (high) and level 2 (low). If you do not specify a priority level, the routers use the default level of 1. Level 1 specifies that low-latency behavior must be given to the traffic class. The high-level queues are serviced until empty before the next-level queues and non-priority queues.

Examples

The following example shows how to configure multi level priority queues. In the example, the traffic class named Customer1 is given high priority (level 1), and the class named Customer2 is given level 2 priority. To prevent Customer2 traffic from becoming starved of bandwidth, Customer1 traffic is policed at 30 percent of the available bandwidth.

```
Router> enable
Router# config terminal
Router(config)# policy-map Business
Router(config-pmap)# class Customer1
Router(config-pmap-c)# priority level 1
Router(config-pmap-c)# police 30
Router(config-pmap-c)# exit
Router(config-pmap)# class Customer2
Router(config-pmap-c)# priority level 2
```

Related Commands

Command	Description
bandwidth	Specifies or modifies the bandwidth allocated for a class belonging to a policy map.
priority	Assigns priority to a class of traffic.
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. Displays statistical information for all priority levels configured.

priority-list default

To assign a priority queue for those packets that do not match any other rule in the priority list, use the **priority-listdefault** command in global configuration mode. To return to the default or assign **normal** as the default, use the **no** form of this command.

priority-list *list-number* **default** {**high**| **medium**| **normal**| **low**}

no priority-list *list-number* **default**

Syntax Description

<i>list-number</i>	Any number from 1 to 16 that identifies the priority list.
high medium normal low	Priority queue level. The normal queue is used if you use the no form of this command.

Command Default

This command is not enabled by default.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

When you use multiple rules, remember that the system reads the priority settings in order of appearance. When classifying a packet, the system searches the list of rules specified by **priority-list** commands for a matching protocol or interface type. When a match is found, the system assigns the packet to the appropriate queue. The system searches the list in the order specified, and the first matching rule terminates the search.

Examples

The following example sets the priority queue for those packets that do not match any other rule in the priority list to a low priority:

```
priority-list 1 default low
```

Related Commands

Command	Description
priority-group	Assigns the specified priority list to an interface.
priority-list interface	Establishes queueing priorities on packets entering from a given interface.
priority-list protocol	Establishes queueing priorities based on the protocol type.
priority-list queue-limit	Specifies the maximum number of packets that can be waiting in each of the priority queues.
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.

priority-list interface

To establish queueing priorities on packets entering from a given interface, use the **priority-list interface** command in global configuration mode. To remove an entry from the list, use the **no** form of this command with the appropriate arguments.

priority-list *list-number* **interface** *interface-type* *interface-number* {**high**| **medium**| **normal**| **low**}

no priority-list *list-number* **interface** *interface-type* *interface-number* {**high**| **medium**| **normal**| **low**}

Syntax Description

<i>list-number</i>	Any number from 1 to 16 that identifies the priority list.
<i>interface-type</i>	The type of the interface.
<i>interface-number</i>	The number of the interface.
high medium normal low	Priority queue level.

Command Default

No queueing priorities are established by default.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

When you use multiple rules, remember that the system reads the priority settings in order of appearance. When classifying a packet, the system searches the list of rules specified by **priority-list** commands for a matching protocol or interface type. When a match is found, the system assigns the packet to the appropriate queue. The system searches the list in the order specified, and the first matching rule terminates the search.

Examples

The following example assigns a list entering on serial interface 0 to a medium priority queue level:

```
priority-list 3 interface serial 0 medium
```

**Note**

This command defines a rule that determines how packets are attached to an interface. Once the rule is defined, the packet is actually attached to the interface using the **priority-group** command.

Related Commands

Command	Description
priority-group	Assigns the specified priority list to an interface.
priority-list default	Assigns a priority queue for those packets that do not match any other rule in the priority list.
priority-list protocol	Establishes queueing priorities based on the protocol type.
priority-list queue-limit	Specifies the maximum number of packets that can be waiting in each of the priority queues.
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.

priority-list protocol

To establish queueing priorities based upon the protocol type, use the **priority-list protocol** command in global configuration mode. To remove a priority list entry assigned by protocol type, use the **no** form of this command with the appropriate arguments.

priority-list *list-number* **protocol** *protocol-name* {**high**|**medium**|**normal**|**low**} *queue-keyword* *keyword-value*
no priority-list *list-number* **protocol** *protocol-name* {**high**|**medium**|**normal**|**low**} *queue-keyword* *keyword-value*

Syntax Description

<i>list-number</i>	Any number from 1 to 16 that identifies the priority list.
<i>protocol-name</i>	Protocol type: aarp , appletalk , arp , bridge (transparent), clns , clns_es , clns_is , compressedtcp , cmns , decnet , decnet_node , decnet_router-l1 , decnet_router-l2 , dls , ip , ipx , pad , rsrb , stun , and x25 .
high medium normal low	Priority queue level.
<i>queue-keyword</i> <i>keyword-value</i>	Possible keywords are fragments , gt , list , lt , tcp , and udp . For more information about keywords and values, see Table 20 in the “Usage Guidelines” section.

Command Default

No queueing priorities are established.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.0	This command was introduced.
12.2(13)T	This command was modified. The apollo , vines , and xns keywords were removed from the list of protocol types. These protocols were removed because Apollo Domain, Banyan VINES, and Xerox Network Systems (XNS) were removed in Release 12.2(13)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Release	Modification
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

When you use multiple rules for a single protocol, remember that the system reads the priority settings in order of appearance. When classifying a packet, the system searches the list of rules specified by **priority-list** commands for a matching protocol type. When a match is found, the system assigns the packet to the appropriate queue. The system searches the list in the order specified, and the first matching rule terminates the search.

The **decnet_router-I1** keyword refers to the multicast address for all level 1 routers, which are intra-area routers, and the **decnet_router-I2** keyword refers to all level 2 routers, which are interarea routers.

The **dlsw**, **rsrb**, and **stun** keywords refer only to direct encapsulation.

Use the tables below to configure the queuing priorities for your system.

Table 4: Protocol Priority Queue Keywords and Values

Option	Description
fragments	<p>Assigns the priority level defined to fragmented IP packets (for use with IP only). More specifically, this command matches IP packets whose fragment offset field is nonzero. The initial fragment of a fragmented IP packet has a fragment offset of zero, so such packets are not matched by this command.</p> <p>Note Packets with a nonzero fragment offset do not contain TCP or User Datagram Protocol (UDP) headers, so other instances of this command that use the tcp or udp keyword will always fail to match such packets.</p>
gt <i>byte-count</i>	<p>Specifies a greater-than count. The priority level assigned goes into effect when a packet size exceeds the value entered for the <i>byte-count</i> argument.</p> <p>Note The size of the packet must also include additional bytes because of MAC encapsulation on the outgoing interface.</p>
list <i>list-number</i>	<p>Assigns traffic priorities according to a specified list when used with AppleTalk, bridging, IP, IPX, VINES, or XNS. The <i>list-number</i> argument is the access list number as specified by the access-list global configuration command for the specified <i>protocol-name</i>. For example, if the protocol is AppleTalk, <i>list-number</i> should be a valid AppleTalk access list number.</p>

Option	Description
lt <i>byte-count</i>	Specifies a less-than count. The priority level assigned goes into effect when a packet size is less than the value entered for the <i>byte-count</i> argument. Note The size of the packet must also include additional bytes because of MAC encapsulation on the outgoing interface.
tcp <i>port</i>	Assigns the priority level defined to TCP segments originating from or destined to a specified port (for use with IP only). Table 21 lists common TCP services and their port numbers.
udp <i>port</i>	Assigns the priority level defined to UDP packets originating from or destined to a specified port (for use with IP only). Table 22 lists common UDP services and their port numbers.

Table 5: Common TCP Services and Their Port Numbers

Service	Port
FTP data	20
FTP	21
Simple Mail Transfer Protocol (SMTP)	25
Telnet	23

**Note**

To display a complete list of TCP services and their port numbers, enter a help string, such as the following example: Router(config)#**prioritylist4protocolipmediumtcp?**

Table 6: Common UDP Services and Their Port Numbers

Service	Port
Domain Name System (DNS)	53
Network File System (NFS)	2049
remote-procedure call (RPC)	111
SNMP	161

Service	Port
TFTP	69

**Note**

To display a complete list of UDP services and their port numbers, enter a help string, such as the following example: Router(config)#**prioritylist4protocolipmediumudp?**

**Note**

The tables above include some of the more common TCP and UDP port numbers. However, you can specify any port number to be prioritized; you are not limited to those listed. For some protocols, such as TFTP and FTP, only the initial request uses port 69. Subsequent packets use a randomly chosen port number. For these types of protocols, the use of port numbers fails to be an effective method to manage queued traffic.

Examples

The following example shows how to assign 1 as the arbitrary priority list number, specify DECnet as the protocol type, and assign a high-priority level to the DECnet packets sent on this interface:

```
priority-list 1 protocol decnet high
```

The following example shows how to assign a medium-priority level to every DECnet packet with a size greater than 200 bytes:

```
priority-list 2 protocol decnet medium gt 200
```

The following example shows how to assign a medium-priority level to every DECnet packet with a size less than 200 bytes:

```
priority-list 4 protocol decnet medium lt 200
```

The following example shows how to assign a high-priority level to traffic that matches IP access list 10:

```
priority-list 1 protocol ip high list 10
```

The following example shows how to assign a medium-priority level to Telnet packets:

```
priority-list 4 protocol ip medium tcp 23
```

The following example shows how to assign a medium-priority level to UDP DNS packets:

```
priority-list 4 protocol ip medium udp 53
```

The following example shows how to assign a high-priority level to traffic that matches Ethernet type code access list 201:

```
priority-list 1 protocol bridge high list 201
```

The following example shows how to assign a high-priority level to data-link switching plus (DLSw+) traffic with TCP encapsulation:

```
priority-list 1 protocol ip high tcp 2065
```

The following example shows how to assign a high-priority level to DLSw+ traffic with direct encapsulation:

```
priority-list 1 protocol dls w high
```

**Note**

This command defines a rule that determines how packets are attached to an interface. Once the rule is defined, the packet is actually attached to the interface using the **priority-group** command.

Related Commands

Command	Description
priority-group	Assigns the specified priority list to an interface.
priority-list default	Assigns a priority queue for those packets that do not match any other rule in the priority list.
priority-list interface	Establishes queueing priorities on packets entering from a given interface.
priority-list queue-limit	Specifies the maximum number of packets that can be waiting in each of the priority queues.
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.

priority-list queue-limit

To specify the maximum number of packets that can be waiting in each of the priority queues, use the **priority-listqueue-limit** command in global configuration mode. To select the normal queue, use the **no** form of this command.

priority-list *list-number* **queue-limit** *high-limit medium-limit normal-limit low-limit*

no priority-list *list-number* **queue-limit**

Syntax Description

<i>list-number</i>	Any number from 1 to 16 that identifies the priority list.
<i>high-limit medium-limit normal-limit low-limit</i>	Priority queue maximum length. A value of 0 for any of the four arguments means that the queue can be of unlimited size for that particular queue. For default values for these arguments, see the table below.

Command Default

None. See the table below in the “Usage Guidelines” section of this command for a list of the default queue limit arguments.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If a priority queue overflows, excess packets are discarded and messages can be sent, if appropriate, for the protocol.

The default queue limit values are listed in the table below.

Table 7: Default Priority Queue Packet Limits

Priority Queue Argument	Packet Limits
<i>high-limit</i>	20
<i>medium-limit</i>	40
<i>normal-limit</i>	60
<i>low-limit</i>	80

**Note**

If priority queueing is enabled and there is an active Integrated Services Digital Network (ISDN) call in the queue, changing the configuration of the **priority-listqueue-limit** command drops the call from the queue. For more information about priority queueing, refer to the *Cisco IOS Quality of Service Solutions Configuration Guide*.

Examples

The following example shows how to set the maximum packets in the priority queue to 10:

```
Router(config)# priority-list 2 queue-limit 10 40 60 80
```

Related Commands

Command	Description
priority-group	Assigns the specified priority list to an interface.
priority-list default	Assigns a priority queue for those packets that do not match any other rule in the priority list.
priority-list interface	Establishes queueing priorities on packets entering from a given interface.
priority-list protocol	Establishes queueing priorities based on the protocol type.
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.

service-policy

To attach a policy map to an input interface, a virtual circuit (VC), an output interface, or a VC that will be used as the service policy for the interface or VC, use the **service-policy** command in the appropriate configuration mode. To remove a service policy from an input or output interface or from an input or output VC, use the **no** form of this command.

service-policy [**type access-control**] {**input**| **output**} *policy-map-name*

no service-policy [**type access-control**] {**input**| **output**} *policy-map-name*

Cisco 10000 Series and Cisco 7600 Series Routers

service-policy [**history**] {**input**| **output**} *policy-map-name* | **type control** *control-policy-name*]

no service-policy [**history**] {**input**| **output**} *policy-map-name* | **type control** *control-policy-name*]

Syntax Description

type access-control	(Optional) Determines the exact pattern to look for in the protocol stack of interest.
input	Attaches the specified policy map to the input interface or input VC.
output	Attaches the specified policy map to the output interface or output VC.
<i>policy-map-name</i>	The name of a service policy map (created using the policy-map command) to be attached. The name can be a maximum of 40 alphanumeric characters in length.
history	(Optional) Maintains a history of quality of service (QoS) metrics.
type control <i>control-policy-name</i>	(Optional) Creates a Class-Based Policy Language (CPL) control policy map that is applied to a context.

Command Default

No service policy is specified. A control policy is not applied to a context. No policy map is attached.

Command Modes

ATM VC bundle configuration (config-atm-bundle)
 ATM PVP configuration (config-if-atm-l2trans-pvp)
 ATM VC configuration mode (config-if-atm-vc)
 Ethernet service configuration (config-if-srv)
 Global configuration (config)

Interface configuration (config-if)

Static maps class configuration (config-map-class)

ATM PVC-in-range configuration (cfg-if-atm-range-pvc)

Subinterface configuration (config-subif)

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.
12.0(17)SL	This command was implemented on the Cisco 10000 series routers.
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 enable low latency queueing (LLQ) on Frame Relay VCs.
12.2(14)SX	Support for this command was implemented on Cisco 7600 series routers. Support was added for output policy maps.
12.2(15)BX	This command was implemented on the ESR-PRE2.
12.2(17d)SXB	This command was implemented on the Supervisor Engine 2 and integrated into Cisco IOS Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(2)T	This command was modified. Support was added for subinterface configuration mode and for ATM PVC-in-range configuration mode to extend policy map functionality on an ATM VC to the ATM VC range.
12.4(4)T	The type stack and type control keywords were added to support flexible packet matching (FPM).
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000 series router.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.3(7)XI2	This command was modified to support subinterface configuration mode and ATM PVC-in-range configuration mode for ATM VCs on the Cisco 10000 series router and the Cisco 7200 series router.
12.2(18)ZY	The type stack and type control keywords were integrated into Cisco IOS Release 12.2(18)ZY on the Catalyst 6500 series of switches equipped with the Programmable Intelligent Services Accelerator (PISA).

Release	Modification
12.2(33)SRC	Support for this command was enhanced on Cisco 7600 series routers.
12.2(33)SB	This command was modified. The command was implemented on the Cisco 10000 series router for the PRE3 and PRE4.
Cisco IOS XE Release 2.3	This command was modified to support ATM PVP configuration mode.
12.4(18e)	This command was modified to prevent simultaneous configuration of legacy traffic-shaping and Cisco Modular QoS CLI (MQC) shaping on the same interface.
Cisco IOS XE Release 3.3S	This command was modified to support Ethernet service configuration mode.
Cisco IOS XE Release 3.5S	This command was modified. An error displays if you try to configure the service-policy input or service-policy output command when the ip subscriber interface command is already configured on the interface.
15.2(1)S	This command was modified to allow simultaneous nonqueueing policies to be enabled on subinterfaces.

Usage Guidelines

The table below shows which configuration mode to choose based on the intended use of the command.

Table 8: Configuration Modes Based on Command Application

Application	Mode
Standalone VC	ATM VC submodule
ATM VC bundle members	ATM VC Bundle configuration
A range of ATM PVCs	Subinterface configuration
Individual PVC within a PVC range	ATM PVC-in-range configuration
Frame Relay VC	Static maps class configuration
Ethernet services, Ethernet VCs (EVCs)	Ethernet service configuration

You can attach a single policy map to one or more interfaces or to one or more VCs to specify the service policy for those interfaces or VCs.

A service policy specifies class-based weighted fair queueing (CBWFQ). The class policies that make up the policy map are then applied to packets that satisfy the class map match criteria for the class.

Before you can attach a policy map to an interface or ATM VC, the aggregate of the configured minimum bandwidths of the classes that make up the policy map must be less than or equal to 75 percent (99 percent on the Cisco 10008 router) of the interface bandwidth or the bandwidth allocated to the VC.

Before you can enable low latency queueing (LLQ) for Frame Relay (priority queueing [PQ]/CBWFQ), you must first enable Frame Relay traffic shaping (FRTS) on the interface using the **frame-relay traffic-shaping** command in interface configuration mode. You then attach an output service policy to the Frame Relay VC using the **service-policy** command in Static maps class configuration mode.

To attach a policy map to an interface or ATM VC, the aggregate of the configured minimum bandwidths of the classes that make up the policy map must be less than or equal to 75 percent of the interface bandwidth or the bandwidth allocated to the VC. For a Frame Relay VC, the total amount of bandwidth allocated must not exceed the minimum committed information rate (CIR) configured for the VC less any bandwidth reserved by the **frame-relay voice bandwidth** or **frame-relay ip rtp priority** Static maps class configuration mode commands. If these values are not configured, the minimum CIR defaults to half of the CIR.

Configuring CBWFQ on a physical interface is possible only if the interface is in the default queueing mode. Serial interfaces at E1 (2.048 Mbps) and below use weighted fair queueing (WFQ) by default. Other interfaces use first-in first-out (FIFO) by default. Enabling CBWFQ on a physical interface overrides the default interface queueing method. Enabling CBWFQ on an ATM permanent virtual circuit (PVC) does not override the default queueing method.

When you attach a service policy with CBWFQ enabled to an interface, commands related to fancy queueing such as those pertaining to fair queueing, custom queueing, priority queueing, and Weighted Random Early Detection (WRED) are available using the modular quality of service CLI (MQC). However, you cannot configure these features directly on the interface until you remove the policy map from the interface.

**Note**

Beginning in Cisco IOS Release 12.4(18e), you cannot configure the traffic-shape rate and MQC shaping on the same interface at the same time. You must remove the traffic-shape rate configured on the interface before you attach the service policy. For example, if you try to enter the **service-policy {input | output} policy-map-name** command when the **traffic-shape rate** command is already in effect, this message is displayed:

```
Remove traffic-shape rate configured on the interface before attaching the service-policy.
If the MQC shaper is attached first, and you enter the legacy traffic-shape rate command on the same
interface, the command is rejected and an error message is displayed.
```

You can modify a policy map attached to an interface or VC, changing the bandwidth of any of the classes that make up the map. Bandwidth changes that you make to an attached policy map are effective only if the aggregate of the bandwidth amount for all classes that make up the policy map, including the modified class bandwidth, is less than or equal to 75 percent of the interface bandwidth or the VC bandwidth. If the new aggregate bandwidth amount exceeds 75 percent of the interface bandwidth or VC bandwidth, the policy map is not modified.

After you apply the **service-policy** command to set a class of service (CoS) bit to an Ethernet interface, the policy remains active as long as there is a subinterface that is performing 802.1Q or Inter-Switch Link (ISL) trunking. Upon reload, however, the service policy is removed from the configuration with the following error message:

```
Process "set" action associated with class-map voip failed: Set cos supported only with
IEEE 802.1Q/ISL interfaces.
```

**Note**

The **service-policy input** and **service-policy output** commands cannot be configured if the **ip subscriber interface** command is already configured on the interface; these commands are mutually exclusive.

Simultaneous Nonqueueing QoS Policies

Beginning in Cisco IOS Release 15.2(1)S, you can configure simultaneous nonqueueing QoS policies on an ATM subinterface and ATM PVC, or on a Frame Relay (FR) subinterface and data-link connection identifier (DLCI). However, simultaneous queueing policies are still not allowed, because they create hierarchical queueing framework layer contention. If you try to configure simultaneous queueing policies, the policies are rejected and the router displays an error message.



Note

If both the PVC or DLCI and subinterface policies are applied under the same subinterface, the policy under the PVC or DLCI takes precedence and the subinterface policy has no effect.

Cisco 10000 Series Router Usage Guidelines

The Cisco 10000 series router does not support applying CBWFQ policies to unspecified bit rate (UBR) VCs.

To attach a policy map to an interface or a VC, the aggregate of the configured minimum bandwidth of the classes that make up the policy map must be less than or equal to 99 percent of the interface bandwidth or the bandwidth allocated to the VC. If you attempt to attach a policy map to an interface when the sum of the bandwidth assigned to classes is greater than 99 percent of the available bandwidth, the router logs a warning message and does not allocate the requested bandwidth to all of the classes. If the policy map is already attached to other interfaces, it is removed from them.

The total bandwidth is the speed (rate) of the ATM layer of the physical interface. The router converts the minimum bandwidth that you specify to the nearest multiple of 1/255 (ESR-PRE1) or 1/65,535 (ESR-PRE2) of the interface speed. When you request a value that is not a multiple of 1/255 or 1/65,535, the router chooses the nearest multiple.

The bandwidth percentage is based on the interface bandwidth. In a hierarchical policy, the bandwidth percentage is based on the nearest parent shape rate.

By default, a minimum bandwidth guaranteed queue has buffers for up to 50 milliseconds of 256-byte packets at line rate, but not less than 32 packets.

For Cisco IOS Release 12.0(22)S and later releases, to enable LLQ for Frame Relay (priority queueing (PQ)/CBWFQ) on the Cisco 10000 series router, first create a policy map and then assign priority to a defined traffic class using the **priority** command. For example, the following sample configuration shows how to configure a priority queue with a guaranteed bandwidth of 8000 kb/s. In the example, the Business class in the policy map named “map1” is configured as the priority queue. The map1 policy also includes the Non-Business class with a minimum bandwidth guarantee of 48 kb/s. The map1 policy is attached to serial interface 2/0/0 in the outbound direction.

```
class-map Business
  match ip precedence 3
policy-map map1
  class Business
    priority
    police 8000
  class Non-Business
    bandwidth 48
interface serial 2/0/0
  frame-relay encapsulation
  service-policy output map1
```

On the PRE2, you can use the **service-policy** command to attach a QoS policy to an ATM subinterface or to a PVC. However, on the PRE3, you can attach a QoS policy only to a PVC.

Cisco 7600 Series Routers

The **output** keyword is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

Do not attach a service policy to a port that is a member of an EtherChannel.

Although the CLI allows you to configure QoS based on policy feature cards (PFCs) on the WAN ports on the OC-12 ATM optical services modules (OSM) and on the WAN ports on the channelized OSMs, PFC-based QoS is not supported on the WAN ports on these OSMs. OSMs are not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 32.

PFC QoS supports the optional **output** keyword only on VLAN interfaces. You can attach both an input policy map and an output-policy map to a VLAN interface.

Cisco 10000 Series Routers Control Policy Maps

Activate a control policy map by applying it to a context. A control policy map can be applied to one or more of the following types of contexts, which are listed in order of precedence:

- 1 Global
- 2 Interface
- 3 Subinterface
- 4 Virtual template
- 5 VC class
- 6 PVC

In general, control policy maps that are applied to more specific contexts take precedence over policy maps applied to more general contexts. In the list, the context types are numbered in order of precedence. For example, a control policy map that is applied to a permanent virtual circuit (PVC) takes precedence over a control policy map that is applied to an interface.

Control policies apply to all sessions hosted on the context. Only one control policy map can be applied to a given context.

Abbreviated Form of the service-policy Command

In Cisco IOS Release 12.2(33)SB and later releases, the router does not accept the abbreviated form (ser) of the **service-policy** command. Instead, you must spell out the command name **service-** before the router accepts the command. For example, the following error message displays when you attempt to use the abbreviated form of the **service-policy** command:

```
interface GigabitEthernet1/1/0
  ser out ?
% Unrecognized command
  ser ?
% Unrecognized command
```

As shown in the following example, when you enter the command as **service-** followed by a space, the router parses the command as **service-policy**. Entering the question mark causes the router to display the command options for the **service-policy** command.

```
service- ?
input Assign policy-map to the input of an interface
output Assign policy-map to the output of an interface
type Configure CPL Service Policy
```

In releases prior to Cisco IOS Release 12.2(33)SB, the router accepts the abbreviated form of the **service-policy** command. For example, the router accepts the following commands:

```
interface GigabitEthernet1/1/0
  ser out test
```

Examples

The following example shows how to attach a policy map to a Fast Ethernet interface:

```
interface fastethernet 5/20
  service-policy input pmap1
```

The following example shows how to attach the service policy map named “policy9” to DLCI 100 on output serial interface 1 and enables LLQ for Frame Relay:

```
interface Serial1/0.1 point-to-point
  frame-relay interface-dlci 100
  class fragment
  map-class frame-relay fragment
  service-policy output policy9
```

The following example shows how to attach the service policy map named “policy9” to input serial interface 1:

```
interface Serial1
  service-policy input policy9
```

The following example attaches the service policy map named “policy9” to the input PVC named “cisco”:

```
pvc cisco 0/34
  service-policy input policy9
  vbr-nt 5000 3000 500
  precedence 4-7
```

The following example shows how to attach the policy named “policy9” to output serial interface 1 to specify the service policy for the interface and enable CBWFQ on it:

```
interface serial1
  service-policy output policy9
```

The following example attaches the service policy map named “policy9” to the output PVC named “cisco”:

```
pvc cisco 0/5
  service-policy output policy9
  vbr-nt 4000 2000 500
  precedence 2-3
```

Examples

The following example shows how to attach the service policy named “userpolicy” to DLCI 100 on serial subinterface 1/0/0.1 for outbound packets:

```
interface serial 1/0/0.1 point-to-point
  frame-relay interface-dlci 100
  service-policy output userpolicy
```



Note

You must be running Cisco IOS Release 12.0(22)S or a later release to attach a policy to a DLCI in this way. If you are running a release prior to Cisco IOS Release 12.0(22)S, attach the service policy as described in the previous configuration examples using the legacy Frame Relay commands, as shown in the example “how to attach the service policy map named “policy9” to DLCI 100 on output serial interface 1 and enable LLQ for Frame Relay”.

The following example shows how to attach a QoS service policy named “map2” to PVC 0/101 on the ATM subinterface 3/0/0.1 for inbound traffic:

```
interface atm 3/0/0
 atm pxf queueing
interface atm 3/0/0.1
 pvc 0/101
 service-policy input map2
```

**Note**

The **atm pxf queueing** command is not supported on the PRE3 or PRE4.

The following example shows how to attach a service policy named “myQoS” to physical Gigabit Ethernet interface 1/0/0 for inbound traffic. VLAN 4, configured on Gigabit Ethernet subinterface 1/0/0.3, inherits the service policy of physical Gigabit Ethernet interface 1/0/0.

```
interface GigabitEthernet 1/0/0
 service-policy input myQoS
interface GigabitEthernet 1/0/0.3
 encapsulation dot1q 4
```

The following example shows how to apply the policy map named “policy1” to the virtual template named “virtual-templatel” for all inbound traffic. In this example, the virtual template configuration also includes Challenge Handshake Authentication Protocol (CHAP) authentication and PPP authorization and accounting.

```
interface virtual-templatel
 ip unnumbered Loopback1
 no peer default ip address
 ppp authentication chap vpn1
 ppp authorization vpn1
 ppp accounting vpn1
 service-policy input policy1
```

The following example shows how to attach the service policy map named “voice” to ATM VC 2/0/0 within a PVC range of a total of three PVCs and enable subinterface configuration mode where a point-to-point subinterface is created for each PVC in the range. Each PVC created as part of the range has the voice service policy attached to it.

```
configure terminal
 interface atm 2/0/0
 range pvc 1/50 1/52
 service-policy input voice
```

The following example shows how to attach the service policy map named “voice” to ATM VC 2/0/0 within a PVC range, where every VC created as part of the range has the voice service policy attached to it. The exception is PVC 1/51, which is configured as an individual PVC within the range and has a different service policy named “data” attached to it in ATM PVC-in-range configuration mode.

```
configure terminal
 interface atm 2/0/0
 range pvc 1/50 1/52
 service-policy input voice
 pvc-in-range 1/51
 service-policy input data
```

The following example shows how to configure a service group named “PREMIUM-SERVICE” and apply the input policy named “PREMIUM-MARK-IN” and the output policy named “PREMIUM-OUT” to the service group:

```
policy-map type service PREMIUM-SERVICE
 service-policy input PREMIUM-MARK-IN
 service-policy output PREMIUM-OUT
```

The following example shows a policy map and interface configuration that supported simultaneous nonqueueing policies:

```
Policy-map p-map
class c-map
set mpls experimental imposition 4

interface ATM1/0/0.1 multipoint
no atm enable-ilmi-trap
xconnect 10.1.1.1 100001 encapsulation mpls
service-policy input p-map
pvc 1/41 l2transport
no epd
!
pvc 1/42 l2transport
no epd
!
pvc 1/43 l2transport
no epd
interface ATM1/0/0.101 multipoint
no atm enable-ilmi-trap
pvc 9/41 l2transport
xconnect 10.1.1.1 1001011 encapsulation mpls
service-policy input p-map
!
pvc 10/41 l2transport
xconnect 10.1.1.1 1001012 encapsulation mpls
!
```

The following example shows how to attach simultaneous nonqueueing QoS policies on an ATM subinterface and ATM PVC:

```
interface atm 1/0/0.101
pvc 9/41
service-policy input p-map
```

Related Commands

Command	Description
class-map	Accesses QoS class-map configuration mode to configure QoS class maps.
frame-relay ip rtp priority	Reserves a strict priority queue on a Frame Relay PVC for a set of RTP packet flows belonging to a range of UDP destination ports,
frame-relay traffic-shaping	Enables both traffic shaping and per-virtual-circuit queueing for all PVCs and SVCs on a Frame Relay interface.
frame-relay voice bandwidth	Specifies the amount of bandwidth to be reserved for voice traffic on a specific DLCI.
ip subscriber interface	Creates an ISG IP interface session.
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
priority	Gives priority to a class of traffic belonging to a policy map.

Command	Description
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.
traffic-shape rate	Enables traffic shaping for outbound traffic on an interface.

set cos

To set the Layer 2 class of service (CoS) value of an outgoing packet, use the **setcos** command in policy-map class configuration mode. To remove a specific CoS value setting, use the **no** form of this command.

set cos {*cos-value*|*from-field* [**table** *table-map-name*]}

no set cos {*cos-value*|*from-field* [**table** *table-map-name*]}

Cisco CMTS and 10000 Series Router

set cos *cos-value*

Syntax Description

<i>cos-value</i>	Specific IEEE 802.1Q CoS value from 0 to 7.
<i>from-field</i>	Specific packet-marking category to be used to set the CoS value of the packet. If you are using a table map for mapping and converting packet-marking values, this establishes the “map from” packet-marking category. Packet-marking category keywords are as follows: <ul style="list-style-type: none">• precedence• dscp
table	(Optional) Indicates that the values set in a specified table map will be used to set the CoS value.
<i>table-map-name</i>	(Optional) Name of the table map used to specify the CoS value. The table map name can be a maximum of 64 alphanumeric characters.

Command Default

No CoS value is set for the outgoing packet.

Command Modes

Policy-map class configuration

Command History

Release	Modification
12.1(5)T	This command was introduced.
12.2(13)T	This command was modified for Enhanced Packet Marking to allow a mapping table (table map) to be used to convert and propagate packet-marking values.

Release	Modification
12.0(16)BX	This command was implemented on the Cisco 10000 series router for the ESR-PRE2.
12.0(31)S	This command was integrated into Cisco IOS Release 12.0(31)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB and implemented on the Cisco 10000 series router.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SCF	This command was integrated into Cisco IOS Release 12.2(33)SCF.
3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

CoS packet marking is supported only in the Cisco Express Forwarding switching path.

The **setcos** command should be used by a router if a user wants to mark a packet that is being sent to a switch. Switches can leverage Layer 2 header information, including a CoS value marking.

The **setcos** command can be used only in service policies that are attached in the output direction of an interface. Packets entering an interface cannot be set with a CoS value.

The **matchcos** and **setcos** commands can be used together to allow routers and switches to interoperate and provide quality of service (QoS) based on the CoS markings.

Layer 2 to Layer 3 mapping can be configured by matching on the CoS value because switches already can match and set CoS values. If a packet that needs to be marked to differentiate user-defined QoS services is leaving a router and entering a switch, the router should set the CoS value of the packet because the switch can process the Layer 2 header.

Using This Command with the Enhanced Packet Marking Feature

You can use this command as part of the Enhanced Packet Marking feature to specify the “from-field” packet-marking category to be used for mapping and setting the CoS value. The “from-field” packet-marking categories are as follows:

- Precedence
- Differentiated services code point (DSCP)

If you specify a “from-field” category but do not specify the **table** keyword and the applicable *table-map-name* argument, the default action will be to copy the value associated with the “from-field” category as the CoS value. For instance, if you configure the **setcosprecedence** command, the precedence value will be copied and used as the CoS value.

You can do the same for the DSCP marking category. That is, you can configure the **setcosdscp** command, and the DSCP value will be copied and used as the CoS value.

**Note**

If you configure the **setcosdscp** command, only the *first three bits* (the class selector bits) of the DSCP field are used.

Examples

In the following example, the policy map called “cos-set” is created to assign different CoS values for different types of traffic. This example assumes that the class maps called “voice” and “video-data” have already been created.

```
Router(config)#  
policy-map cos-set  
Router(config-pmap)#  
class voice  
Router(config-pmap-c)#  
set cos 1  
Router(config-pmap-c)#  
exit  
Router(config-pmap)#  
class video-data  
Router(config-pmap-c)#  
set cos 2  
Router(config-pmap-c)#  
end
```

Examples

In the following example, the policy map called “policy-cos” is created to use the values defined in a table map called “table-map1”. The table map called “table-map1” was created earlier with the **table-map** (value mapping) command. For more information about the **table-map** (value mapping) command, see the **table-map**(value mapping) command page.

In this example, the setting of the CoS value is based on the precedence value defined in “table-map1”:

```
Router(config)#  
policy-map policy-cos  
Router(config-pmap)#  
class class-default  
Router(config-pmap-c)#  
set cos precedence table table-map1  
Router(config-pmap-c)#  
end
```

Examples

The following example shows how to set the class of service for the 802.1p domain:

```
Router(config)# policy-map cos7
Router(config-pmap)# class cos7
Router(config-pmap-c)# set cos 2
Router(config-pmap-c)# end
```



Note

The **setcos** command is applied when you create a service policy in QoS policy-map configuration mode and attach the service policy to an interface or ATM virtual circuit (VC). For information on attaching a service policy, 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
match cos	Matches a packet on the basis of Layer 2 CoS marking.
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 dscp	Marks a packet by setting the Layer 3 DSCP value in the ToS byte.
set precedence	Sets the precedence value in the packet header.
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 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.

set qos-group

To set a quality of service (QoS) group identifier (ID) that can be used later to classify packets, use the **set qos-group** command in policy-map class configuration mode. To remove the group ID, use the **no** form of this command.

Supported Platforms Except the Cisco 10000 Series Router

set qos-group {*group-id*|*from-field* [**table** *table-map-name*]}

no set qos-group {*group-id*|*from-field* [**table** *table-map-name*]}

Cisco 10000 Series Router

set qos-group *group-id*

no set qos-group *group-id*

Syntax Description

<i>group-id</i>	Group ID number in the range from 0 to 99.
<i>from-field</i>	<p>Specific packet-marking category to be used to set the QoS group value of the packet. If you are using a table map for mapping and converting packet-marking values, this establishes the “map from” packet-marking category. Packet-marking category keywords are as follows:</p> <ul style="list-style-type: none"> • cos --Specifies that the QoS group value is set from the packet’s original 802.1P class of service (CoS) field. • precedence --Specifies that the QoS group value is set from the packet’s original IP precedence field. • dscp --Specifies that the QoS group value is set from the packet’s original Differentiated Services Code Point (DSCP) field. • mpls exp topmost --Specifies that the QoS group value is set from the packet’s original topmost MPLS EXP field .
table <i>table-map-name</i>	(Optional) Used in conjunction with the <i>from-field</i> argument. Indicates that the values set in a table map specified by <i>table-map-name</i> will be used to set the QoS group value.

Command Default

No group ID is specified.

Command Modes

Policy-map class configuration (config-pmap-c)

Command History

Release	Modification
11.1CC	This command was introduced.
12.0(5)XE	This command was integrated into Cisco IOS Release 12.0(5)XE.
12.0(17)SL	This command was introduced on the Cisco 10000 series router.
12.2(13)T	This command can now be used with the random-detectdiscard-class-based command, and 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(18)SXE	This command was integrated into Cisco IOS 12.2(18)SXE, and the cos keyword was added.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.
Cisco IOS XE Release 2.1	This command was implemented on Cisco ASR 1000 series routers.
15.1(2)SNH	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

The **setqos-group** command allows you to associate a group ID with a packet. The group ID can be used later to classify packets into QoS groups based as prefix, autonomous system, and community string.

A QoS group and discard class are required when the input per-hop behavior (PHB) marking will be used for classifying packets on the output interface.

Using This Command with the Enhanced Packet Marking Feature

If you are using this command as part of the Enhanced Packet Marking feature, you can use this command to specify the “from-field” packet-marking category to be used for mapping and setting the precedence value.

If you specify a “from-field” category but do not specify the **table** keyword and the applicable *table-map-name* argument, the default action will be to copy the value associated with the “from-field” category as the precedence value. For instance, if you enter **setqos-groupprecedence**, the precedence value will be copied and used as the QoS group value.

A packet is marked with a QoS group value only while it is being processed within the router. The QoS group value is not included in the packet’s header when the packet is transmitted over the output interface. However, the QoS group value can be used to set the value of a Layer 2 or Layer 3 field that is included as part of the packet’s headers (such as the MPLS EXP, CoS, and DSCP fields).

**Note**

The **setqos-groupcos** and **setqos-groupprecedence** commands are equivalent to the **mlsqostrustcos** and **mlsqostrustprec** commands.

**Tip**

The **setqos-group** command cannot be applied until you create a service policy in policy-map configuration mode and then attach the service policy to an interface or ATM virtual circuit (VC). For information on attaching a service policy, refer to the “Modular Quality of Service Command-Line Interface Overview” chapter of the *Cisco IOS Quality of Service Solutions Configuration Guide*.

Examples

The following example shows how to set the QoS group to 1 for all packets that match the class map called class 1. These packets are then rate limited on the basis of the QoS group ID.

```
Router(config)#
policy-map policy1
Router(config-pmap)#
class class1
Router(config-pmap-c)#
set qos-group 1
Router(config-pmap-c)#
end
```

The following example shows how to set the QoS group value based on the packet's original 802.1P CoS value:

```
Router(config)# policy map policy1
Router(config-pmap)# class class-default
Router(config-pmap-c)#
set qos-group cos
Router(config-pmap-c)#
end
```

Examples

The following example shows how to set the QoS group value based on the values defined in a table map called table-map1. This table map is configured in a policy map called policy1. Policy map policy1 converts and propagates the QoS value according to the values defined in table-map1.

In this example, the QoS group value will be set according to the precedence value defined in table-map1.

```
Router(config)# policy map policy1
Router(config-pmap)# class class-default
Router(config-pmap-c)#
set qos-group precedence table table-map1
Router(config-pmap-c)#
end
```

Related Commands

Command	Description
match input vlan	Configures a class map to match incoming packets that have a specific VLAN ID.
match qos-group	Identifies a specified QoS group value as a match criterion.
mls qos trust	Sets the trusted state of an interface to determine which incoming QoS field on a packet, if any, should be preserved.
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.
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.

show auto discovery qos

To display the data collected during the Auto-Discovery (data collection) phase of the AutoQoS for the Enterprise feature, use the **show autodiscovery qos** command in privileged EXEC mode.

show auto discovery qos [**interface** *[type number]*]

Syntax Description

interface	(Optional) Indicates that the configurations for a specific interface type will be displayed.
<i>type number</i>	(Optional) Specifies the interface type and number.

Command Default

Displays the configurations created for all interface types.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.3(11)T	Command output was modified to include suggested policy map information.

Usage Guidelines

The suggested policy output (shown in the example below) lets you preview class maps and policy maps before you issue the **auto qos** command on an interface. You can then continue with the Auto-Discovery phase until more data is gathered or you can cut and paste the existing data and edit it as desired.

Examples

The following is sample output from the **show autodiscovery qos** command. This example displays the data collected during the Auto-Discovery (data collection) phase using DSCP classification in trusted mode and includes suggested policy map information.

```
Router# show auto discovery qos
Serial2/1.1
AutoQoS Discovery enabled for trusted DSCP
Discovery up time: 2 hours, 42 minutes
AutoQoS Class information:
Class Voice:
  Recommended Minimum Bandwidth: 118 Kbps/1% (PeakRate)
Detected DSCPs and data:
DSCP value      AverageRate      PeakRate          Total
-----      (kbps/%)      (kbps/%)          (bytes)
-----
46/ef          106/1          118/1          129510064
Class Interactive Video:
```

```

Recommended Minimum Bandwidth: 25 Kbps/<1% (AverageRate)
Detected DSCPs and data:
DSCP value      AverageRate      PeakRate      Total
                  (kbps/%)          (kbps/%)      (bytes)
-----
34/af41          25/<1            28/<1          31084292
Class Signaling:
Recommended Minimum Bandwidth: 50 Kbps/<1% (AverageRate)
Detected DSCPs and data:
DSCP value      AverageRate      PeakRate      Total
                  (kbps/%)          (kbps/%)      (bytes)
-----
24/cs3           50/<1            56/<1          61838040
Class Streaming Video:
Recommended Minimum Bandwidth: 79 Kbps/<1% (AverageRate)
Detected DSCPs and data:
DSCP value      AverageRate      PeakRate      Total
                  (kbps/%)          (kbps/%)      (bytes)
-----
32/cs4           79/<1            88/<1          96451788
Class Transactional:
Recommended Minimum Bandwidth: 105 Kbps/1% (AverageRate)
Detected DSCPs and data:
DSCP value      AverageRate      PeakRate      Total
                  (kbps/%)          (kbps/%)      (bytes)
-----
18/af21          105/1            117/1          127798678
Class Bulk:
Recommended Minimum Bandwidth: 132 Kbps/1% (AverageRate)
Detected DSCPs and data:
DSCP value      AverageRate      PeakRate      Total
                  (kbps/%)          (kbps/%)      (bytes)
-----
10/af11          132/1            147/1          160953984
Class Scavenger:
Recommended Minimum Bandwidth: 24 Kbps (AverageRate)/0% (fixed)
Detected DSCPs and data:
DSCP value      AverageRate      PeakRate      Total
                  (kbps/%)          (kbps/%)      (bytes)
-----
8/cs1            24/<1            27/<1          30141238
Class Management:
Recommended Minimum Bandwidth: 34 Kbps/<1% (AverageRate)
Detected DSCPs and data:
DSCP value      AverageRate      PeakRate      Total
                  (kbps/%)          (kbps/%)      (bytes)
-----
16/cs2           34/<1            38/<1          41419740
Class Routing:
Recommended Minimum Bandwidth: 7 Kbps/<1% (AverageRate)
Detected DSCPs and data:
DSCP value      AverageRate      PeakRate      Total
                  (kbps/%)          (kbps/%)      (bytes)
-----
48/cs6           7/<1             7/<1           8634024
Class Best Effort:
Current Bandwidth Estimation: 820 Kbps/8% (AverageRate)
Detected DSCPs and data:
DSCP value      AverageRate      PeakRate      Total
                  (kbps/%)          (kbps/%)      (bytes)
-----
0/default        820/8            915/9          997576380
Suggested AutoQoS Policy based on a discovery uptime of 2 hours, 42 minutes:
!
class-map match-any AutoQoS-Voice-Trust
  match ip dscp ef
!
class-map match-any AutoQoS-Inter-Video-Trust
  match ip dscp af41
!
class-map match-any AutoQoS-Signaling-Trust
  match ip dscp cs3
!

```

```

class-map match-any AutoQoS-Stream-Video-Trust
  match ip dscp cs4
!
class-map match-any AutoQoS-Transactional-Trust
  match ip dscp af21
  match ip dscp af22
  match ip dscp af23
!
class-map match-any AutoQoS-Bulk-Trust
  match ip dscp af11
  match ip dscp af12
  match ip dscp af13
!
class-map match-any AutoQoS-Scavenger-Trust
  match ip dscp cs1
!
class-map match-any AutoQoS-Management-Trust
  match ip dscp cs2
!
class-map match-any AutoQoS-Routing-Trust
  match ip dscp cs6
!
policy-map AutoQoS-Policy-S2/1.1Trust
  class AutoQoS-Voice-Trust
    priority percent 1
  class AutoQoS-Inter-Video-Trust
    bandwidth remaining percent 1
  class AutoQoS-Signaling-Trust
    bandwidth remaining percent 1
  class AutoQoS-Stream-Video-Trust
    bandwidth remaining percent 1
  class AutoQoS-Transactional-Trust
    bandwidth remaining percent 1
    random-detect dscp-based
  class AutoQoS-Bulk-Trust
    bandwidth remaining percent 1
    random-detect dscp-based
  class AutoQoS-Scavenger-Trust
    bandwidth remaining percent 1
  class AutoQoS-Management-Trust
    bandwidth remaining percent 1
  class AutoQoS-Routing-Trust
    bandwidth remaining percent 1
  class class-default
    fair-queue

```

The table below describes the significant fields shown in the display.

Table 9: show auto discovery qos Field Descriptions

Field	Description
Serial2/1.1	The interface or subinterface on which data is being collected.
AutoQoS Discovery enabled for trusted DSCP	Indicates that the data collection phase of AutoQoS has been enabled.
Discovery up time	Indicates the period of time in which data was collected.
AutoQoS Class information	Displays information for each AutoQoS class.

Field	Description
Class Voice	Information for the named class, along with data pertaining to the detected applications. This data includes DSCP value, average rate (in kilobits per second (kbps)), peak rate (kbps), and total packets (bytes).
Suggested AutoQoS Policy based on a discovery uptime of hours and minutes	Policy-map and class-map statistics based on a specified discovery time.

Related Commands

Command	Description
auto qos	Installs the QoS class maps and policy maps created by the AutoQoS for the Enterprise feature.
auto discovery qos	Begins discovering and collecting data for configuring the AutoQoS for the Enterprise feature.
show auto qos	Displays the interface configurations, policy maps, and class maps created by AutoQoS on a specific interface or all interfaces.

show auto qos

To display the interface configurations, policy maps, and class maps created by AutoQoS on a specific interface or all interfaces, use the **show auto qos** command in privileged EXEC mode.

show auto qos [**interface** [*type slot/ port*]]

Syntax Description

interface	(Optional) Displays the configurations created by the AutoQoS--VoIP feature on all the interfaces or PVCs on which the AutoQoS--VoIP feature is enabled. • If you configure the interface keyword but do not specify an interface type, the show auto qos interface command displays the configurations created by the AutoQoS--VoIP feature on all the interfaces or PVCs on which the AutoQoS--VoIP feature is enabled.
<i>type</i>	(Optional) Interface type; valid values are atm , ethernet , fastethernet , ge-wan , gigabitethernet , pos , and tengigabitethernet .
<i>slot / port</i>	(Optional) Slot and port number.

Command Default

If no arguments or keywords are specified, configurations created for all interface types are displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(15)T	This command was introduced as part of the AutoQoS--VoIP feature.
12.3(7)T	This command was modified for the AutoQoS for the Enterprise feature. The output was modified to display the classes, class maps, and policy maps created on the basis of the data collected during the Auto-Discovery phase of the AutoQoS for the Enterprise feature.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
15.2(1)T	This command was modified. The output does not display the Frame Relay traffic shaping configuration.

Usage Guidelines

The **showautoqosinterface** command can be used with Frame Relay data-link connection identifiers (DLCIs) and ATM PVCs.

When the AutoQoS--VoIP or the AutoQoS for the Enterprise features are enabled, configurations are generated for each interface or PVC. These configurations are then used to create the interface configurations, policy maps, class maps, and access control lists (ACLs) for use on the network. The **showautoqos** command can be used to verify the contents of the interface configurations, policy maps, class maps, and ACLs.

Catalyst 6500 Series Switches

AutoQoS is supported on the following modules:

- WS-X6548-RJ45
- WS-X6548-RJ21
- WS-X6148-GE-TX
- WS-X6548-GE-TX-CR
- WS-X6148-RJ45V
- WS-X6148-RJ21V
- WS-X6348-RJ45
- WS-X6348-RJ21
- WS-X6248-TEL

Examples

Examples

The **showautoqosinterfacetypeslot/port** command displays the configurations created by the AutoQoS--VoIP feature on the specified interface.

In the following example, the serial subinterface 6/1.1 has been specified:

```
Router# show auto qos interface serial 6/1.1
S6/1.1: DLCI 100 -
!
interface Serial6/1.1 point-to-point
 frame-relay interface-dlci 100
   class AutoQoS-VoIP-FR-Serial6/1-100
 frame-relay ip rtp header-compression
!
map-class frame-relay AutoQoS-VoIP-FR-Serial6/1-100
 frame-relay cir 512000
 frame-relay bc 5120
 frame-relay be 0
 frame-relay mincir 512000
 service-policy output AutoQoS-Policy-UnTrust
 frame-relay fragment 640
```

When the **interface** keyword is configured but an interface type is not specified, the **showautoqosinterface** command displays the configurations created by the AutoQoS--VoIP feature on all the interfaces or PVCs on which the AutoQoS--VoIP feature is enabled.

```
Router# show auto qos interface
Serial6/1.1: DLCI 100 -
!
interface Serial6/1.1 point-to-point
```

```

frame-relay interface-dlci 100
  class AutoQoS-VoIP-FR-Serial6/1-100
frame-relay ip rtp header-compression
!
map-class frame-relay AutoQoS-VoIP-FR-Serial6/1-100
frame-relay cir 512000
frame-relay bc 5120
frame-relay be 0
frame-relay mincir 512000
service-policy output AutoQoS-Policy-UnTrust
frame-relay fragment 640
ATM2/0.1: PVC 1/100 -
!
interface ATM2/0.1 point-to-point
pvc 1/100
tx-ring-limit 3
encapsulation aal5mux ppp Virtual-Template200
!
interface Virtual-Template200
bandwidth 512
ip address 10.10.107.1 255.255.255.0
service-policy output AutoQoS-Policy-UnTrust
ppp multilink
ppp multilink fragment-delay 10
ppp multilink interleave

```

The following example displays all of the configurations created by the AutoQoS--VoIP feature:

```

Router# show auto qos
Serial6/1.1: DLCI 100 -
!
interface Serial6/1.1 point-to-point
  frame-relay interface-dlci 100
    class AutoQoS-VoIP-FR-Serial6/1-100
frame-relay ip rtp header-compression
!
map-class frame-relay AutoQoS-VoIP-FR-Serial6/1-100
frame-relay cir 512000
frame-relay bc 5120
frame-relay be 0
frame-relay mincir 512000
service-policy output AutoQoS-Policy-UnTrust
frame-relay fragment 640

```

The table below describes the significant fields shown in the display.

Table 10: show auto qos Field Descriptions (AutoQoS--VoIP Feature Configured)

Field	Description
class AutoQoS-VoIP-FR-Serial6/1-100	Name of the class created by the AutoQoS-VoIP feature. In this instance, the name of the class is AutoQoS-VoIP-FR-Serial6/1-100.
service-policy output AutoQoS-Policy-UnTrust	Indicates that the policy map called “AutoQoS-Policy-UnTrust” has been attached to an interface in the outbound direction of the interface.

show auto qos interface Command: Configured for the AutoQoS for the Enterprise Feature

The following is sample output from the **showautoqos** command. This example displays the classes, class maps, and policy maps created on the basis of the data collected during the Auto-Discovery phase of the AutoQoS for the Enterprise feature.

```
Router# show auto qos
!
policy-map AutoQoS-Policy-Se2/1.1
class AutoQoS-Voice-Se2/1.1
  priority percent 70
  set dscp ef
class AutoQoS-Inter-Video-Se2/1.1
  bandwidth remaining percent 10
  set dscp af41
class AutoQoS-Stream-Video-Se2/1.1
  bandwidth remaining percent 1
  set dscp cs4
class AutoQoS-Transactional-Se2/1.1
  bandwidth remaining percent 1
  set dscp af21
class AutoQoS-Scavenger-Se2/1.1
  bandwidth remaining percent 1
  set dscp cs1
class class-default
  fair-queue
!
policy-map AutoQoS-Policy-Se2/1.1-Parent
class class-default
  shape average 1024000
  service-policy AutoQoS-Policy-Se2/1.1
!
class-map match-any AutoQoS-Stream-Video-Se2/1.1
match protocol cuseeme
!
class-map match-any AutoQoS-Transactional-Se2/1.1
match protocol sqlnet
!
class-map match-any AutoQoS-Voice-Se2/1.1
match protocol rtp audio
!
class-map match-any AutoQoS-Inter-Video-Se2/1.1
match protocol rtp video
!
rmon event 33333 log trap AutoQoS description "AutoQoS SNMP traps for Voice Drops" owner
AutoQoS
Serial2/1.1: DLCI 58 -
!
interface Serial2/1.1 point-to-point
frame-relay interface-dlci 58
  class AutoQoS-FR-Serial2/1-58
!
map-class frame-relay AutoQoS-FR-Serial2/1-58
frame-relay cir 1024000
frame-relay bc 10240
frame-relay be 0
frame-relay mincir 1024000
service-policy output AutoQoS-Policy-Se2/1.1-Parent
```

The table below describes the significant fields shown in the display.

Table 11: show auto qos Field Descriptions (AutoQoS for the Enterprise Feature Configured)

Field	Description
policy-map AutoQoS-Policy-Se2/1.1	Name of the policy map created by the AutoQoS feature. In this instance, the name of the policy map is AutoQoS-Policy-Se2/1.1.

Field	Description
class AutoQoS-Voice-Se2/1.1 priority percent 70 set dscp ef	Name of the class created by the AutoQoS feature. In this instance, the name of the class is AutoQoS-Voice-Se2/1.1. Following the class name, the specific QoS features configured for the class are displayed.
class-map match-any AutoQoS-Stream-Video-Se2/1.1 match protocol cuseeme	Name of the class map and the packet matching criteria specified.

Related Commands

Command	Description
auto discovery qos	Begins discovering and collecting data for configuring the AutoQoS for the Enterprise feature.
auto qos	Installs the QoS class maps and policy maps created by the AutoQoS for the Enterprise feature.
auto qos voip	Configures the AutoQoS--VoIP feature on an interface.
show auto discovery qos	Displays the data collected during the Auto-Discovery phase of the AutoQoS for the Enterprise feature.

show policy-map

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

show policy-map [*policy-map*]

Syntax Description

<i>policy-map</i>	(Optional) Name of the service policy map whose complete configuration is to be displayed. The name can be a maximum of 40 characters.
-------------------	----------------------------------------------------------------------------------------------------------------------------------------

Command Default

All existing policy map configurations are displayed.

Command Modes

User EXEC (>) 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 intergrated 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(4)T	This command was modified for two-rate traffic policing to display burst parameters and associated actions.
12.2(8)T	The command was modified for the Policer Enhancement--Multiple Actions feature and the Weighted Random Early Detection (WRED)--Explicit Congestion Notification (ECN) feature.
12.2(13)T	<p>The following modifications were made:</p> <ul style="list-style-type: none"> • The output was modified for the Percentage-Based Policing and Shaping feature. • This command was modified as part of the Modular QoS CLI (MQC) Unconditional Packet Discard feature. Traffic classes can now be configured to discard packets belonging to a specified class. • 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.

Release	Modification
12.2(15)T	This command was modified to support display of Frame Relay voice-adaptive traffic-shaping information.
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(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	This command was implemented on the Supervisor Engine 2 and integrated into Cisco IOS Release 12.2(17d)SXB.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB, and the command was modified to display information about Layer 2 Tunnel Protocol Version 3 (L2TPv3) tunnel marking.
12.2(31)SB2	This command was enhanced to display bandwidth-remaining ratios configured on traffic classes and ATM overhead accounting, and was implemented on the Cisco 10000 series router for the PRE3.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRC	Support for the Cisco 7600 series router was added.
12.4(15)T2	<p>This command was modified to display information about Generic Routing Encapsulation (GRE) tunnel marking.</p> <p>Note For this release, GRE-tunnel marking is supported on the Cisco MGX Route Processor Module (RPM-XF) platform <i>only</i>.</p>
12.2(33)SB	This command was modified to display information about GRE-tunnel marking, and support for the Cisco 7300 series router was added. This command's output was modified on the Cisco 10000 series router for the PRE3 and PRE4.
Cisco IOS XE 2.1	This command was integrated into Cisco IOS XE Release 2.1 and was implemented on the Cisco ASR 1000 series router.
12.4(20)T	This command was modified. Support was added for hierarchical queueing framework (HQF) using the Modular Quality of Service (QoS) Command-Line Interface (CLI) (MQC).

Usage Guidelines

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

- ECN marking information only if ECN is enabled on the interface.

- Bandwidth-remaining ratio configuration and statistical information, if configured and used to determine the amount of unused (excess) bandwidth to allocate to a class queue during periods of congestion.

Cisco 10000 Series Router

In Cisco IOS Release 12.2(33)SB, the output of the show policy-map command is slightly different from previous releases when the policy is a hierarchical policy.

For example, in Cisco IOS Release 12.2(33)SB output similar to the following displays when you specify a hierarchical policy in the show policy-map command:

```
Router# show policy-map Bronze
policy-map bronze
  class class-default
  shape average 34386000
  service-policy Child
```

In Cisco IOS Release 12.2(31)SB, output similar to the following displays when you specify a hierarchical policy in the show policy-map command:

```
Router# show policy-map Gold
policy-map Gold
  Class class-default
  Average Rate Traffic Shaping
  cir 34386000 (bps)
  service-policy Child2
```

In Cisco IOS Release 12.2(33)SB, the output from the show policy-map command displays police actions on separate lines as shown in the following sample output:

```
Router# show policy-map Premium
Policy Map Premium
  Class P1
  priority
  police percent 50 25 ms 0 ms
  conform-action transmit
  exceed-action transmit
  violate-action drop
```

In Cisco IOS Release 12.2(31)SB, the output from the show policy-map command displays police actions on one line as shown in the following sample output:

```
Router# show policy-map Premium
Policy Map Premium
  Class P2
  priority
  police percent 50 25 ms 0 ms conform-action transmit exceed-action transmit violate- action
  drop
```

Examples

This section provides sample output from typical **showpolicy-map** commands. Depending upon the interface or platform in use and the options enabled (for example, Weighted Fair Queueing [WFQ]), the output you see may vary slightly from the ones shown below.

Weighted Fair Queueing: Example

The following example displays the contents of the service policy map called pol1. In this example, WFQ is enabled.

```
Router# show policy-map pol1
Policy Map pol1
  Weighted Fair Queueing
    Class class1
      Bandwidth 937 (kbps) Max thresh 64 (packets)
    Class class2
```

```

    Bandwidth 937 (kbps)  Max thresh 64 (packets)
Class class3
    Bandwidth 937 (kbps)  Max thresh 64 (packets)
Class class4
    Bandwidth 937 (kbps)  Max thresh 64 (packets)
Class class5
    Bandwidth 937 (kbps)  Max thresh 64 (packets)
Class class6
    Bandwidth 937 (kbps)  Max thresh 64 (packets)
Class class7
    Bandwidth 937 (kbps)  Max thresh 64 (packets)
Class class8
    Bandwidth 937 (kbps)  Max thresh 64 (packets)

```

The following example displays the contents of all policy maps on the router. Again, WFQ is enabled.

```

Router# show policy-map

Policy Map poH1
  Weighted Fair Queueing
    Class class1
      Bandwidth 937 (kbps) Max thresh 64 (packets)
    Class class2
      Bandwidth 937 (kbps) Max thresh 64 (packets)
    Class class3
      Bandwidth 937 (kbps) Max thresh 64 (packets)
    Class class4
      Bandwidth 937 (kbps) Max thresh 64 (packets)
    Class class5
      Bandwidth 937 (kbps) Max thresh 64 (packets)
    Class class6
      Bandwidth 937 (kbps) Max thresh 64 (packets)
    Class class7
      Bandwidth 937 (kbps) Max thresh 64 (packets)
    Class class8
      Bandwidth 937 (kbps) Max thresh 64 (packets)
Policy Map policy2
  Weighted Fair Queueing
    Class class1
      Bandwidth 300 (kbps) Max thresh 64 (packets)
    Class class2
      Bandwidth 300 (kbps) Max thresh 64 (packets)
    Class class3
      Bandwidth 300 (kbps) Max thresh 64 (packets)
    Class class4
      Bandwidth 300 (kbps) Max thresh 64 (packets)
    Class class5
      Bandwidth 300 (kbps) Max thresh 64 (packets)
    Class class6
      Bandwidth 300 (kbps) Max thresh 64 (packets)

```

The table below describes the significant fields shown in the display.

Table 12: show policy-map Field Descriptions--Configured for WFQ

Field	Description
Policy Map	Policy map name.
Class	Class name.
Bandwidth	Amount of bandwidth in kbps allocated to class.
Max thresh	Maximum threshold in number of packets.

Frame Relay Voice-Adaptive Traffic-Shaping: Example

The following sample output for the **show-policy-map** command indicates that Frame Relay voice-adaptive traffic-shaping is configured in the class-default class in the policy map MQC-SHAPE-LLQ1 and that the deactivation timer is set to 30 seconds.

```
Router# show policy-map
Policy Map VSD1
  Class VOICE1
    Strict Priority
    Bandwidth 10 (kbps) Burst 250 (Bytes)
  Class SIGNALS1
    Bandwidth 8 (kbps) Max Threshold 64 (packets)
  Class DATA1
    Bandwidth 15 (kbps) Max Threshold 64 (packets)
Policy Map MQC-SHAPE-LLQ1
  Class class-default
    Traffic Shaping
      Average Rate Traffic Shaping
        CIR 63000 (bps) Max. Buffers Limit 1000 (Packets)
        Adapt to 8000 (bps)
        Voice Adapt Deactivation Timer 30 Sec
  service-policy VSD1
```

**Note**

In Cisco IOS Release 12.4(20)T, if an interface configured with a policy map is full of heavy traffic, the implicit policer allows the traffic as defined in the bandwidth statement of each traffic class.

The table below describes the significant fields shown in the display.

Table 13: show policy-map Field Descriptions--Configured for Frame Relay Voice-Adaptive Traffic-Shaping

Field	Description
Strict Priority	Indicates the queueing priority assigned to the traffic in this class.
Burst	Specifies the traffic burst size in bytes.
Traffic Shaping	Indicates that Traffic Shaping is enabled.
Average Rate Traffic Shaping	Indicates the type of Traffic Shaping enabled. Choices are Peak Rate Traffic Shaping or Average Rate Traffic Shaping.
CIR	Committed Information Rate (CIR) in bps.
Max. Buffers Limit	Maximum memory buffer size in packets.
Adapt to	Traffic rate when shaping is active.
Voice Adapt Deactivation Timer	Indicates that Frame Relay voice-adaptive traffic-shaping is configured, and that the deactivation timer is set to 30 seconds.
service-policy	Name of the service policy configured in the policy map "MQC-SHAPE-LLQ1".

Traffic Policing: Example

The following is sample output from the **showpolicy-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
```

The table below describes the significant fields shown in the display.

Table 14: show policy-map Field Descriptions--Configured for Traffic Policing

Field	Description
Policy Map	Name of policy map displayed.
Class	Name of the class configured in the 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.

Two-Rate Traffic Policing: Example

The following is sample output from the **showpolicy-map** command when two-rate traffic policing has been configured. As shown below, two-rate traffic policing has been configured for a class called police. In turn, the class called police has been configured in a policy map called policy1. Two-rate traffic policing has been configured 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)# interface serial3/0
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
The following sample output shows the contents of the policy map called policy1 :
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 exceeding 1 Mbps will be dropped. The burst parameters are set to 10000 bytes.

The table below describes the significant fields shown in the display.

Table 15: show policy-map 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 (bc), peak information rate (PIR), and peak burst (BE) size used for marking packets.
conform-action	Displays the action to be taken on packets conforming to a specified rate.
exceed-action	Displays the action to be taken on packets exceeding a specified rate.
violate-action	Displays the action to be taken on packets violating a specified rate.

Multiple Traffic Policing Actions: Example

The following is sample output from the **showpolicy-map** command when the Policer Enhancement--Multiple Actions feature has been configured. The following sample output from the **showpolicy-map** command displays the configuration for a service policy called police. In this service policy, traffic policing has been configured to allow multiple actions for packets marked as conforming to, exceeding, or violating the CIR or the PIR shown in the example.

```
Router# show policy-map police
  Policy Map police
    Class class-default
      police cir 1000000 bc 31250 pir 2000000 be 31250
        conform-action transmit
        exceed-action set-prec-transmit 4
        exceed-action set-frde-transmit
        violate-action set-prec-transmit 2
        violate-action set-frde-transmit
```

Packets conforming to the specified CIR (1000000 bps) are marked as conforming packets. These are transmitted unaltered.

Packets exceeding the specified CIR (but not the specified PIR, 2000000 bps) are marked as exceeding packets. For these packets, the IP Precedence level is set to 4, the discard eligibility (DE) bit is set to 1, and the packet is transmitted.

Packets exceeding the specified PIR are marked as violating packets. For these packets, the IP Precedence level is set to 2, the DE bit is set to 1, and the packet is transmitted.

**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.

The table below describes the significant fields shown in the display.

Table 16: show policy-map 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, BC, PIR, and BE used for marking packets.
conform-action	Displays the one or more actions to be taken on packets conforming to a specified rate.
exceed-action	Displays the one or more actions to be taken on packets exceeding a specified rate.
violate-action	Displays the one or more actions to be taken on packets violating a specified rate.

Explicit Congestion Notification: Example

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

```

Router# show policy-map
  Policy Map poll
    Class class-default
      Weighted Fair Queueing
        Bandwidth 70 (%)
        exponential weight 9
        explicit congestion notification
        class      min-threshold  max-threshold  mark-probability
        -----
        0          -              -              1/10
        1          -              -              1/10
        2          -              -              1/10
        3          -              -              1/10
        4          -              -              1/10
        5          -              -              1/10
        6          -              -              1/10
        7          -              -              1/10
        rsvp       -              -              1/10

```

The table below describes the significant fields shown in the display.

Table 17: show policy-map Field Descriptions--Configured for ECN

Field	Description
explicit congestion notification	Indication that Explicit Congestion Notification is enabled.
class	IP precedence value.
min-threshold	Minimum threshold. Minimum WRED threshold in number of packets.
max-threshold	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.

Modular QoS CLI (MQC) Unconditional Packet Discard: Example

The following example displays the contents of the policy map called policy1. All the packets belonging to the class called c1 are discarded.

```
Router# show policy-map
policy1
  Policy Map policy1
    Class c1
      drop
```

The table below describes the significant fields shown in the display.

Table 18: show policy-map Field Descriptions--Configured for MQC Unconditional Packet Discard

Field	Description
Policy Map	Name of the policy map being displayed.
Class	Name of the class in the policy map being displayed.
drop	Indicates that the packet discarding action for all the packets belonging to the specified class has been configured.

Percentage-Based Policing and Shaping: Example

The following example displays the contents of two service policy maps--one called policy1 and one called policy2. In policy1, traffic policing based on a CIR of 50 percent has been configured. In policy 2, traffic shaping based on an average rate of 35 percent has been configured.

```
Router# show policy-map policy1
Policy Map policy1
  class class1
    police cir percent 50
```

```
Router# show policy-map policy2
Policy Map policy2
  class class2
    shape average percent 35
```

The following example displays the contents of the service policy map called po1 :

```
Router# show policy-map po1
Policy Map po1
  Weighted Fair Queueing
    Class class1
      Bandwidth 937 (kbps) Max thresh 64 (packets)
    Class class2
      Bandwidth 937 (kbps) Max thresh 64 (packets)
    Class class3
      Bandwidth 937 (kbps) Max thresh 64 (packets)
    Class class4
      Bandwidth 937 (kbps) Max thresh 64 (packets)
```

The following example displays the contents of all policy maps on the router:

```
Router# show policy-map

Policy Map poH1
  Weighted Fair Queueing
    Class class1
      Bandwidth 937 (kbps) Max thresh 64 (packets)
    Class class2
      Bandwidth 937 (kbps) Max thresh 64 (packets)
    Class class3
      Bandwidth 937 (kbps) Max thresh 64 (packets)
    Class class4
      Bandwidth 937 (kbps) Max thresh 64 (packets)
Policy Map policy2
  Weighted Fair Queueing
    Class class1
      Bandwidth 300 (kbps) Max thresh 64 (packets)
    Class class2
      Bandwidth 300 (kbps) Max thresh 64 (packets)
    Class class3
      Bandwidth 300 (kbps) Max thresh 64 (packets)
    Class class4
      Bandwidth 300 (kbps) Max thresh 64 (packets)
```

The table below describes the significant fields shown in the display.

Table 19: show policy-map Field Descriptions--Configured for Percentage-Based Policing and Shaping

Field	Description
Policy Map	Name of policy map displayed.
Weighted Fair Queueing	Indicates that weighted fair queueing (WFQ) has been enabled.
Class	Name of class configured in policy map displayed.
Bandwidth	Bandwidth, in kbps, configured for this class.
Max threshold	Maximum threshold. Maximum WRED threshold in number of packets.

Enhanced Packet Marking: Example

The following sample output from the **showpolicy-map** command displays the configuration for policy maps called policy1 and policy2.

In policy1 , a table map called table-map-cos1 has been configured to determine the precedence based on the class of service (CoS) value. Policy map policy 1 converts and propagates the packet markings defined in the table map called table-map-cos1.

The following sample output from the **showpolicy-map** command displays the configuration for service polices called policy1 and policy2 . In policy1 , a table map called table-map1 has been configured to determine the precedence according to the CoS value. In policy2 , a table map called table-map2 has been configured to determine the CoS value according to the precedence value.

```
Router# show policy-map policy1
  Policy Map policy1
    Class class-default
      set precedence cos table table-map1
Router# show policy-map policy2
  Policy Map policy2
    Class class-default
      set cos precedence table table-map2
```

The table below describes the fields shown in the display.

Table 20: show policy-map Field Descriptions--Configured for Enhanced Packet Marking

Field	Description
Policy Map	Name of the policy map being displayed.
Class	Name of the class in the policy map being displayed.
set precedence cos table table-map1 or set cos precedence table table-map2	<p>Name of the set command used to set the specified value.</p> <p>For instance, set precedence cos table-map1 indicates that a table map called table-map1 has been configured to set the precedence value on the basis of the values defined in the table map.</p> <p>Alternately, set cos table table-map2 indicates that a table map called table-map2 has been configured to set the CoS value on the basis of the values defined in the table map.</p>

Bandwidth-Remaining Ratio: Example

The following sample output for the show policy-map command indicates that the class-default class of the policy map named vlan10_policy has a bandwidth-remaining ratio of 10. When congestion occurs, the scheduler allocates class-default traffic 10 times the unused bandwidth allocated in relation to other subinterfaces.

```
Router# show policy-map vlan10_policy
  Policy Map vlan10_policy
    Class class-default
      Average Rate Traffic Shaping
        cir 1000000 (bps)
        bandwidth remaining ratio 10
        service-policy child_policy
```

The table below describes the fields shown in the display.

Table 21: show policy-map Field Descriptions--Configured for Bandwidth-Remaining Ratio

Field	Description
Policy Map	Name of the policy map being displayed.
Class	Name of the class in the policy map being displayed.
Average Rate Traffic Shaping	Indicates that Average Rate Traffic Shaping is configured.
cir	Committed information rate (CIR) used to shape traffic.
bandwidth remaining ratio	Indicates the ratio used to allocate excess bandwidth.

ATM Overhead Accounting: Example

The following sample output for the show policy-map command indicates that ATM overhead accounting is enabled for the class-default class. The BRAS-DSLAM encapsulation is dot1q and the subscriber encapsulation is snap-rbe for the AAL5 service.

```
Policy Map unit-test
Class class-default
Average Rate Traffic Shaping
cir 10% account dot1q aal5 snap-rbe
```

The table below describes the significant fields shown in the display.

Table 22: show policy-map Field Descriptions--Configured for ATM Overhead Accounting

Field	Description
Average Rate	Committed burst (Bc) is the maximum number of bits sent out in each interval.
cir 10%	Committed information rate (CIR) is 10 percent of the available interface bandwidth.
dot1q	BRAS-DSLAM encapsulation is 802.1Q VLAN.
aal5	DSLAM-CPE encapsulation type is based on the ATM Adaptation Layer 5 service. AAL5 supports connection-oriented variable bit rate (VBR) services.
snap-rbe	Subscriber encapsulation type.

Tunnel-Marking: Example

In this sample output of the **show policy-map** command, the character string “ip precedence tunnel 4” indicates that tunnel marking (either L2TPv3 or GRE) has been configured to set the IP precedence value to 4 in the header of a tunneled packet.

**Note**

In Cisco IOS Release 12.4(15)T2, GRE-tunnel marking is supported on the RPM-XF platform *only*.

```
Router# show policy-map
Policy Map TUNNEL_MARKING
  Class MATCH_FRDE
    set ip precedence tunnel 4
```

The table below describes the fields shown in the display.

Table 23: show policy-map Field Descriptions--Configured for Tunnel Marking

Field	Description
Policy Map	Name of the policy map being displayed.
Class	Name of the class in the policy map being displayed.
set ip precedence tunnel	Indicates that tunnel marking has been configured.

HQF: Example 1

The following sample output from the **showpolicy-map** command displays the configuration for a policy map called test1:

```
Router# show policy-map test1
Policy Map test1
  Class class-default
    Average Rate Traffic Shaping
      cir 1536000 (bps)
    service-policy test2
```

The table below describes the fields shown in the display.

Table 24: show policy-map Field Descriptions--Configured for HQF

Field	Description
Policy Map	Name of the policy map being displayed.
Class	Name of the class in the policy map being displayed.
Average Rate Traffic Shaping	Indicates that Average Rate Traffic Shaping is configured.
cir	Committed information rate (CIR) in bps.
service-policy	Name of the service policy configured in policy map "test1".

HQF: Example 2

The following sample output from the **show policy-map** command displays the configuration for a policy map called test2:

```
Router# show policy-map test2
Policy Map test2
  Class RT
    priority 20 (%)
  Class BH
    bandwidth 40 (%)
    queue-limit 128 packets
  Class BL
    bandwidth 35 (%)
    packet-based wred, exponential weight 9

  dscp      min-threshold  max-threshold  mark-probability
  -----
  af21 (18)    100             400             1/10
  default (0)   -               -               1/10
```

The table below describes the fields shown in the display.

Table 25: show policy-map Field Descriptions--Configured for HQF

Field	Description
Policy Map	Name of the policy map being displayed.
Class	Name of the class in the policy map being displayed.
Average Rate Traffic Shaping	Indicates that Average Rate Traffic Shaping is configured.
priority	Indicates the queueing priority percentage assigned to traffic in this class.
bandwidth	Indicates the bandwidth percentage allocated to traffic in this class.
queue-limit	Indicates the queue limit in packets for this traffic class.
packet-based wred, exponential weight	Indicates that random detect is being applied and the units used are packets. Exponential weight is a factor for calculating the average queue size used with WRED.

Field	Description
dscp	Differentiated services code point (DSCP). Values can be the following: <ul style="list-style-type: none"> • 0 to 63--Numerical DSCP values. The default value is 0. • af1 to af43--Assured forwarding (AF) DSCP values. • cs1 to cs7--Type of service (ToS) precedence values. • default--Default DSCP value. • ef--Expedited forwarding (EF) DSCP values.
min-threshold	Minimum threshold. Minimum WRED threshold in number of packets.
max-threshold	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.

Related Commands

Command	Description
bandwidth	Specifies or modifies the bandwidth allocated for a class belonging to a policy map, and enables ATM overhead accounting.
bandwidth remaining ratio	Specifies a bandwidth-remaining ratio for class queues and subinterface-level queues to determine the amount of unused (excess) bandwidth to allocate to the queue during congestion.
class (policy map)	Specifies the name of the class whose policy you want to create or change, and the default class (commonly known as the class-default class) before you configure its policy.
class-map	Creates a class map to be used for matching packets to a specified class.
drop	Configures a traffic class to discard packets belonging to a specific class.
police	Configures traffic policing.

Command	Description
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	Shapes traffic to the indicated bit rate according to the algorithm specified, and enables ATM overhead accounting.
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 running-config	Displays the current configuration of the router. If configured, the command output includes information about ATM overhead accounting.
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.

show policy-map class

To display the configuration for the specified class of the specified policy map, use the **showpolicy-mapclass** command in EXEC mode.

show policy-map *policy-map* **class** *class-name*

Syntax Description

<i>policy-map</i>	The name of a policy map that contains the class configuration to be displayed.
<i>class-name</i>	The name of the class whose configuration is to be 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(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.1	This command was implemented on Cisco ASR 1000 series routers.

Usage Guidelines

You can use the **showpolicy-mapclass** command to display any single class configuration for any service policy map, whether or not the specified service policy map has been attached to an interface.

Examples

The following example displays configurations for the class called class7 that belongs to the policy map called pol:

```
Router# show policy-map pol class class7
```

```
Class class7  
Bandwidth 937 (kbps) Max Thresh 64 (packets)
```

Related Commands

Command	Description
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.

show policy-map interface

To display the statistics and the configurations of the input and output policies that are attached to an interface, use the **show policy-map interface** command in user EXEC or privileged EXEC mode.

ATM Shared Port Adapters

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

Cisco CMTS Routers

show policy-map interface *interface-type slot/subslot/port*

Cisco 3660, 3845, 7200, 7400, 7500, Cisco ASR 903 Series Routers, and Cisco ASR 1000 Series Routers

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

Cisco 6500 Series Switches

show policy-map interface [*interface-type interface-number| vlan vlan-id*] [*detailed*] [{*input| output*} [*class class-name*]]

show policy-map interface [*port-channel channel-number*] [*class class-name*]]

Cisco 7600 Series Routers

show policy-map interface [*interface-type interface-number| null 0| vlan vlan-id*] [*input| output*]

Syntax Description

<i>slot</i>	(CMTS and ATM shared port adapter only) Chassis slot number. See the appropriate hardware manual for slot information. For SIPs, see 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>	(CMTS and ATM shared port adapter only) Secondary slot number on an SPA interface processor (SIP) where a SPA is installed. See the platform-specific SPA hardware installation guide and the corresponding “Specifying the Interface Address on an SPA” topic in the platform-specific SPA software configuration guide for subslot information.

<i>port</i>	(CMTS and ATM shared port adapter only) Port or interface number. See the appropriate hardware manual for port information. For SPAs, see 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.
<i>type</i>	Type of interface or subinterface whose policy configuration is to be displayed.
<i>type-parameter</i>	Port, connector, interface card number, class-map name or other parameter associated with the interface or subinterface type.
vc	(Optional) For ATM interfaces only, shows the policy configuration for a specified PVC.
<i>vpi /</i>	(Optional) ATM network virtual path identifier (VPI) for this permanent virtual circuit (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. The absence of both the forward slash (/) and a <i>vpi</i> value defaults the <i>vpi</i> value to 0. If this value is omitted, information for all virtual circuits (VCs) on the specified ATM interface or subinterface is displayed.
<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 atmvc-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 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.
class <i>class-name</i>	(Optional) Displays the QoS policy actions for the specified class.
<i>interface-type</i>	(Optional) Interface type; possible valid values are atm , ethernet , fastethernet , ge-wan gigabitethernet , pos , pseudowire and tengigabitethernet .
<i>interface-number</i>	(Optional) Module and port number; see the “Usage Guidelines” section for valid values.
vlan <i>vlan-id</i>	(Optional) Specifies the VLAN ID; valid values are from 1 to 4094.
detailed	(Optional) Displays additional statistics.
port-channel <i>channel-number</i>	(Optional) Displays the EtherChannel port-channel interface.
null 0	(Optional) Specifies the null interface; the only valid value is 0.

Command Default

This command displays the packet statistics of all classes that are configured for all service policies on the specified interface or subinterface or on a specific permanent virtual circuit (PVC) on the interface.

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

Command Modes

Privileged EXEC (#)

ATM Shared Port Adapter

User EXEC (>)

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.
12.0(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.
12.1(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 and can display burst parameters and associated actions.
12.2(8)T	<p>This 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>

Release	Modification
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(14)SX	This command was modified. Support for this command was introduced on Cisco 7600 series routers.
12.2(15)T	This command was modified to display Frame Relay voice-adaptive traffic-shaping information.
12.2(17d)SXB	This command was implemented on the Supervisor Engine 2 and integrated into Cisco IOS Release 12.2(17d)SXB.
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	This command was modified. The typeaccess-control keywords were added to support flexible packet matching.
12.2(28)SB	<p>This command was integrated into Cisco IOS Release 12.2(28)SB, and the following modifications were made:</p> <ul style="list-style-type: none"> • This command was modified to display either legacy (undistributed processing) QoS or hierarchical queueing framework (HQF) parameters on Frame Relay interfaces or PVCs. • This command was modified to display information about Layer 2 Tunnel Protocol Version 3 (L2TPv3) tunnel marking.

Release	Modification
12.2(31)SB2	<p>The following modifications were made:</p> <ul style="list-style-type: none"> • This command was enhanced to display statistical information for each level of priority service configured and information about bandwidth-remaining ratios, and this command was implemented on the Cisco 10000 series router for the PRE3. • This command was modified to display statistics for matching packets on the basis of VLAN identification numbers. As of Cisco IOS Release 12.2(31)SB2, matching packets on the basis of VLAN identification numbers is supported on Cisco 10000 series routers only.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.4(15)T2	<p>This command was modified to display information about Generic Routing Encapsulation (GRE) tunnel marking.</p> <p>Note As of this release, GRE-tunnel marking is supported on the Cisco MGX Route Processor Module (RPM-XF) platform <i>only</i>.</p>
12.2(33)SB	This command was modified to display information about GRE-tunnel marking, and support for the Cisco 7300 series router was added.
Cisco IOS XE 2.1	This command was integrated into Cisco IOS XE Release 2.1 and was implemented on the Cisco ASR 1000 series router.
12.4(20)T	This command was modified. Support was added for hierarchical queueing framework (HQF) using the Modular Quality of Service (QoS) Command-Line Interface (CLI) (MQC).
12.2(33)SXI	This command was implemented on the Catalyst 6500 series switch and modified to display the strict level in the priority feature and the counts per level.
12.2(33)SRE	This command was modified to automatically round off the bc and be values, in the MQC police policy map, to the interface's MTU size.
Cisco IOS XE Release 2.6	The command output was modified to display information about subscriber QoS statistics.
12.2(54)SG	This command was modified to display only the applicable count of policer statistics.
12.2(33)SCF	This command was integrated into Cisco IOS Release 12.2(33)SCF.
Cisco IOS XE Release 3.7S	This command was implemented on Cisco ASR 903 Series Routers.
Cisco IOS XE Release 3.8S	This command was modified. The <i>pseudowire</i> interface type was added.

Release	Modification
Cisco IOS XE Release 3.8S	This command was modified. The <i>pseudowire</i> interface type was added on Cisco 1000 Series Routers.
Cisco IOS Release 15.3(1)S	This command was modified. The <i>pseudowire</i> interface type was added.

Usage Guidelines

Cisco 3660, 3845, 7200, 7400, 7500, Cisco ASR 903 Series Routers, and Cisco ASR 1000 Series Routers

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.

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.

In HQF images for Cisco IOS Releases 12.4(20)T and later, the packets delayed and the bytes delayed counters were removed for traffic shaping classes.

Cisco 7600 Series Routers and Catalyst 6500 Series Switches

The pos, atm, and ge-wan interfaces are not supported on Cisco 7600 series routers or Catalyst 6500 series switches that are configured with a Supervisor Engine 720

Cisco 7600 series routers and Catalyst 6500 series switches that are configured with a Supervisor Engine 2 display packet counters.

Cisco 7600 series routers and Catalyst 6500 series switches that are configured with a Supervisor Engine 720 display byte counters.

The output does not display policed-counter information; 0 is displayed in its place (for example, 0 packets, 0 bytes). To display dropped and forwarded policed-counter information, enter the **show mls qos** command.

On the Cisco 7600 series router, for OSM WAN interfaces only, if you configure policing within a policy map, the hardware counters are displayed and the class-default counters are not displayed. If you do not configure policing within a policy map, the class-default counters are displayed.

On the Catalyst 6500 series switch, the **show policy-map interface** command displays the strict level in the priority feature and the counts per level.

The *interface-number* argument designates the module and port number. Valid values for *interface-number* depend on the specified interface type and the chassis and module that are used. For example, if you specify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the module number are from 1 to 13 and valid values for the port number are from 1 to 48.

HQF

When you configure HQF, the **show policy-map interface** command displays additional fields that include the differentiated services code point (DSCP) value, WRED statistics in bytes, transmitted packets by WRED, and a counter that displays packets output/bytes output in each class.

Examples

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

Examples

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 the table below 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 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

```

Examples

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 the table below for an explanation of the significant fields that commonly appear in the command output.



Note

In HQF images for Cisco IOS Releases 12.4(20)T and later, the packets delayed and bytes delayed counters were removed for traffic shaping classes.

```

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

```

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

Table 26: show policy-map interface Field Descriptions

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.

Field	Description
packets and bytes	Number of packets (also shown in bytes) identified as belonging to the class of traffic being displayed.
offered rate	<p>Rate, in kbps, of packets coming in to the class.</p> <p>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.</p>
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.
<p>Note In distributed architecture platforms (such as the Cisco 7500 series platform), 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.</p>	
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 that are available, see the “Classifying Network Traffic” module in the <i>Cisco IOS Quality of Service Solutions Configuration Guide</i> .
Fields Associated with Queueing (if Enabled)	

Field	Description
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.
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	<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>

Field	Description
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).
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.

Field	Description
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.

Examples

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 classthrough Mark Prob statistics are aggregated by subclasses. See the table below 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)# exit
Router(config-pmap)# exit
Router(config)# interface ATM4/1/0.10 point-to-point
Router(config-if)# ip address 10.0.0.2 255.255.255.0
Router(config-if)# pvc 10/110
Router(config-if)# service-policy output prec-aggr-wred

Router# show policy-map interface atm4/1/0.10

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/bytes pkts/bytes pkts/bytes thresh thresh prob
    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
```

Examples

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 the table below 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-pmap-c)# exit
Router(config-pmap)# exit
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 atm4/1/0.11

```

```

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/bytes pkts/bytes pkts/bytes thresh thresh prob
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

```

The table below describes the significant fields shown in the display when aggregate WRED is configured for an ATM shared port adapter.

Table 27: 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.

Field	Description
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.

Examples

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.



Note

In HQF images for Cisco IOS Releases 12.4(20)T and later, the packets delayed and bytes delayed counters were removed for traffic shaping classes.

```
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

```

The table below describes the significant fields shown in the display. Significant fields that are not described in the table below are described in the table above (for “show policy-map interface Field Descriptions”).

Table 28: 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.

Examples

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.

The table below describes the significant fields shown in the display.

Table 29: 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.

Examples

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.

The table below describes the significant fields shown in the display.

Table 30: 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.

Examples

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

```

The table below describes the significant fields shown in the display.

Table 31: 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>

Field	Description
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.
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.

Examples

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
```

The table below describes the significant fields shown in the display.

Table 32: show policy-map interface Field Descriptions—Configured for Class-Based RTP and TCP Header Compression

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	<p>Rate, in kbps, of packets coming in to the class.</p> <p>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.</p>
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.

Field	Description
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.

**Note**

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.

Examples

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
```

The table below describes the significant fields shown in the display.

Table 33: show policy-map interface Field Descriptions—Configured for MQC Unconditional Packet Discard

Field	Description
Service-policy output	Name of the output service policy applied to the specified interface or VC.

Field	Description
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	<p>Rate, in kbps, of packets coming in to the class.</p> <p>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.</p>
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 Cisco 7500), 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.

Field	Description
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 that are available, see the “Classifying Network Traffic” module 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.

**Note**

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.

Examples

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

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
```

The table below describes the significant fields shown in the display. 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.

Table 34: show policy-map interface Field Descriptions—Configured for Percentage-Based Policing and Shaping.

Field	Description
Service-policy output	Name of the output service policy applied to the specified interface or VC.

Field	Description
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	<p>Rate, in kbps, of packets coming in to the class.</p> <p>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.</p>
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.

Examples

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.

**Note**

In HQF images for Cisco IOS Releases 12.4(20)T and later, the packets delayed and bytes delayed counters were removed for traffic shaping classes.

```
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 Rate	Byte Limit	Sustain bits/int	Excess bits/int	Interval (ms)	Increment (bytes)	Adapt 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	

The table below describes the significant fields shown in the display. 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.

Table 35: show policy-map interface Field Descriptions—Configured for Percentage-Based Policing and Shaping (with Traffic Shaping Enabled).

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.

Field	Description
offered rate	<p>Rate, in kbps, of packets coming in to the class.</p> <p>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.</p>
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 that are available, see the “Classifying Network Traffic” module in the <i>Quality of Service Solutions Configuration Guide</i> .
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.
Byte Limit	<p>Maximum number of bytes that can be transmitted per interval. Calculated as follows:</p> $((Bc+Be) / 8) \times 1$
Sustain bits/int	Committed burst (Bc) rate.
Excess bits/int	Excess burst (Be) rate.

Field	Description
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. Note In Cisco IOS Release 12.4(20)T, this counter was removed.
Bytes Delayed	Total number of bytes delayed in the queue of the traffic shaper before being transmitted. Note In Cisco IOS Release 12.4(20)T, this counter was removed.
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.

Examples

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
```

The table below describes the significant fields shown in the display. 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.

Table 36: show policy-map interface Field Descriptions—Configured for Packet Classification Based on Layer 3 Packet Length.

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	<p>Rate, in kbps, of packets coming in to the class.</p> <p>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.</p>
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.

Examples

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
```

The table below describes the fields shown in the display. 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.

Table 37: show policy-map interface Field Descriptions—Configured for Enhanced Packet Marking.

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 that are available, see the “Classifying Network Traffic” module in the <i>Quality of Service Solutions Configuration Guide</i> .
QoS Set	Indicates that QoS group (set) has been configured for the particular class.

Field	Description
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.

Examples

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.

Examples

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:

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

Examples

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.

Examples

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:

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

Examples

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:

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

The table below describes the significant fields shown in the display.

Table 38: show policy-map interface Field Descriptions

Field	Description
Service-policy output	Name of the output service policy applied to the specified interface or VC.

Field	Description
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 that are available, see the “Classifying Network Traffic” module in the <i>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.

Examples

The following sample output from the **show policy-map interface** command displays statistics for the Fast Ethernet 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

```

Examples

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.



Note

In HQF images for Cisco IOS Releases 12.4(20)T and later, the packets delayed and bytes delayed counters were removed for traffic shaping classes.

```

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

```

Examples

**Note**

As of Cisco IOS Release 12.2(31)SB2, matching packets on the basis of VLAN ID numbers is supported on the Catalyst 1000 platform only.

The following is a sample configuration in which packets are matched and classified on the basis of the VLAN ID number. In this sample configuration, packets that match VLAN ID number 150 are placed in a class called “class1.”

```
Router# show class-map
```

```
Class Map match-all class1 (id 3)
Match vlan 150
```

Class1 is then configured as part of the policy map called “policy1.” The policy map is attached to Fast Ethernet subinterface 0/0.1.

The following sample output of the **show policy-map interface** command displays the packet statistics for the policy maps attached to Fast Ethernet subinterface 0/0.1. It displays the statistics for policy1, in which class1 has been configured.

```
Router# show policy-map interface
```

```
FastEthernet0/0.1
! Policy-map name.
Service-policy input: policy1
! Class configured in the policy map.
Class-map: class1 (match-all)
0 packets, 0 bytes
5 minute offered rate 0 bps, drop rate 0 bps
! VLAN ID 150 is the match criterion for the class.
Match: vlan 150
police:
cir 8000000 bps, bc 512000000 bytes
conformed 0 packets, 0 bytes; actions:
transmit
exceeded 0 packets, 0 bytes; actions:
drop
conformed 0 bps, exceed 0 bps
Class-map: class-default (match-any)
10 packets, 1140 bytes
5 minute offered rate 0 bps, drop rate 0 bps
Match: any
10 packets, 1140 bytes
5 minute rate 0 bps
```

The table below describes the significant fields shown in the display. 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.

Table 39: show policy-map interface Field Descriptions—Packets Matched on the Basis of VLAN ID Number.

Field	Description
Service-policy input	Name of the input service policy applied to the specified interface or VC.

Field	Description
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 VLAN ID number, 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 that are available, see the “Classifying Network Traffic” module in the <i>Cisco IOS Quality of Service Solutions Configuration Guide</i> .

Examples

The following example shows how to display the statistics and the configurations of all the input and output policies that are attached to an interface on a Cisco 7600 series router:

```
Router# show policy-map interface

FastEthernet5/36
  service-policy input: max-pol-ipp5
    class-map: ipp5 (match-all)
      0 packets, 0 bytes
      5 minute rate 0 bps
      match: ip precedence 5
    class ipp5
      police 2000000000 2000000 conform-action set-prec-transmit 6 exceed-action p
policed-dscp-transmit
```

The following example shows how to display the input-policy statistics and the configurations for a specific interface on a Cisco 7600 series router:

```
Router# show policy-map interface fastethernet 5/36 input

FastEthernet5/36
  service-policy input: max-pol-ipp5
    class-map: ipp5 (match-all)
      0 packets, 0 bytes
      5 minute rate 0 bps
      match: ip precedence 5
    class ipp5
      police 2000000000 2000000 conform-action set-prec-transmit 6 exceed-action p
policed-dscp-transmit
```

The table below describes the significant fields shown in the display.

Table 40: show policy-map interface Field Descriptions—Cisco 7600 Series Routers

Field	Description
service-policy input	Name of the input service policy applied to the specified interface.
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.
minute 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 VLAN ID number, 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 that are available, see the “Classifying Network Traffic” module in the <i>Cisco IOS Quality of Service Solutions Configuration Guide</i> .
class	Precedence value.
police	Indicates that the police command has been configured to enable traffic policing.

Examples

The following example shows the automatic rounding-off of the **bc** and **be** values, in the MQC police policy-map, to the interface’s MTU size in a Cisco 7200 series router. The rounding-off is done only when the bc and be values are lesser than the interface’s MTU size.

```
Router# show policy-map interface

Service-policy output: p2
Service-policy output: p2
  Class-map: class-default (match-any)
    2 packets, 106 bytes
    30 second offered rate 0000 bps, drop rate 0000 bps
  Match: any
    2 packets, 106 bytes
    30 second rate 0 bps
  police:
    cir 10000 bps, bc 4470 bytes
    pir 20000 bps, be 4470 bytes
    conformed 0 packets, 0 bytes; actions:
```



```

        transmit
exceeded 0 packets, 0 bytes; actions:
  drop
violated 0 packets, 0 bytes; actions:
  drop
conformed 0000 bps, exceed 0000 bps, violate 0000 bps

```

Examples

The following sample output from the show policy-map interface command shows the types of statistical information that displays when multiple priority queues are configured. Depending upon the interface in use and the options enabled, the output that you see may vary slightly from the output shown below.

```

Router# show policy-map interface

Serial2/1/0
Service-policy output: P1
Queue statistics for all priority classes:
.
.
.
Class-map: Gold (match-all)
0 packets, 0 bytes /*Updated for each priority level configured.*/
5 minute offered rate 0 bps, drop rate 0 bps
Match: ip precedence 2
Priority: 0 kbps, burst bytes 1500, b/w exceed drops: 0
Priority Level 4:
0 packets, 0 bytes

```

Examples

The following sample output from the show policy-map interface command indicates that bandwidth-remaining ratios are configured for class queues. As shown in the example, the classes precedence_0, precedence_1, and precedence_2 have bandwidth-remaining ratios of 20, 40, and 60, respectively.

```

Router# show policy-map interface GigabitEthernet1/0/0.10

Service-policy output: vlan10_policy
Class-map: class-default (match-any)
 0 packets, 0 bytes
 30 second offered rate 0 bps, drop rate 0 bps
Match: any
 0 packets, 0 bytes
 30 second rate 0 bps
Queueing
queue limit 250 packets
(queue depth/total drops/no-buffer drops) 0/0/0
(pkts output/bytes output) 0/0
shape (average) cir 1000000, bc 4000, be 4000
target shape rate 1000000
bandwidth remaining ratio 10
Service-policy : child_policy
  Class-map: precedence_0 (match-all)
    0 packets, 0 bytes
    30 second offered rate 0 bps, drop rate 0 bps
    Match: ip precedence 0
    Queueing
    queue limit 62 packets
    (queue depth/total drops/no-buffer drops) 0/0/0
    (pkts output/bytes output) 0/0
    shape (average) cir 500000, bc 2000, be 2000
    target shape rate 500000
    bandwidth remaining ratio 20
  Class-map: precedence_1 (match-all)
    0 packets, 0 bytes
    30 second offered rate 0 bps, drop rate 0 bps
    Match: ip precedence 1
    Queueing
    queue limit 62 packets
    (queue depth/total drops/no-buffer drops) 0/0/0

```

```

(pkts output/bytes output) 0/0
shape (average) cir 500000, bc 2000, be 2000
target shape rate 500000
bandwidth remaining ratio 40
Class-map: precedence_2 (match-all)
  0 packets, 0 bytes
  30 second offered rate 0 bps, drop rate 0 bps
  Match: ip precedence 2
  Queueing
    queue limit 62 packets
    (queue depth/total drops/no-buffer drops) 0/0/0
    (pkts output/bytes output) 0/0
    shape (average) cir 500000, bc 2000, be 2000
    target shape rate 500000
    bandwidth remaining ratio 60
Class-map: class-default (match-any)
  0 packets, 0 bytes
  30 second offered rate 0 bps, drop rate 0 bps
  Match: any
    0 packets, 0 bytes
    30 second rate 0 bps

queue limit 62 packets
(queue depth/total drops/no-buffer drops) 0/0/0
(pkts output/bytes output) 0/0

```

The table below describes the significant fields shown in the display.

Table 41: show policy-map interface Field Descriptions—Configured for Bandwidth-Remaining Ratios

Field	Description
Service-policy output	Name of the output service policy applied to the specified interface.
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.
bandwidth remaining ratio	Indicates the ratio used to allocate excess bandwidth.

Examples

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

Router# **show policy-map interface**

```

Serial0
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 table below describes the significant fields shown in the display.

Table 42: show policy-map interface Field Descriptions—Configured for Tunnel Marking

Field	Description
service-policy input	Name of the input service policy applied to the specified interface.
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 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. In this example, the Frame Relay Discard Eligible (DE) bit has been specified as the match criterion. For more information about the variety of match criteria that are available, see the “Classifying Network Traffic” module in the <i>Cisco IOS Quality of Service Solutions Configuration Guide</i> .
ip dscp tunnel	Indicates that tunnel marking has been configured to set the DSCP in the header of a tunneled packet to a value of 3.

Examples

The following output from the show policy-map interface command indicates that ATM overhead accounting is enabled for shaping and disabled for bandwidth:

```

Router# show policy-map interface
Service-policy output:unit-test

```

```

Class-map: class-default (match-any)
100 packets, 1000 bytes
30 second offered rate 800 bps, drop rate 0 bps
Match: any
shape (average) cir 154400, bc 7720, be 7720
target shape rate 154400
overhead accounting: enabled
bandwidth 30% (463 kbps)
overhead accounting: disabled
queue limit 64 packets
(queue depth/total drops/no-buffer drops) 0/0/0
(packets output/bytes output) 100/1000

```

The table below describes the significant fields shown in the display.

Table 43: show policy-map interface Field Descriptions—Configured for Traffic Shaping Overhead Accounting for ATM

Field	Description
service-policy output	Name of the output service policy applied to the specified interface.
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 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. In this example, the Frame Relay Discard Eligible (DE) bit has been specified as the match criterion. For more information about the variety of match criteria that are available, see the “Classifying Network Traffic” module in the <i>Cisco IOS Quality of Service Solutions Configuration Guide</i> .
target shape rate	Indicates that traffic shaping is enabled at the specified rate.
overhead accounting	Indicates whether overhead accounting is enabled or disabled for traffic shaping.
bandwidth	Indicates the percentage of bandwidth allocated for traffic queueing.

Field	Description
overhead accounting:	Indicates whether overhead accounting is enabled or disabled for traffic queueing.

Examples

The following output from the show policy-map interface command displays the configuration for Fast Ethernet interface 0/0:



Note

In HQF images for Cisco IOS Releases 12.4(20)T and later releases, the packets delayed and bytes delayed counters were removed for traffic shaping classes.

```
Router# show policy-map interface FastEthernet0/0
FastEthernet0/0

Service-policy output: test1

Class-map: class-default (match-any)
  129 packets, 12562 bytes
  30 second offered rate 0 bps, drop rate 0 bps
  Match: any
  Queueing
    queue limit 64 packets
    (queue depth/total drops/no-buffer drops) 0/0/0
    (pkts output/bytes output) 129/12562
  shape (average) cir 1536000, bc 6144, be 6144
  target shape rate 1536000

Service-policy : test2

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: RT (match-all)
  0 packets, 0 bytes
  30 second offered rate 0 bps, drop rate 0 bps
  Match: ip dscp ef (46)
  Priority: 20% (307 kbps), burst bytes 7650, b/w exceed drops: 0

Class-map: BH (match-all)
  0 packets, 0 bytes
  30 second offered rate 0 bps, drop rate 0 bps
  Match: ip dscp af41 (34)
  Queueing
    queue limit 128 packets
    (queue depth/total drops/no-buffer drops) 0/0/0
    (pkts output/bytes output) 0/0
  bandwidth 40% (614 kbps)

Class-map: BL (match-all)
  0 packets, 0 bytes
  30 second offered rate 0 bps, drop rate 0 bps
  Match: ip dscp af21 (18)
  Queueing
    queue limit 64 packets
    (queue depth/total drops/no-buffer drops) 0/0/0
    (pkts output/bytes output) 0/0
  bandwidth 35% (537 kbps)
  Exp-weight-constant: 9 (1/512)
```

```

Mean queue depth: 0 packets
dscp      Transmitted   Random drop   Tail drop   Minimum   Maximum   Mark
          pkts/bytes    pkts/bytes    pkts/bytes  thresh    thresh    prob

af21      0/0          0/0          0/0         100       400       1/10

Class-map: class-default (match-any)
  129 packets, 12562 bytes
  30 second offered rate 0 bps, drop rate 0 bps
  Match: any

  queue limit 64 packets
    (queue depth/total drops/no-buffer drops) 0/0/0
    (pkts output/bytes output) 129/12562

```

The table below describes the significant fields shown in the display.

Table 44: show policy-map interface Field Descriptions—Configured for HQF

Field	Description
FastEthernet	Name of the interface.
service-policy output	Name of the output service policy applied to the specified interface.
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 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. Note For more information about the variety of match criteria that are available, see the “Classifying Network Traffic” module in the <i>Cisco IOS Quality of Service Solutions Configuration Guide</i> .
Queueing	Indicates that queueing is enabled.
queue limit	Maximum number of packets that a queue can hold for a class policy configured in a policy map.

Field	Description
bandwidth	Indicates the percentage of bandwidth allocated for traffic queueing.
dscp	<p>Differentiated services code point (DSCP). Values can be the following:</p> <ul style="list-style-type: none"> • 0 to 63—Numerical DSCP values. The default value is 0. • af1 to af43—Assured forwarding (AF) DSCP values. • cs1 to cs7—Type of service (ToS) precedence values. • default—Default DSCP value. • ef—Expedited forwarding (EF) DSCP values.

Examples

The following example shows the new output fields associated with the QoS: Policies Aggregation Enhancements feature beginning in Cisco IOS XE Release 2.6 for subscriber statistics. The new output fields begin with the label “Account QoS Statistics.”

```
Router# show policy-map interface port-channel 1.1

Port-channel1.1
  Service-policy input: input_policy
    Class-map: class-default (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: any
      QoS Set
      dscp default
      No packet marking statistics available
  Service-policy output: Port-channel_1_subscriber
    Class-map: EF (match-any)
      105233 packets, 6734912 bytes
      5 minute offered rate 134000 bps, drop rate 0000 bps
      Match: dscp ef (46)
      Match: access-group name VLAN_REMARK_EF
      Match: qos-group 3
      Account QoS statistics
        Queueing
          Packets dropped 0 packets/0 bytes
      QoS Set
      cos 5
      No packet marking statistics available
      dscp ef
      No packet marking statistics available
    Class-map: AF4 (match-all)
      105234 packets, 6734976 bytes
      5 minute offered rate 134000 bps, drop rate 0000 bps
      Match: dscp cs4 (32)
      Account QoS statistics
        Queueing
          Packets dropped 0 packets/0 bytes
      QoS Set
      cos 4
      No packet marking statistics available
```

```

Class-map: AF1 (match-any)
  315690 packets, 20204160 bytes
  5 minute offered rate 402000 bps, drop rate 0000 bps
  Match: dscp cs1 (8)
  Match: dscp af11 (10)
  Match: dscp af12 (12)
  Account QoS statistics
    Queueing
      Packets dropped 0 packets/0 bytes
    QoS Set
      cos 1
  No packet marking statistics available
Class-map: class-default (match-any) fragment Port-channel_BE
  315677 packets, 20203328 bytes
  5 minute offered rate 402000 bps, drop rate 0000 bps
  Match: any
  Queueing
    queue limit 31250 bytes
    (queue depth/total drops/no-buffer drops) 0/0/0
    (pkts output/bytes output) 315679/20203482
    bandwidth remaining ratio 1

```

Examples

The following example shows how to display the policer statistics (the packet and byte count). The output displays only the applicable count (either packets or bytes) with the actual number.

```
Router# show policy-map interface GigabitEthernet 3/1 input
```

```

GigabitEthernet3/1
  Service-policy input: in1
    Class-map: p1 (match-all)
      0 packets
      Match: precedence 1
        QoS Set
          ip precedence 7
    police:
      cir 20 %
      cir 200000000 bps, bc 6250000 bytes
      conformed 0 bytes; actions:
        transmit
      exceeded 0 bytes; actions:
        drop
      conformed 0000 bps, exceed 0000 bps
    Class-map: class-default (match-any)
      10000000 packets
      Match: any
      police:
        cir 20 %
        cir 200000000 bps, bc 6250000 bytes
        conformed 174304448 bytes; actions:
          transmit
        exceeded 465695552 bytes; actions:
          drop
        conformed 4287000 bps, exceed 11492000 bps

```

Examples

The following example shows how to display the statistics and the configurations of the input and output service policies that are attached to an interface:

```
Router# show policy-map interface GigabitEthernet 1/2/0
```

```

Load for five secs: 1%/0%; one minute: 1%; five minutes: 1%
Time source is hardware calendar, *23:02:40.857 pst Thu Mar 3 2011

```

```
GigabitEthernet1/2/0
```

```
  Service-policy input: policy-in
```

```
    Class-map: class-exp-0 (match-all)
```



```

6647740 packets, 9304674796 bytes
30 second offered rate 3234000 bps, drop rate 0 bps
Match: mpls experimental topmost 0
QoS Set
  precedence 3
  Packets marked 6647740

Class-map: class-default (match-any)
  1386487 packets, 1903797872 bytes
  30 second offered rate 658000 bps, drop rate 0 bps
  Match: any

Service-policy output: policy-out

Class-map: class-pre-1 (match-all)
  2041355 packets, 2857897000 bytes
  30 second offered rate 986000 bps, drop rate 0 bps

  Match: ip precedence 1
  QoS Set
    mpls experimental topmost 1
    Packets marked 2041355

Class-map: class-default (match-any)
  6129975 packets, 8575183331 bytes
  30 second offered rate 2960000 bps, drop rate 0 bps
  Match: any

```

The table below describes the significant fields shown in the display.

Table 45: show policy-map interface Field Descriptions—Cisco Catalyst 4000 Series Routers

Field	Description
class-map	Displays the class of traffic. 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.
conformed	Displays the action to be taken on packets conforming to a specified rate. Also displays the number of packets and bytes on which the action was taken.
drop	Indicates that the packet discarding action for all the packets belonging to the specified class has been configured.
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.
match	Match criteria specified for the class of traffic.
packets, bytes	Number of the packets (also shown in bytes) identified as belonging to the class of traffic being displayed.

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.
QoS Set	Indicates that QoS group (set) has been configured for the particular class.
service-policy input	Name of the input service policy applied to the specified interface.

Examples

The following example shows how to display the class maps configured for a pseudowire interface:

```
Router# show policy-map interface pseudowire2
pseudowire2
  Service-policy output: pw_brr

  Class-map: prec1 (match-all)
    0 packets, 0 bytes
    30 second offered rate 0000 bps, drop rate 0000 bps
    Match: ip precedence 1
    Queueing
      queue limit 4166 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 0/0
      bandwidth remaining ratio 1

  Class-map: prec2 (match-all)
    0 packets, 0 bytes
    30 second offered rate 0000 bps, drop rate 0000 bps
    Match: ip precedence 2
    Queueing
      queue limit 4166 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 0/0
      bandwidth remaining ratio 2

  Class-map: prec3 (match-all)
    0 packets, 0 bytes
    30 second offered rate 0000 bps, drop rate 0000 bps
    Match: ip precedence 3
    Queueing
      queue limit 4166 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 0/0
      bandwidth remaining ratio 3

  Class-map: class-default (match-any)
    0 packets, 0 bytes
    30 second offered rate 0000 bps, drop rate 0000 bps
    Match: any
    Queueing
      queue limit 4166 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 0/0
      bandwidth remaining ratio 4
Device#
```

The table below describes the significant fields shown in the display.

Table 46: show policy-map interface Field Descriptions—Pseudowire Policy Map Information

Field	Description
bandwidth	Indicates the percentage of bandwidth allocated for traffic queueing.
Class-map	Displays the class of traffic. 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.
Match	Match criteria specified for the class of traffic.
packets, bytes	Number of the packets (also shown in bytes) identified as belonging to the class of traffic being displayed.
Queueing	Indicates that queueing is enabled.
queue limit	Maximum number of packets that a queue can hold for a class policy configured in a policy map.
service-policy output	Name of the output service policy applied to the specified interface.

Related Commands

Command	Description
bandwidth remaining ratio	Specifies a bandwidth-remaining ratio for class queues and subinterface-level queues to determine the amount of unused (excess) bandwidth to allocate to the queue during congestion.
class-map	Creates a class map to be used for matching packets to a specified class.
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.

Command	Description
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.
priority	Specifies that low-latency behavior must be given to a traffic class and configures multiple priority queues.
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 class-map	Display all class maps and their matching criteria.
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 mls qos	Displays MLS QoS information.
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.

show queue



Note

Effective with Cisco IOS XE Release 2.6, Cisco IOS Release 15.0(1)S, and Cisco IOS Release 15.1(3)T, the **showqueue** command is hidden. Although this command is still available in Cisco IOS software, the CLI interactive Help does not display it if you attempt to view it by entering a question mark at the command line. This command will be completely removed in a future release, which means that you will need to use the appropriate replacement command (or sequence of commands). For more information (including a list of replacement commands), see the "Legacy QoS Command Deprecation" feature document in the *Cisco IOS XE Quality of Service Solutions Configuration Guide* or the "Legacy QoS Command Deprecation" feature document in the *Cisco IOS Quality of Service Solutions Configuration Guide*.



Note

Effective with Cisco IOS XE Release 3.2S, the **showqueue** command is replaced by a modular QoS CLI (MQC) command (or sequence of MQC commands). For the appropriate replacement command (or sequence of commands), see the "Legacy QoS Command Deprecation" feature document in the *Cisco IOS XE Quality of Service Solutions Configuration Guide*.

To display the contents of packets inside a queue for a particular interface or virtual circuit (VC), use the **showqueue** command in user EXEC or privileged EXEC mode.

show queue *interface-name interface-number* [**queue-number**][**vc vpi/ vci**]

Syntax Description

<i>interface-name</i>	The name of the interface.
<i>interface-number</i>	The number of the interface.
<i>queue-number</i>	(Optional) The number of the queue. The queue number is a number from 1 to 16.
vc	(Optional) For ATM interfaces only, shows the fair queueing configuration for a specified permanent virtual circuit (PVC). The name can be up to 16 characters long.
<i>vpi /</i>	<p>(Optional) ATM network virtual path identifier (VPI) for this PVC. The absence of the "/" and a <i>vpi</i> value defaults the <i>vpi</i> value to 0.</p> <p>On the Cisco 7200 and Cisco 7500 series routers, this value ranges from 0 to 255.</p> <p>The <i>vpi</i> and <i>vci</i> arguments cannot both be set to 0; if one is 0, the other cannot be 0.</p> <p>If this value is omitted, information for all VCs on the specified ATM interface or subinterface is displayed.</p>

<i>vci</i>	<p>(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 atmvc-per-vp command. Typically, lower values 0 to 31 are reserved for specific traffic (F4 Operation, Administration, and Maintenance (OAM), switched virtual circuit (SVC) signalling, Integrated Local Management Interface (ILMI), and so on) and should not be used.</p> <p>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.</p> <p>The <i>vpi</i> and <i>vci</i> arguments cannot both be set to 0; if one is 0, the other cannot be 0.</p>
------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
10.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T, but without support for hierarchical queueing framework (HQF). See the “Usage Guidelines” for additional information.
Cisco IOS XE Release 2.6	This command was modified. This command was hidden.
15.0(1)S	This command was modified. This command was hidden.
15.1(3)T	This command was modified. This command was hidden.
Cisco IOS XE Release 3.2S	This command was replaced by an MQC command (or sequence of MQC commands).

Usage Guidelines

This command displays the contents of packets inside a queue for a particular interface or VC.

This command does not support VIP-distributed Weighted Random Early Detection WRED (DWRED). You can use the **vc** keyword and the **showqueue** command arguments to display output for a PVC only on Enhanced ATM port adapters (PA-A3) that support per-VC queueing.

This command does not support HQF. Use the **showpolicy-map** and the **showpolicy-mapinterface** commands to gather HQF information and statistics.

Examples

The following examples show sample output when the **showqueue** command is entered and either weighted fair queueing (WFQ), WRED, or flow-based WRED are configured.

Examples

The following is sample output from the **showqueue** command for PVC 33 on the atm2/0.33 ATM subinterface. Two conversations are active on this interface. WFQ ensures that both data streams receive equal bandwidth on the interface while they have messages in the pipeline.

```
Router# show queue
      atm2/0.33 vc 33
Interface ATM2/0.33 VC 0/33
  Queueing strategy: weighted fair
  Total output drops per VC: 18149
  Output queue: 57/512/64/18149 (size/max total/threshold/drops)
    Conversations 2/2/256 (active/max active/max total)
    Reserved Conversations 3/3 (allocated/max allocated)
    (depth/weight/discards/tail drops/interleaves) 29/4096/7908/0/0
  Conversation 264, linktype: ip, length: 254
    source: 10.1.1.1, destination: 10.0.2.20, id: 0x0000, ttl: 59,
    TOS: 0 prot: 17, source port 1, destination port 1
    (depth/weight/discards/tail drops/interleaves) 28/4096/10369/0/0
  Conversation 265, linktype: ip, length: 254
    source: 10.1.1.1, destination: 10.0.2.20, id: 0x0000, ttl: 59,
    TOS: 32 prot: 17, source port 1, destination port 2
```

The table below describes the significant fields shown in the display.

Table 47: show queue Field Descriptions for WFQ

Field	Description
Queueing strategy	Type of queueing active on this interface.
Total output drops per VC	Total output packet drops.
Output queue	Output queue size, in packets. Max total defines the aggregate queue size of all the WFQ flows. Threshold is the individual queue size of each conversation. Drops are the dropped packets from all the conversations in WFQ.
Conversations	WFQ conversation number. A conversation becomes inactive or times out when its queue is empty. Each traffic flow in WFQ is based on a queue and represented by a conversation. Max active is the number of active conversations that have occurred since the queueing feature was configured. Max total is the number of conversations allowed simultaneously.

Field	Description
Reserved Conversations	Traffic flows not captured by WFQ, such as class-based weighted fair queueing (CBWFQ) configured by the bandwidth command or a Resource Reservation Protocol (RSVP) flow, have a separate queue that is represented by a reserved conversation. Allocated is the current number of reserved conversations. Max allocated is the maximum number of allocated reserved conversations that have occurred.
depth	Queue depth for the conversation, in packets.
weight	Weight used in WFQ.
discards	Number of packets dropped from the conversation's queue.
tail drops	Number of packets dropped from the conversation when the queue is at capacity.
interleaves	Number of packets interleaved.
linktype	Protocol name.
length	Packet length.
source	Source IP address.
destination	Destination IP address.
id	Packet ID.
ttl	Time to live count.
TOS	IP type of service.
prot	Layer 4 protocol number.

Examples

The following is sample output from the **showqueue** command issued for serial interface 1 on which flow-based WRED is configured. The output shows information for each packet in the queue; the data identifies the packet by number, the flow-based queue to which the packet belongs, the protocol used, and so forth.

```
Router# show queue Serial1
Output queue for Serial1 is 2/0

Packet 1, flow id:160, linktype:ip, length:118, flags:0x88
source:10.1.3.4, destination:10.1.2.2, id:0x0000, ttl:59,
TOS:32 prot:17, source port 1, destination port 515
```



```

data:0x0001 0x0203 0x0405 0x0607 0x0809 0x0A0B 0x0C0D
      0x0E0F 0x1011 0x1213 0x1415 0x1617 0x1819 0x1A1B

Packet 2, flow id:161, linktype:ip, length:118, flags:0x88
source:10.1.3.5, destination:10.1.2.2, id:0x0000, ttl:59,
TOS:64 prot:17, source port 1, destination port 515
data:0x0001 0x0203 0x0405 0x0607 0x0809 0x0A0B 0x0C0D
      0x0E0F 0x1011 0x1213 0x1415 0x1617 0x1819 0x1A1B

```

The table below describes the significant fields shown in the display.

Table 48: show queue Field Descriptions for Flow-Based WRED

Field	Description
Packet	Packet number.
flow id	Flow-based WRED number.
linktype	Protocol name.
length	Packet length.
flags	Internal version-specific flags.
source	Source IP address.
destination	Destination IP address.
id	Packet ID.
ttl	Time to live count.
prot	Layer 4 protocol number.
data	Packet data.

Examples

The following is sample output from the **show queue** command issued for serial interface 3 on which WRED is configured. The output has been truncated to show only 2 of the 24 packets.

```

Router# show queue Serial3
Output queue for Serial3 is 24/0

Packet 1, linktype:ip, length:118, flags:0x88
source:10.1.3.25, destination:10.1.2.2, id:0x0000, ttl:59,
TOS:192 prot:17, source port 1, destination port 515
data:0x0001 0x0203 0x0405 0x0607 0x0809 0x0A0B 0x0C0D
      0x0E0F 0x1011 0x1213 0x1415 0x1617 0x1819 0x1A1B

Packet 2, linktype:ip, length:118, flags:0x88
source:10.1.3.26, destination:10.1.2.2, id:0x0000, ttl:59,
TOS:224 prot:17, source port 1, destination port 515
data:0x0001 0x0203 0x0405 0x0607 0x0809 0x0A0B 0x0C0D
      0x0E0F 0x1011 0x1213 0x1415 0x1617 0x1819 0x1A1B

```

Related Commands

Command	Description
atm vc-per-vp	Sets the maximum number of VCIs to support per VPI.
custom-queue-list	Assigns a custom queue list to an interface.
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.
fair-queue (WFQ)	Enables WFQ for an interface.
priority-group	Assigns the specified priority list to an interface.
random-detect (interface)	Enables WRED or DWRED.
random-detect flow	Enables flow-based WRED.
show frame-relay pvc	Displays information and statistics about WFQ for a VIP-based interface.
show queueing	Lists all or selected configured queueing strategies.

show queueing



Note

Effective with Cisco IOS XE Release 2.6, Cisco IOS Release 15.0(1)S, and Cisco IOS Release 15.1(3)T, the **showqueueing** command is hidden. Although this command is still available in Cisco IOS software, the CLI interactive Help does not display it if you attempt to view it by entering a question mark at the command line. This command will be completely removed in a future release, which means that you will need to use the appropriate replacement command (or sequence of commands). For more information (including a list of replacement commands), see the "Legacy QoS Command Deprecation" feature document in the *Cisco IOS XE Quality of Service Solutions Configuration Guide* or the "Legacy QoS Command Deprecation" feature document in the *Cisco IOS Quality of Service Solutions Configuration Guide*.



Note

Effective with Cisco IOS XE Release 3.2S, the **showqueueing** command is replaced by a modular QoS CLI (MQC) command (or sequence of MQC commands). For the appropriate replacement command (or sequence of commands), see the "Legacy QoS Command Deprecation" feature document in the *Cisco IOS XE Quality of Service Solutions Configuration Guide*.

To list all or selected configured queueing strategies, use the **showqueueing** command in user EXEC or privileged EXEC mode.

show queueing [**custom**| **fair**| **priority**| **random-detect** [**interface** *atm-subinterface* [**vc** [[*vpi*] *vci*]]]]

Syntax Description

custom	(Optional) Status of the custom queueing list configuration.
fair	(Optional) Status of the fair queueing configuration.
priority	(Optional) Status of the priority queueing list configuration.
random-detect	(Optional) Status of the Weighted Random Early Detection (WRED) and distributed WRED (DWRED) configuration, including configuration of flow-based WRED.
interface <i>atm-subinterface</i>	(Optional) Displays the WRED parameters of every virtual circuit (VC) with WRED enabled on the specified ATM subinterface.
vc	(Optional) Displays the WRED parameters associated with a specific VC. If desired, both the virtual path identifier (VPI) and virtual circuit identifier (VCI) values, or just the VCI value, can be specified.

<i>vpi</i> /	(Optional) Specifies the VPI. If the <i>vpi</i> argument is omitted, 0 is used as the VPI value for locating the permanent virtual circuit (PVC). If the <i>vpi</i> argument is specified, the/separator is required.
<i>vci</i>	(Optional) Specifies the VCI.

Command Default

If no optional keyword is entered, this command shows the configuration of all interfaces.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
10.3	This command was introduced.
12.0(4)T	This command was integrated into Cisco IOS Release 12.0(4)T. The red keyword was changed to random-detect .
12.1(2)T	This command was modified. This command was modified to include information about the Frame Relay PVC Interface Priority Queueing (FR PIPQ) feature.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.0(24)S	This command was integrated into Cisco IOS Release 12.0(24)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXF2	This command was integrated into Cisco IOS Release 12.2(18)SXF2.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Cisco IOS XE Release 2.6	This command was modified. This command was hidden.
15.0(1)S	This command was modified. This command was hidden.
15.1(3)T	This command was modified. This command was hidden.
Cisco IOS XE Release 3.2S	This command was replaced by an MQC command (or sequence of MQC commands).

Usage Guidelines

This command does not support HQF. Use the **showpolicy-map** and the **showpolicy-mapinterface** commands to gather HQF information and statistics.

Examples

This section provides sample output from **show queueing** commands. Depending upon the interface or platform in use and the options enabled, the output that you see may vary slightly from the examples shown below.

Examples

The following sample output shows that FR PIPQ (referred to as “DLCI priority queue”) is configured on serial interface 0. The output also shows the size of the four data-link connection identifier (DLCI) priority queues.

```
Router# show queueing
Current fair queue configuration:
  Interface      Discard      Dynamic      Reserved
                threshold queue count  queue count
  Serial3/1      64           256          0
  Serial3/3      64           256          0
Current DLCI priority queue configuration:
  Interface      High      Medium      Normal      Low
                limit   limit   limit   limit
  Serial0        20       40       60       80
Current priority queue configuration:
List  Queue  Args
1     low   protocol ipx
1     normal protocol vines
1     normal protocol appletalk
1     normal protocol ip
1     normal protocol decnet
1     normal protocol decnet_node
1     normal protocol decnet_rout
1     normal protocol decnet_rout
1     medium protocol xns
1     high  protocol clns
1     normal protocol bridge
1     normal protocol arp
Current custom queue configuration:
Current random-detect configuration:
```

Examples

The following is sample output from the **show queueing** command. There are two active conversations in serial interface 0. Weighted fair queueing (WFQ) ensures that both of these IP data streams--both using TCP--receive equal bandwidth on the interface while they have messages in the pipeline, even though more FTP data is in the queue than remote-procedure call (RCP) data.

```
Router# show queueing
Current fair queue configuration:
Interface      Discard      Dynamic      Reserved
                threshold queue count  queue count
  Serial0       64           256          0
  Serial1       64           256          0
  Serial2       64           256          0
  Serial3       64           256          0
Current priority queue configuration:
List  Queue  Args
1     high  protocol cdp
2     medium interface Ethernet1
Current custom queue configuration:
Current random-detect configuration:
  Serial5
    Queueing strategy:random early detection (WRED)
    Exp-weight-constant:9 (1/512)
    Mean queue depth:40
    Class  Random      Tail      Minimum      Maximum      Mark
          drop      drop threshold threshold probability
      0    1401      9066        20         40        1/10
      1         0         0         22         40        1/10
      2         0         0         24         40        1/10
```

3	0	0	26	40	1/10
4	0	0	28	40	1/10
5	0	0	31	40	1/10
6	0	0	33	40	1/10
7	0	0	35	40	1/10
rsvp	0	0	37	40	1/10

Examples

The following is sample output from the **show queueing custom** command:

```
Router# show queueing custom
Current custom queue configuration:
List Queue Args
3 10 default
3 3 interface Tunnel3
3 3 protocol ip
3 3 byte-count 444 limit 3
```

Examples

The following is sample output from the **show queueing random-detect** command. The output shows that the interface is configured for flow-based WRED to ensure fair packet drop among flows. The **random-detect flow average-depth-factor** command was used to configure a scaling factor of 8 for this interface. The scaling factor is used to scale the number of buffers available per flow and to determine the number of packets allowed in the output queue of each active flow before the queue is susceptible to packet drop. The maximum flow count for this interface was set to 16 by the **random-detect flow count** command.

```
Router# show queueing random-detect
Current random-detect configuration:
Serial1
Queueing strategy: random early detection (WRED)
Exp-weight-constant: 9 (1/512)
Mean queue depth: 29
Max flow count: 16          Average depth factor: 8
Flows (active/max active/max): 39/40/16
```

Class	Random drop	Tail drop	Minimum threshold	Maximum threshold	Mark probability
0	31	0	20	40	1/10
1	33	0	22	40	1/10
2	18	0	24	40	1/10
3	14	0	26	40	1/10
4	10	0	28	40	1/10
5	0	0	31	40	1/10
6	0	0	33	40	1/10
7	0	0	35	40	1/10
rsvp	0	0	37	40	1/10

Examples

The following is sample output from the **show queueing random-detect** command for DWRED:

```
Current random-detect configuration:
Serial1
Queueing strategy: random early detection (WRED)
Exp-weight-constant: 9 (1/512)
Mean queue depth: 29
Max flow count: 16          Average depth factor: 8
Flows (active/max active/max): 39/40/16
```

Class	Random drop	Tail drop	Minimum threshold	Maximum threshold	Mark probability
0	31	0	20	40	1/10
1	33	0	22	40	1/10
2	18	0	24	40	1/10
3	14	0	26	40	1/10
4	10	0	28	40	1/10

```

          5          0          0          31          40          1/10
          6          0          0          33          40          1/10
          7          0          0          35          40          1/10
    rsvp          0          0          37          40          1/10
Current random-detect configuration:
FastEthernet2/0/0
Queueing strategy:fifo
Packet drop strategy:VIP-based random early detection (DWRED)
Exp-weight-constant:9 (1/512)
Mean queue depth:0
Queue size:0          Maximum available buffers:6308
Output packets:5 WRED drops:0 No buffer:0
Class    Random      Tail    Minimum    Maximum    Mark      Output
          drop        drop    threshold threshold probability Packets
0          0          0       109        218        1/10        5
1          0          0       122        218        1/10        0
2          0          0       135        218        1/10        0
3          0          0       148        218        1/10        0
4          0          0       161        218        1/10        0
5          0          0       174        218        1/10        0
6          0          0       187        218        1/10        0
7          0          0       200        218        1/10        0

```

The table below describes the significant fields shown in the display.

Table 49: show queueing Field Descriptions

Field	Description
Discard threshold	Number of messages allowed in each queue.
Dynamic queue count	Number of dynamic queues used for best-effort conversations.
Reserved queue count	Number of reservable queues used for reserved conversations.
High limit	High DLCI priority queue size in maximum number of packets.
Medium limit	Medium DLCI priority queue size, in maximum number of packets.
Normal limit	Normal DLCI priority queue size, in maximum number of packets.
Low limit	Low DLCI priority queue size, in maximum number of packets.
List	Custom queueing--Number of the queue list. Priority queueing--Number of the priority list.
Queue	Custom queueing--Number of the queue. Priority queueing--Priority queue level (high , medium , normal , or low keyword).
Args	Packet matching criteria for that queue.

Field	Description
Exp-weight-constant	Exponential weight factor.
Mean queue depth	Average queue depth. It is calculated 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.
Random drop	Number of packets 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	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.
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.

Related Commands

Command	Description
custom-queue-list	Assigns a custom queue list to an interface.
exponential-weighting-constant	Configures the exponential weight factor for the average queue size calculation for a WRED parameter group.
fair-queue (WFQ)	Enables WFQ for an interface.
frame-relay interface-queue priority	Enables the FR PIPQ feature.
precedence (WRED group)	Configures a WRED group for a particular IP Precedence.
priority-group	Assigns the specified priority list to an interface.
priority-list interface	Establishes queueing priorities on packets entering from a given interface.

Command	Description
priority-list queue-limit	Specifies the maximum number of packets that can be waiting in each of the priority queues.
queue-list interface	Establishes queueing priorities on packets entering on an interface.
queue-list queue byte-count	Specifies how many bytes the system allows to be delivered from a given queue during a particular cycle.
random-detect (interface)	Enables WRED or DWRED.
random-detect flow average-depth-factor	Sets the multiplier to be used in determining the average depth factor for a flow when flow-based WRED is enabled.
random-detect flow count	Sets the flow count for flow-based WRED.
show interfaces	Displays the statistical information specific to a serial interface.
show queue	Displays the contents of packets inside a queue for a particular interface or VC.
show queueing interface	Displays the queueing statistics of an interface or VC.

show queueing interface

To display the queueing statistics of an interface, use the **showqueueinginterface** command in user EXEC or privileged EXEC mode.

show queueing interface *type number* [**vc** [*vpi* /] *vci*]]

Catalyst 6500 Series Switches

show queueing interface {*type number*| **null 0**| **vlan** *vlan-id*} [**detailed**]

Cisco 7600 Series Routers

show queueing interface {*type number*| **null 0**| **vlan** *vlan-id*}

Syntax Description

<i>type number</i>	Interface type and interface number. For Cisco 7600 series routers, the valid interface types are ethernet , fastethernet , gigabitethernet , tengigabitethernet , pos , atm , and ge-wan . For Cisco 7600 series routers, the interface number is the module and port number. See the “Usage Guidelines” section for more information.
vc	(Optional) Shows the weighted fair queueing (WFQ) and Weighted Random Early Detection (WRED) parameters associated with a specific virtual circuit (VC). If desired, both the virtual path identifier (VPI) and virtual channel identifier (VCI) values, or just the VCI value, can be specified.
<i>vpi</i> /	(Optional) The VPI. If the <i>vpi</i> argument is omitted, 0 is used as the VPI value for locating the permanent virtual circuit (PVC). If the <i>vpi</i> argument is specified, the/separator is required.
<i>vci</i>	(Optional) The VCI.
null 0	Specifies the null interface number; the only valid value is 0.
vlan <i>vlan-id</i>	Specifies the VLAN identification number; valid values are from 1 to 4094.
detailed	(Optional) Displays the detailed statistics information per policy class.

Command Modes

User EXEC (>) Privileged EXEC (#)

Cisco 7600 Series Routers

User EXEC (>)

Command History

Release	Modification
11.1(22)CC	This command was introduced.
12.2(14)SX	This command was implemented on the Supervisor Engine 720.
12.2(17d)SXB	This command was implemented on the Supervisor Engine 2 and integrated into Cisco IOS Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXI	The detailed keyword was added.

Usage Guidelines**Cisco 7600 Series Routers**

The pos, atm, and ge-wan interfaces are supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2 only.

The *typenumber* argument used with the **interface** keyword designates the module and port number. Valid values depend on the specified interface type and the chassis and module that are used. For example, if you specify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module installed in a 13-slot chassis, valid values for the module number are from 1 to 13 and valid values for the port number are from 1 to 48.

The **show queueing interface** command does not display the absolute values that are programmed in the hardware. Use the **show qm-spport-data** command to verify the values that are programmed in the hardware.

Catalyst 6500 Series Switches

In Cisco IOS Release 12.2(33)SXI and later releases, the optional **detailed** keyword is available. The **show queueing interface detailed** command output includes the following information:

- Display of the last 30-second counters.
- Display of the peak 30-second counters over the last 5 minutes.
- Display of the 5-minute average and peak bps rates.
- The peak rates are monitored with 10-second resolution. Releases prior to Cisco IOS Release 12.2(33)SXI were monitored at 30-second resolution.

Examples

The following is sample output from the **show queueing interface** command. In this example, WRED is the queueing strategy in use. The output varies according to queueing strategy in use.

```
Router# show queueing interface atm 2/0
```

```

Interface ATM2/0 VC 201/201
Queueing strategy:random early detection (WRED)
Exp-weight-constant:9 (1/512)
Mean queue depth:49
Total output drops per VC:759
Class      Random      Tail      Minimum      Maximum      Mark
           drop       drop    threshold threshold probability
0           165         26         30          50         1/10
1           167         12         32          50         1/10
2           173         14         34          50         1/10
3           177         25         36          50         1/10
4            0           0         38          50         1/10
5            0           0         40          50         1/10
6            0           0         42          50         1/10
7            0           0         44          50         1/10
rsvp        0           0         46          50         1/10

```

The table below describes the significant fields shown in the display.

Table 50: show queueing interface Field Descriptions

Field	Description
Queueing strategy	Name of the queueing strategy in use (for example, WRED).
Exp-weight-constant	Exponential weight constant. 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.
Random drop	Number of packets 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	Number of packets dropped when the mean queue depth is greater than the maximum threshold value for the specified IP precedence level.
Minimum threshold	Minimum WRED threshold in packets.
Maximum threshold	Maximum WRED threshold in packets.
Mark probability	Fraction of packets dropped when the average queue depth is at the maximum threshold.

The following is sample output from the **show queueing interface** command in Cisco IOS Release 12.2(33)SXI and later releases:

```
Router# show queueing interface gigabitethernet 3/27 detailed
.
.
.
Packets dropped on Transmit:
  BPDUs: 0
  queue  Total pkts  30-s pkts / peak  5 min average/peak pps  [cos-map]
-----
  1      443340      55523 / 66671      3334 / 44455      [0 1 ]
  1      7778888      55555 / 66666      23333 / 34000      [2 3 ]
  2         0         0 / 0         0 / 0         [4 5 ]
  2         0         0 / 0         0 / 0         [6 7 ]
.
.
.
```

The table below describes the significant fields added when you enter the **detailed** keyword.

Table 51: show queueing interface detailed Field Descriptions

Field	Description
Packets dropped on Transmit	Displays information regarding the packets dropped in transmission.
BPDUs	Number of Bridge Protocol Data Unit (BPDU) packets.
queue	Queue number.
Total pkts	Display of the last 30-second counters.
30-s pkts / peak	Display of the peak 30-second counters over the last 5 minutes.
5 min average/peak pps	Display of the 5-minute average and peak rates in packets per second (pps).
cos-map	Class of service (CoS) mapping.

Related Commands

custom-queue-list	Assigns a custom queue list to an interface.
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.
fair-queue (WFQ)	Enables WFQ for an interface.
priority-group	Assigns the specified priority list to an interface.

random-detect flow	Enables flow-based WRED.
random-detect (interface)	Enables WRED or DWRED.
random-detect (per VC)	Enables per-VC WRED or per-VC DWRED.
show frame-relay pvc	Displays information and statistics about WFQ for a VIP-based interface.
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 qm-sp port-data	Displays information about the QoS manager switch processor.
show queueing	Lists all or selected configured queueing strategies.

vbr-nrt

To configure the variable bit rate-nonreal time (VBR-NRT) quality of service (QoS) and specify output peak cell rate (PCR), output sustainable cell rate (SCR), and output maximum burst cell size for an ATM permanent virtual circuit (PVC), PVC range, switched virtual circuit (SVC), VC class, or VC bundle member, use the **vbr-nrt** command in the appropriate command mode. To remove the VBR-NRT parameters, use the **no** form of this command.

vbr-nrt *output-pcr output-scr output-maxburstsize* [*input-pcr*] [*input-scr*] [*input-maxburstsize*]

no vbr-nrt *output-pcr output-scr output-maxburstsize* [*input-pcr*] [*input-scr*] [*input-maxburstsize*]

Cisco 10000 Series Router

vbr-nrt *output-pcr output-scr output-maxburstsize*

no vbr-nrt *output-pcr output-scr output-maxburstsize*

Syntax Description

<i>output-pcr</i>	The output PCR, in kilobytes per second (kbps).
<i>output-scr</i>	The output SCR, in kbps.
<i>output-maxburstsize</i>	The output maximum burst cell size, expressed in number of cells.
<i>input-pcr</i>	(Optional for SVCs only) The input PCR, in kbps.
<i>input-scr</i>	(Optional for SVCs only) The input SCR, in kbps.
<i>input-maxburstsize</i>	(Optional for SVCs only) The input maximum burst cell size, expressed in number of cells.

Command Default

Unspecified bit rate (UBR) QoS at the maximum line rate of the physical interface is the default.

Command Modes

ATM PVC-in-range configuration (for an individual PVC within a PVC range) ATM PVC range configuration (for an ATM PVC range) ATM PVP configuration Bundle-vc configuration (for ATM VC bundle members) Interface-ATM-VC configuration (for an ATM PVC or SVC) VC-class configuration (for a VC class)

Command History

Release	Modification
11.3T	This command was introduced.
12.0(3)T	This command was enhanced to support configuration of VBR-NRT QoS and specification of output PCR, output SCR, and output maximum burst cell size for ATM bundles and VC bundle members.

Release	Modification
12.0(25)SX	This command was integrated into Cisco IOS Release 12.0(25)SX and implemented on the Cisco 10000 series router.
12.1(5)T	This command was made available in PVC range and PVC-in-range configuration modes.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.3	This command was made available in ATM PVP configuration mode.

Usage Guidelines

Configure QoS parameters using the **ubr**, **ubr+**, or **vbr-nrt** command. The last command you enter will apply to the PVC or SVC you are configuring.

If the **vbr-nrt** command is not explicitly configured on an ATM PVC or SVC, the VC inherits the following default configuration (listed in order of precedence):

- Configuration of any QoS command (**ubr**, **ubr+**, or **vbr-nrt**) in a VC class assigned to the PVC or SVC itself.
- Configuration of any QoS command (**ubr**, **ubr+**, or **vbr-nrt**) in a VC class assigned to the PVC's or SVC's ATM subinterface.
- Configuration of any QoS command (**ubr**, **ubr+**, or **vbr-nrt**) in a VC class assigned to the PVC's or SVC's ATM main interface.
- Global default: UBR QoS at the maximum line rate of the PVC or SVC.

To use this command in VC-class configuration mode, enter the **vc-class atm** global configuration command before you enter the **vbr-nrt** command. This command has no effect if the VC class that contains the command is attached to a standalone VC, that is, if the VC is not a bundle member.

To use this command in bundle-vc configuration mode, enter the **pvc-bundle** configuration command and add the VC as a bundle member.

VCs in a VC bundle are subject to the following configuration inheritance rules (listed in order of precedence):

- VC configuration in bundle-vc mode
- Bundle configuration in bundle mode (with the effect of assigned VC-class configuration)
- Subinterface configuration in subinterface mode

Cisco 10000 Series Router

Input PCR, input SCR, and input maximum burst size (MBS) are not supported.

For Cisco IOS Release 12.2(31)SB2 and later releases, if you set the output PCR and SCR to the same value, the Cisco IOS software allows a maximum burst cell size of 1. For example:

Prior to Cisco IOS Release 12.2(31)SB2

```
interface ATM2/0/0.81801 point-to-point
 bandwidth 11760
 pvc 81/801
  vbr-nrt 11760 11760 32
  encapsulation aal5snap
  protocol pppoe
```

Cisco IOS Release 12.2(31)SB2 and Later Releases

```
interface ATM2/0/0.81801 point-to-point
 bandwidth 11760
 pvc 81/801
  vbr-nrt 11760 11760 1
  encapsulation aal5snap
  protocol pppoe
```

Examples

The following example specifies the output PCR for an ATM PVC to be 100,000 kbps, the output SCR to be 50,000 kbps, and the output MBS to be 64:

```
pvc 1/32
 vbr-nrt 100000 50000 64
```

The following example specifies the VBR-NRT output and input parameters for an ATM SVC:

```
svc atm-svc1 nsap 47.0091.81.000000.0040.0B0A.2501.ABC1.3333.3333.05
 vbr-nrt 10000 5000 32 20000 10000 64
```

Related Commands

Command	Description
abr	Selects ABR QoS and configures output peak cell rate and output minimum guaranteed cell rate for an ATM PVC or virtual circuit class.
broadcast	Configures broadcast packet duplication and transmission for an ATM VC class, PVC, SVC, or VC bundle.
bump	Configures the bumping rules for a virtual circuit class that can be assigned to a virtual circuit bundle.
bundle	Creates a bundle or modifies an existing bundle to enter bundle configuration mode.
class-int	Assigns a VC class to an ATM main interface or subinterface.
class-vc	Assigns a VC class to an ATM PVC, SVC, or VC bundle member.
encapsulation	Sets the encapsulation method used by the interface.

Command	Description
inarp	Configures the Inverse ARP time period for an ATM PVC, VC class, or VC bundle.
oam-bundle	Enables end-to-end F5 OAM loopback cell generation and OAM management for a virtual circuit class that can be applied to a virtual circuit bundle.
oam retry	Configures parameters related to OAM management for an ATM PVC, SVC, VC class, or VC bundle.
precedence	Configures precedence levels for a virtual circuit class that can be assigned to a virtual circuit bundle and thus applied to all virtual circuit members of that bundle.
protect	Configures a virtual circuit class with protected group or protected virtual circuit status for application to a virtual circuit bundle member.
protocol (ATM)	Configures a static map for an ATM PVC, SVC, VC class, or VC bundle, and enables Inverse ARP or Inverse ARP broadcasts on an ATM PVC by either configuring Inverse ARP directly on the PVC, on the VC bundle, or in a VC class (applies to IP and IPX protocols only).
pvc-bundle	Adds a PVC to a bundle as a member of the bundle and enters bundle-vc configuration mode in order to configure that PVC bundle member.
ubr	Configures UBR QoS and specifies the output peak cell rate for an ATM PVC, SVC, VC class, or VC bundle member.
ubr+	Configures UBR QoS and specifies the output peak cell rate and output minimum guaranteed cell rate for an ATM PVC, SVC, VC class, or VC bundle member.
vc-class atm	Creates a VC class for an ATM PVC, SVC, or ATM interface, and enters vc-class configuration mode.