P through V

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.
log-policy	(Optional) Type of log policy for control-plane logging.
policy-map-name	Name of the policy map.
control	(Optional) Creates a control policy map.

control-name	Name of the control policy map.
service	(Optional) Creates a service policy map.
service-name	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.
unicast-name	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. • 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 groupassignment, use the **no** form of this command.

priority-group *list-number*

no priority-group *list-number*

Syntax Description

list-number	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**showqueueing**and**showinterfaces** 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

level	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. 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.

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

list-number	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-listinterface** 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

list-number	Any number from 1 to 16 that identifies the priority list.
interface-type	The type of the interface.
interface-number	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-listprotocol** 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

list-number	Any number from 1 to 16 that identifies the priority list.
protocol-name	Protocol type: **aarp**, **appletalk**, **arp**, **bridge** (transparent), **clns**, **clns_es**, **clns_is**, **compressedtcp**, **cmns**, **decnet**, **decnet_node**, **decnet_router-l1**, **decnet_router-l2**, **dlsw**, **ip**, **ipx**, **pad**, **rsrb**, **stun**, and **x25**.
high | **medium** | **normal** | **low**	Priority queue level.
queue-keyword keyword-value	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-l1** keyword refers to the multicast address for all level 1 routers, which are intra-area routers, and the **decnet_router-l2** 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 queueing priorities for your system.

Table 1: Protocol Priority Queue Keywords and Values

Option	Description
fragments	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. **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.
gt *byte-count*	Specifies a greater-than count. The priority level assigned goes into effect when a packet size exceeds the value entered for the *byte-count*argument. **Note** The size of the packet must also include additional bytes because of MAC encapsulation on the outgoing interface.
list *list-number*	Assigns traffic priorities according to a specified list when used with AppleTalk, bridging, IP, IPX, VINES, or XNS. The *list-number*argument is the access list number as specified by the**access-list** global configuration command for the specified *protocol-name* . For example, if the protocol is AppleTalk, *list-number* should be a valid AppleTalk access list number.

Option	Description
lt *byte-count*	Specifies a less-than count. The priority level assigned goes into effect when a packet size is less than the value entered for the *byte-count* argument. **Note** The size of the packet must also include additional bytes because of MAC encapsulation on the outgoing interface.
tcp *port*	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 *port*	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 2: 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 3: 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 dlsw high
```

Note This command define 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 thiscommand.

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

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

Syntax Description

list-number	Any number from 1 to 16 that identifies the priority list.
high-limit medium-limit normal-limit low-limit	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 4: Default Priority Queue Packet Limits

Priority Queue Argument	Packet Limits
high-limit	20
medium-limit	40
normal-limit	60
low-limit	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.
policy-map-name	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 *control-policy-name*	(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 5: Configuration Modes Based on Command Application

Application	Mode
Standalone VC	ATM VC submode
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 8021.Q 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-template1” 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-template1
 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

cos-value	Specific IEEE 802.1Q CoS value from 0 to 7.
from-field	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: • **precedence** • **dscp**
table	(Optional) Indicates that the values set in a specified table map will be used to set the CoS value.
table-map-name	(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-nam* e 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 **setqos-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

group-id	Group ID number in the range from 0 to 99.
from-field	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: • **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 *table-map-name*	(Optional) Used in conjunction with the *from-field*argument. Indicates that the values set in a table map specified by *table-map-name*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 **showautodiscoveryqos**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.
type number	(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 **autoqos** 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 **showautodiscoveryqos** 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 6: 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 **showautoqos**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 **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.
type	(Optional) Interface type; valid values are **atm**, **ethernet**, **fastethernet**, **ge-wan**, **gigabitethernet**, **pos**, and**tengigabitethernet**.
slot / *port*	(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 **showautoqosinterface***typeslot/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 7: 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 8: 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 **showpolicy-map**command in user EXEC or privileged EXEC mode.

show policy-map [*policy-map*]

Syntax Description

policy-map	(Optional) Name of the service policy map whose complete configuration is to be displayed. 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	The following modifications were made: • 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	This command was modified to display information about Generic Routing Encapsulation (GRE) tunnel marking. **Note** For this release, GRE-tunnel marking is supported on the Cisco MGX Route Processor Module (RPM-XF) platform *only* .
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 po1. In this example, WFQ is enabled.

```
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)
    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 9: 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-policymap** 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 10: 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 11: 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 12: 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 13: 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 **showpolicy-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 pol1
     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 14: 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 15: 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 16: 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 17: 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	Name of the set command used to set the specified value. 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. 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.

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 18: 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 19: 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**showpolicy-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 20: 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 21: 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 **showpolicy-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-probablity
      ----------------------------------------------------------
      af21 (18)     100              400              1/10
      default (0)   -                -                1/10
```

The table below describes the fields shown in the display.

Table 22: 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: • 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 inEXEC mode.

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

Syntax Description

policy-map	The name of a policy map that contains the class configuration to be displayed.
class-name	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 po1:

```
Router# show policy-map po1 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

slot	(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.
/subslot	(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.

port	(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.
.*subinterface*	(ATM shared port adapter only—Optional) Subinterface number. The number that precedes the period must match the number to which this subinterface belongs. The range is 1 to 4,294,967,293.
type	Type of interface or subinterface whose policy configuration is to be displayed.
type-parameter	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.
vpi /	(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 *vpi* and *vci* 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 *vpi* value defaults the *vpi* value to 0. If this value is omitted, information for all virtual circuits (VCs) on the specified ATM interface or subinterface is displayed.
vci	(Optional) ATM network virtual channel identifier (VCI) for this PVC. This value ranges from 0 to 1 less than the maximum value set for this interface by the **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 *vpi* and *vci* 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.
dlci	(Optional) A specific data-link connection identifier (DLCI) number used on the interface. Policy configuration for the corresponding PVC will be displayed when a DLCI is specified.
input	(Optional) Indicates that the statistics for the attached input policy will be displayed.
output	(Optional) Indicates that the statistics for the attached output policy will be displayed.
class *class-name*	(Optional) Displays the QoS policy actions for the specified class.
interface-type	(Optional) Interface type; possible valid values are **atm**, **ethernet**, **fastethernet**, **ge-wan gigabitethernet**, **pos**, **pseudowire** and **tengigabitethernet**.
interface-number	(Optional) Module and port number; see the "Usage Guidelines" section for valid values.
vlan *vlan-id*	(Optional) Specifies the VLAN ID; valid values are from 1 to 4094.
detailed	(Optional) Displays additional statistics.
port-channel *channel-number*	(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	This command was modified for the Policer Enhancement—Multiple Actions feature and the WRED—Explicit Congestion Notification (ECN) feature. For the Policer Enhancement—Multiple Actions feature, the command was modified to display the multiple actions configured for packets conforming to, exceeding, or violating a specific rate. For the WRED—Explicit Congestion Notification (ECN) feature, the command displays ECN marking information.

Release	Modification
12.2(13)T	The following modifications were made: • This command was modified for the Percentage-Based Policing and Shaping feature. • This command was modified for the Class-Based RTP and TCP Header Compression feature. • This command was modified as part of the Modular QoS CLI (MQC) Unconditional Packet Discard feature. Traffic classes in policy maps can now be configured to discard packets belonging to a specified class. • This command was modified to display the Frame Relay DLCI number as a criterion for matching traffic inside a class map. • This command was modified to display Layer 3 packet length as a criterion for matching traffic inside a class map. • This command was modified for the Enhanced Packet Marking feature. A mapping table (table map) can now be used to convert and propagate packet-marking values.
12.2(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	This command was integrated into Cisco IOS Release 12.2(28)SB, and the following modifications were made: • 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	The following modifications were made: • 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	This command was modified to display information about Generic Routing Encapsulation (GRE) tunnel marking. **Note** As of this release, GRE-tunnel marking is supported on the Cisco MGX Route Processor Module (RPM-XF) platform *only* .
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 *pseudowire* interface type was added.

Release	Modification
Cisco IOS XE Release 3.8S	This command was modified. The *pseudowire* interface type was added on Cisco 1000 Series Routers.
Cisco IOS Release 15.3(1)S	This command was modified. The *pseudowire* 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       Random drop      Tail drop    Minimum Maximum  Mark
          pkts/bytes        pkts/bytes       pkts/bytes    thresh  thresh  prob
0            0/0               0/0              0/0           20      40  1/10
1            0/0               0/0              0/0           22      40  1/10
2            0/0               0/0              0/0           24      40  1/10
3            0/0               0/0              0/0           26      40  1/10
4            0/0               0/0              0/0           28      40  1/10
5            0/0               0/0              0/0           30      40  1/10
6            0/0               0/0              0/0           32      40  1/10
7            0/0               0/0              0/0           34      40  1/10
```

```
rsvp          0/0               0/0              0/0           36      40  1/10
Class-map: class-default (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
```

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 23: 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	Rate, in kbps, of packets coming in to the class. **Note** If the packets are compressed over an outgoing interface, the improved packet rate achieved by packet compression is not reflected in the offered rate. Also, if the packets are classified *before* they enter a combination of tunnels (for example, a generic routing encapsulation (GRE) tunnel and an IP Security (IPSec) tunnel), the offered rate does not include all the extra overhead associated with tunnel encapsulation in general. Depending on the configuration, the offered rate may include no overhead, may include the overhead for only *one* tunnel encapsulation, or may include the overhead for *all* tunnel encapsulations. In most of the GRE and IPSec tunnel configurations, the offered rate includes the overhead for GRE tunnel encapsulation only.
drop rate	Rate, in kbps, at which packets are dropped from the class. The drop rate is calculated by subtracting the number of successfully transmitted packets from the offered rate.
Note In distributed architecture platforms (such as the 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.	
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 *Cisco IOS Quality of Service Solutions Configuration Guide* .
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	Number of packets (also shown in bytes) passed through WRED and not dropped by WRED. **Note** If there is insufficient memory in the buffer to accommodate the packet, the packet can be dropped *after* the packet passes through WRED. Packets dropped because of insufficient memory in the buffer (sometimes referred to as “no-buffer drops”) are not taken into account by the WRED packet counter.

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) x 1
Sustain bits/int	Committed burst (Bc) rate.
Excess bits/int	Excess burst (Be) rate.
Interval (ms)	Time interval value in milliseconds (ms).
Increment (bytes)	Number of credits (in bytes) received in the token bucket of the traffic shaper during each time interval.
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 24: 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 *after* the packet passes through WRED. Packets dropped because of insufficient memory in the buffer (sometimes referred to as "no-buffer drops") are not taken into account by the WRED packet counter.
Random drop pkts/bytes	Number of packets (also shown in bytes) randomly dropped when the mean queue depth is between the minimum threshold value and the maximum threshold value for the specified IP precedence level or DSCP value.
Tail drop pkts/bytes	Number of packets dropped when the mean queue depth is greater than the maximum threshold value for the specified IP precedence level or DSCP value.
Minimum thresh	Minimum threshold. Minimum WRED threshold in number of packets.
Maximum thresh	Maximum threshold. Maximum WRED threshold in number of packets.
Mark prob	Mark probability. Fraction of packets dropped when the average queue depth is at the maximum threshold.

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 25: 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 26: 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 27: 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 28: show policy-map interface Field Descriptions—Configured for ECN

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

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 29: 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	Rate, in kbps, of packets coming in to the class. **Note** If the packets are compressed over an outgoing interface, the improved packet rate achieved by packet compression is not reflected in the offered rate. Also, if the packets are classified *before* they enter a combination of tunnels (for example, a generic routing encapsulation (GRE) tunnel and an IP Security (IPSec) tunnel), the offered rate does not include all the extra overhead associated with tunnel encapsulation in general. Depending on the configuration, the offered rate may include no overhead, may include the overhead for only *one* tunnel encapsulation, or may include the overhead for *all* tunnel encapsulations. In most of the GRE and IPSec tunnel configurations, the offered rate includes the overhead for GRE tunnel encapsulation only.
UDP/RTP Compression	Indicates that RTP header compression has been configured for the class.
Sent total	Count of every packet sent, both compressed packets and full-header packets.
Sent compressed	Count of number of compressed packets sent.
bytes saved	Total number of bytes saved (that is, bytes not needing to be sent).
bytes sent	Total number of bytes sent for both compressed and full-header packets.

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 30: 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	Rate, in kbps, of packets coming in to the class. **Note** If the packets are compressed over an outgoing interface, the improved packet rate achieved by packet compression is not reflected in the offered rate. Also, if the packets are classified *before* they enter a combination of tunnels (for example, a generic routing encapsulation (GRE) tunnel and an IP Security (IPSec) tunnel), the offered rate does not include all the extra overhead associated with tunnel encapsulation in general. Depending on the configuration, the offered rate may include no overhead, may include the overhead for only *one* tunnel encapsulation, or may include the overhead for *all* tunnel encapsulations. In most of the GRE and IPSec tunnel configurations, the offered rate includes the overhead for GRE tunnel encapsulation only.
drop rate	Rate, in kbps, at which packets are dropped from the class. The drop rate is calculated by subtracting the number of successfully transmitted packets from the offered rate.
Note In distributed architecture platforms (such as the 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 *Cisco IOS Quality of Service Solutions Configuration Guide* .
drop	Indicates that the packet discarding action for all the packets belonging to the specified class has been configured.

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 31: 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	Rate, in kbps, of packets coming in to the class. **Note** If the packets are compressed over an outgoing interface, the improved packet rate achieved by packet compression is not reflected in the offered rate. Also, if the packets are classified *before* they enter a combination of tunnels (for example, a generic routing encapsulation (GRE) tunnel and an IP Security (IPSec) tunnel), the offered rate does not include all the extra overhead associated with tunnel encapsulation in general. Depending on the configuration, the offered rate may include no overhead, may include the overhead for only *one* tunnel encapsulation, or may include the overhead for *all* tunnel encapsulations. In most of the GRE and IPSec tunnel configurations, the offered rate includes the overhead for GRE tunnel encapsulation only.
police	Indicates that traffic policing based on a percentage of bandwidth has been enabled. Also, displays the bandwidth percentage, the CIR, and the committed burst (Bc) size in ms.
conformed, actions	Displays the number of packets and bytes marked as conforming to the specified rates, and the action to be taken on those packets.
exceeded, actions	Displays the number of packets and bytes marked as exceeding the specified rates, and the action to be taken on those packets.

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      Byte   Sustain    Excess      Interval  Increment  Adapt
        Rate              Limit  bits/int  bits/int    (ms)     (bytes)   Active
         20 %                        10 (ms)    20 (ms)
        201500/201500       1952   7808       7808        38         976       -
        Queue     Packets   Bytes     Packets   Bytes     Shaping
        Depth                         Delayed   Delayed   Active
        0         0         0         0         0         no
```

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 32: 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	Rate, in kbps, of packets coming in to the class. **Note** If the packets are compressed over an outgoing interface, the improved packet rate achieved by packet compression is not reflected in the offered rate. Also, if the packets are classified *before* they enter a combination of tunnels (for example, a generic routing encapsulation (GRE) tunnel and an IP Security (IPSec) tunnel), the offered rate does not include all the extra overhead associated with tunnel encapsulation in general. Depending on the configuration, the offered rate may include no overhead, may include the overhead for only *one* tunnel encapsulation, or may include the overhead for *all* tunnel encapsulations. In most of the GRE and IPSec tunnel configurations, the offered rate includes the overhead for GRE tunnel encapsulation only.
drop rate	Rate, in kbps, at which packets are dropped from the class. The drop rate is calculated by subtracting the number of successfully transmitted packets from the offered rate.
Match	Match criteria specified for the class of traffic. Choices include criteria such as the Layer 3 packet length, IP precedence, IP DSCP value, MPLS experimental value, access groups, and quality of service (QoS) groups. For more information about the variety of match criteria that are available, see the "Classifying Network Traffic" module in the *Quality of Service Solutions Configuration Guide*.
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	Maximum number of bytes that can be transmitted per interval. Calculated as follows: ((Bc+Be) /8) x 1
Sustain bits/int	Committed burst (Bc) rate.
Excess bits/int	Excess burst (Be) rate.

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 33: 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	Rate, in kbps, of packets coming in to the class. **Note** If the packets are compressed over an outgoing interface, the improved packet rate achieved by packet compression is not reflected in the offered rate. Also, if the packets are classified *before* they enter a combination of tunnels (for example, a generic routing encapsulation (GRE) tunnel and an IP Security (IPSec) tunnel), the offered rate does not include all the extra overhead associated with tunnel encapsulation in general. Depending on the configuration, the offered rate may include no overhead, may include the overhead for only *one* tunnel encapsulation, or may include the overhead for *all* tunnel encapsulations. In most of the GRE and IPSec tunnel configurations, the offered rate includes the overhead for GRE tunnel encapsulation only.
drop rate	Rate, in kbps, at which packets are dropped from the class. The drop rate is calculated by subtracting the number of successfully transmitted packets from the offered rate.
Match	Match criteria specified for the class of traffic. Choices include criteria such as the Layer 3 packet length, IP precedence, IP DSCP value, MPLS experimental value, access groups, and QoS groups.
QoS Set, qos-group, Packets marked	Indicates that class-based packet marking based on the QoS group has been configured. Includes the qos-group number and the number of packets marked.

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 34: 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 *Quality of Service Solutions Configuration Guide*.
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 kbps = 409600 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 kbps = 819200 bps

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

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 ms * 409600 bps = 15360 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 ms * 819200 bps = 40960 bytes

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

Table 35: 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 *Quality of Service Solutions Configuration Guide* .
police	Indicates that traffic policing has been enabled. Display includes the CIR, PIR (in both a percentage of bandwidth and in bps) and the bc and be in bytes and milliseconds. Also displays the optional conform, exceed, and violate actions, if any, and the statistics associated with these optional actions.

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-mapinterface** 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 36: 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 *Cisco IOS Quality of Service Solutions Configuration Guide* .

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 37: 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 *Cisco IOS Quality of Service Solutions Configuration Guide* .
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 38: 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 39: 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 *Cisco IOS Quality of Service Solutions Configuration Guide*.
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 40: 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 *Cisco IOS Quality of Service Solutions Configuration Guide*.
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 41: 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 *Cisco IOS Quality of Service Solutions Configuration Guide*.
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	Differentiated services code point (DSCP). Values can be the following: • 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 42: 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 43: 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 EXECmode.

show queue *interface-name interface-number* [**queue-number**][**vc vpi/ vci**]

Syntax Description

interface-name	The name of the interface.
interface-number	The number of the interface.
queue-number	(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.
vpi /	(Optional) ATM network virtual path identifier (VPI) for this PVC. The absence of the "/" and a *vpi* value defaults the *vpi* value to 0. On the Cisco 7200 and Cisco 7500 series routers, this value ranges from 0 to 255. The *vpi* and *vci* arguments cannot both be set to 0; if one is 0, the other cannot be 0. If this value is omitted, information for all VCs on the specified ATM interface or subinterface is displayed.

vci	(Optional) ATM network virtual channel identifier (VCI) for this PVC. This value ranges from 0 to 1 less than the maximum value set for this interface by the **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. The VCI is a 16-bit field in the header of the ATM cell. The VCI value is unique only on a single link, not throughout the ATM network, because it has local significance only. The *vpi* and *vci* arguments cannot both be set to 0; if one is 0, the other cannot be 0.

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 44: 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 45: 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 **showqueue**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 *atm-subinterface*	(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.

vpi /	(Optional) Specifies the VPI. If the *vpi* argument is omitted, 0 is used as the VPI value for locating the permanent virtual circuit (PVC). If the *vpi* argument is specified, the/separator is required.
vci	(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 **showqueueing**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 **showqueueing** 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 **showqueueingcustom** 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**showqueueingrandom-detect** command. The output shows that the interface is configured for flow-based WRED to ensure fair packet drop among flows. The **random-detectflowaverage-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-detectflowcount**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       Tail    Minimum    Maximum     Mark
                  drop       drop  threshold  threshold  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 **showqueueingrandom-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       Tail    Minimum    Maximum     Mark
                  drop       drop  threshold  threshold  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 46: 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

type number	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.
vpi /	(Optional) The VPI. If the *vpi* argument is omitted, 0 is used as the VPI value for locating the permanent virtual circuit (PVC). If the *vpi* argument is specified, the/separator is required.
vci	(Optional) The VCI.
null 0	Specifies the null interface number; the only valid value is 0.
vlan *vlan-id*	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-waninterfaces 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 **showqueueinginterface** command does not display the absolute values that are programmed in the hardware. Use the **showqm-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 **showqueueinginterfacedetailed** 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 **showqueueinginterface**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 47: 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 **showqueueinginterface**command in Cisco IOS Release 12.2(33)SXI and later releases:

```
Router# show queueing interface gigabitethernet 3/27 detailed

.
.
.
  Packets dropped on Transmit:
    BPDU packets:  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      555555 / 666666    233333 / 340000          [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 48: show queueing interface detailed Field Descriptions

Field	Description
Packets dropped on Transmit	Displays information regarding the packets dropped in transmission.
BPDU packets	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

output-pcr	The output PCR, in kilobytes per second (kbps).
output-scr	The output SCR, in kbps.
output-maxburstsize	The output maximum burst cell size, expressed in number of cells.
input-pcr	(Optional for SVCs only) The input PCR, in kbps.
input-scr	(Optional for SVCs only) The input SCR, in kbps.
input-maxburstsize	(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-classatm** 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.