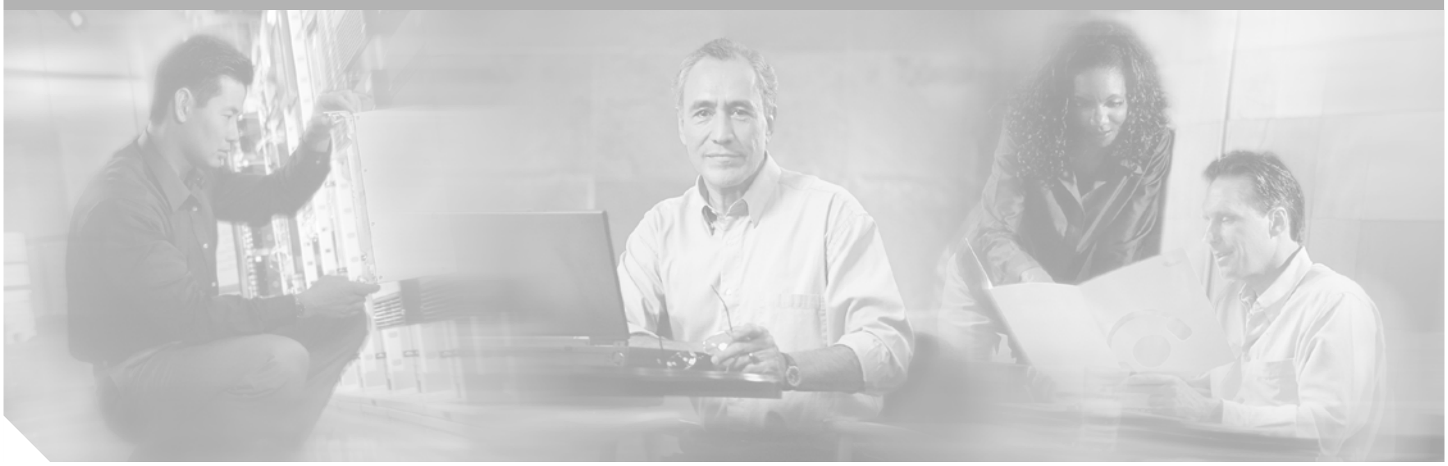
CISCO SYSTEMS



Cisco IOS
Quality of Service Solutions
Command Reference

Release 12.2 T

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

CONTENTS

Quality of Service Commands

Use the commands in this chapter to configure quality of service (QoS), a measure of performance for a transmission system that reflects its transmission quality and service availability. The commands are arranged alphabetically.

For QoS configuration information and examples, refer to the *Cisco IOS Quality of Service Solutions Configuration Guide*.

access-list rate-limit

To configure an access list for use with committed access rate (CAR) policies, use the **access-list rate-limit** command in global configuration mode. To remove the access list from the configuration, use the **no** form of this command.

access-list rate-limit *acl-index* {*precedence* | *mac-address* | *exp* | **mask** *mask*}

no access-list rate-limit *acl-index* {*precedence* | *mac-address* | *exp* | **mask** *mask*}

Syntax Description

acl-index	Access list number. To classify packets by • IP precedence, use any number from 1 to 99 • MAC address, use any number from 100 to 199 • Multiprotocol Label Switching (MPLS) experimental field, use any number from 200 to 299
precedence	IP precedence. Valid values are numbers from 0 to 7.
mac-address	MAC address.
exp	MPLS experimental field. Valid values are numbers from 0 to 7.
mask *mask*	Mask. Use this option if you want to assign multiple IP precedences or MPLS experimental field values to the same rate-limit access list.

Defaults

No CAR access lists are configured.

Command Modes

Global configuration

Command History

Release	Modification
11.1 CC	This command was introduced.
12.1(5)T	This command now includes an access list based on the MPLS experimental field.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(4)T	This command was implemented on the Cisco MGX 8850 switch and the MGX 8950 switch with a Cisco MGX RPM-PR card.
12.2(4)T2	This command was implemented on the Cisco 7500 series.

Usage Guidelines

Use this command to classify packets by the specified IP precedence, MAC address, or MPLS experimental field values for a particular CAR access list. You can then apply CAR policies, using the **rate-limit** command, to individual rate-limit access lists. When packets in an access list are classified in this manner, the packets with different IP precedences, MAC addresses, or MPLS experimental field values are treated differently by the CAR process.

You can specify only one command for each rate-limit access list. If you enter this command multiple times using the same access list number, the new command overwrites the previous command.

Use the **mask** keyword to assign multiple IP precedences or MPLS experimental field values to the same rate-limit list. To ascertain the **mask** value, perform the following steps:

Step 1 Decide which precedences you want to assign to this rate-limit access list.

Step 2 Convert the precedences or MPLS experimental field values into 8-bit numbers with each bit corresponding to one value. For example, an MPLS experimental field value of 0 corresponds to 00000001; 1 corresponds to 00000010; 6 corresponds to 01000000; and 7 corresponds to 10000000.

Step 3 Add the 8-bit numbers for the selected MPLS experimental field values. For example, the mask for MPLS experimental field values 1 and 6 is 01000010.

Step 4 The **access-list rate-limit** command expects hexadecimal format. Convert the binary mask into the corresponding hexadecimal number. For example, 01000010 becomes 42 and is used in the command. Any packets that have an MPLS experimental field value of 1 or 6 will match this access list.

A mask of FF matches any precedence, and 00 does not match any precedence.

Examples

In the following example, MPLS experimental fields with the value of 7 are assigned to the rate-limit access list 200:

```
Router(config)# access-list rate-limit 200 7
```

You can then use the rate-limit access list in a **rate-limit** command so that the rate limit is applied only to packets matching the rate-limit access list.

```
Router(config)# interface atm4/0.1 mpls
Router(config-if)# rate-limit input access-group rate-limit 200 8000 8000 8000
conform-action set-mpls-exp-transmit 4 exceed-action set-mpls-exp-transmit 0
```

Related Commands

Command	Description
rate-limit	Configures CAR and DCAR policies.
show access-lists rate-limit	Displays information about rate-limit access lists.

auto qos voip

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

auto qos voip [**trust**] [**fr-atm**]

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

Syntax Description

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

Defaults

No default behavior or values

Command Modes

Interface configuration

Frame Relay DLCI configuration (for use with Frame Relay DLCIs)

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

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

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

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

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

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

These policy maps should not be attached to an interface or PVC by using the **service-policy** command. If the policy maps are attached in this manner, the AutoQoS — VoIP feature (that is, the policy maps, class maps, and access control lists (ACLs)) will not be removed properly when the **no auto qos voip** command is configured.

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

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

The **auto qos voip** command is not supported on subinterfaces.

The **auto qos voip** command is available for Frame Relay DLCIs.

Disabling AutoQoS — VoIP

The **no auto qos voip** command disables the AutoQoS — VoIP feature and removes the configurations associated with the feature.

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

Note If you delete a subinterface or PVC (either ATM or Frame Relay PVCs) without configuring the **no auto qos voip** command, the AutoQoS — VoIP feature will not be removed properly.

Examples

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

```
Router> enable
Router# configure terminal
Router(config)# interface s4/1.2 point-to-point
Router(config-if)# bandwidth 100
Router(config-if)# ip address 192.168.0.0 255.255.255.0
Router(config-if)# frame-relay interface-dlci 102
Router(config-fr-dlci)# auto qos voip trust fr-dlci
Router(config-if# exit
```

Related Commands

Command	Description
service policy	Attaches a policy map to an input interface or VC, or an output interface or VC, to be used as the service policy for that interface or VC.
show auto qos	Displays the configurations created by the AutoQoS — VoIP feature on a specific interface or all interfaces.

bandwidth (policy-map class)

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

bandwidth {*bandwidth-kbps* | **remaining percent** *percentage* | **percent** *percentage*}

no bandwidth {*bandwidth-kbps* | **remaining percent** *percentage* | **percent** *percentage*}

Syntax Description

bandwidth-kbps	Amount of bandwidth, in number of kbps, to be assigned to the class. The amount of bandwidth varies according to the interface and platform in use.
remaining percent	Amount of guaranteed bandwidth, based on a relative percent of available bandwidth.
percentage	Used in conjunction with the **remaining percent** keyword, a percentage. The percentage can be a number from 1 to 100.
percent	Amount of guaranteed bandwidth, based on an absolute percent of available bandwidth.
percentage	Used in conjunction with the **percent** keyword, the percentage of the total available bandwidth to be set aside for the priority class. The percentage can be a number from 1 to 100.

Defaults

No default behavior or values

Command Modes

Policy-map class configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(5)XE	This command was incorporated into Cisco IOS Release 12.0(5)XE. Support for Versatile Interface Processor (VIP)-enabled Cisco 7500 series routers was added.
12.0(7)T	The **percent** keyword was added.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T. Support for VIP-enabled Cisco 7500 series routers was added.
12.2(2)T	The **remaining percent** keyword was added.

Usage Guidelines

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

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

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

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

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

For more information on bandwidth allocation, refer to the chapter "Congestion Management Overview" in the *Cisco IOS Quality of Service Solutions Configuration Guide,* Release 12.2.

Examples

CBWFQ Bandwidth Guarantee Example

The following example illustrates how bandwidth is guaranteed when only CBWFQ is configured:

```
! The following commands create a policy map with two classes:
policy-map policy1
 class class1
  bandwidth percent 50
  exit

 class class2
  bandwidth percent 25
  exit
 end

!The following commands attach the policy to interface s3/2:
interface s3/2
 service output policy1
 end
```

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

```
Router# show policy-map policy1

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

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

```
Router# show policy-map interface s3/2

 Serial3/2

  Service-policy output:policy1

    Class-map:class1 (match-all)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match:none
      Weighted Fair Queueing
        Output Queue:Conversation 265
        Bandwidth 50 (%)
        Bandwidth 772 (kbps) Max Threshold 64 (packets)
        (pkts matched/bytes matched) 0/0
        (depth/total drops/no-buffer drops) 0/0/0

    Class-map:class2 (match-all)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match:none
      Weighted Fair Queueing
        Output Queue:Conversation 266
        Bandwidth 25 (%)
        Bandwidth 386 (kbps) Max Threshold 64 (packets)
        (pkts matched/bytes matched) 0/0
        (depth/total drops/no-buffer drops) 0/0/0

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

In this example, interface s3/2 has a total bandwidth of 1544 kbps. During periods of congestion, 50 percent (or 772 kbps) of the bandwidth is guaranteed to the class called class1, and 25 percent (or 386 kbps) of the link bandwidth is guaranteed to the class called class2.

CBWFQ and LLQ Bandwidth Allocation Example

The following output from the **show policy-map** command shows the configuration for a policy map called p1:

```
Router# show policy-map p1

  Policy Map p1
    Class voice
      Weighted Fair Queueing
            Strict Priority
            Bandwidth 500 (kbps) Burst 12500 (Bytes)
    Class class1
      Weighted Fair Queueing
            Bandwidth remaining 50 (%) Max Threshold 64 (packets)
    Class class2
      Weighted Fair Queueing
            Bandwidth remaining 25 (%) Max Threshold 64 (packets)
```

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

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

```
Router# show policy-map interface s3/2

 Serial3/2

  Service-policy output:p1

    Class-map:voice (match-all)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match:ip precedence 5
      Weighted Fair Queueing
        Strict Priority
        Output Queue:Conversation 264
        Bandwidth 500 (kbps) Burst 12500 (Bytes)
        (pkts matched/bytes matched) 0/0
        (total drops/bytes drops) 0/0

    Class-map:class1 (match-all)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match:none
      Weighted Fair Queueing
        Output Queue:Conversation 265
        Bandwidth remaining 50 (%) Max Threshold 64 (packets)
        (pkts matched/bytes matched) 0/0
        (depth/total drops/no-buffer drops) 0/0/0
```

```
Class-map:class2 (match-all)
  0 packets, 0 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
  Match:none
  Weighted Fair Queueing
    Output Queue:Conversation 266
    Bandwidth remaining 25 (%) Max Threshold 64 (packets)
    (pkts matched/bytes matched) 0/0
    (depth/total drops/no-buffer drops) 0/0/0

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

Related Commands

Command	Description
class (policy-map)	Specifies the name of the class whose policy you want to create or change, and the default class (commonly known as the class-default class) before you configure its policy.
class-map	Creates a class map to be used for matching packets to a specified class.
max-reserved-bandwidth	Changes the percent of interface bandwidth allocated for CBWFQ, LLQ, and IP RTP Priority.
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
queue-limit	Specifies or modifies the maximum number of packets the queue can hold for a class policy configured in a policy map.
random-detect (interface)	Enables WRED or DWRED.
random-detect exponential-weighting-constant	Configures the WRED and DWRED exponential weight factor for the average queue size calculation.
random-detect precedence	Configures WRED and DWRED parameters for a particular IP precedence.
show policy-map	Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps.
show policy-map interface	Displays the packet statistics of all classes that are configured for all service policies either on the specified interface or subinterface or on a specific PVC on the interface.

bump

To configure the bumping rules for a virtual circuit (VC) class that can be assigned to a VC bundle, use the **bump** command in VC-class configuration mode. To remove the explicit bumping rules for the VCs assigned to this class and return to the default condition of implicit bumping, use the **no bump explicit** command or the **bump implicit** command. To specify that the VC bundle members do not accept any bumped traffic, use the **no** form of this command.

To configure the bumping rules for a specific VC or permanent virtual circuit (PVC) member of a bundle, use the **bump** command in bundle-vc or SVC (switched virtual circuit)-bundle-member configuration mode. To remove the explicit bumping rules for the VC or PVC bundle member and return to the default condition of implicit bumping, use the **bump implicit** command. To specify that the VC or PVC bundle member does not accept any bumped traffic, use the **no bump traffic** command.

bump {**explicit** *precedence-level* | **implicit** | **traffic**}

no bump {**explicit** *precedence-level* | **implicit** | **traffic**}

Syntax Description

explicit *precedence-level*	Specifies the precedence level to which traffic on a VC or PVC will be bumped when the VC or PVC goes down. Valid values for the *precedence-level* argument are numbers from 0 to 7.
implicit	Applies the implicit bumping rule, which is the default, to a single VC or PVC bundle member or to all VCs in the bundle (VC-class mode). The implicit bumping rule stipulates that bumped traffic is to be carried by a VC or PVC with a lower precedence level.
traffic	Specifies that the VC or PVC accepts bumped traffic (the default condition). The **no** form stipulates that the VC or PVC does not accept any bumped traffic.

Defaults

Implicit bumping

Permit bumping (VCs accept bumped traffic)

Command Modes

VC-class configuration (for a VC class)

Bundle-vc configuration (for an ATM VC bundle member)

SVC-bundle-member configuration (for an SVC bundle member)

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.2(4)T	This command was made available in SVC-bundle-member configuration mode.
12.0(23)S	This command was made available in vc-class and bundle-vc configuration modes on the 8-port OC-3 STM-1 ATM line card for Cisco 12000 series Internet routers.

Usage Guidelines

Use the **bump** command in bundle-vc configuration mode (for an ATM VC bundle member), SVC-bundle-member configuration mode (for an SVC bundle member) to configure bumping rules for a discrete VC or PVC bundle member. Use the **bump** command in vc-class configuration mode to configure a VC class that can be assigned to a bundle member.

The effects of different bumping configuration approaches are as follows:

- Implicit bumping: If you configure implicit bumping, bumped traffic is sent to the VC or PVC configured to handle the next lower precedence level. When the original VC or PVC that bumped the traffic comes back up, the traffic that it is configured to carry is restored to it. If no other positive forms of the **bump** command are configured, the **bump implicit** command takes effect.
- Explicit bumping: If you configure a VC or PVC with the **bump explicit** command, you can specify the precedence level to which traffic will be bumped when that VC or PVC goes down, and the traffic will be directed to a VC or PVC mapped with that precedence level. If the VC or PVC that picks up and carries the traffic goes down, the traffic is subject to the bumping rules for that VC or PVC. You can specify only one precedence level for bumping.
- Permit bumping: The VC or PVC accepts bumped traffic by default. If the VC or PVC has been previously configured to reject bumped traffic, you must use the **bump traffic** command to return the VC or PVC to its default condition.
- Reject bumping: To configure a discrete VC or PVC to reject bumped traffic when the traffic is directed to it, use the **no bump traffic** command.

Note When no alternative VC or PVC can be found to handle bumped traffic, the bundle is declared down. To avoid this occurrence, configure explicitly the bundle member VC or PVC that has the lowest precedence level.

To use this command in VC-class configuration mode, you must enter the **vc-class atm** global configuration command before you enter this command.

To use this command to configure an individual bundle member in bundle-VC configuration mode, first issue the **bundle** command to enter bundle configuration mode for the bundle to which you want to add or modify the VC member to be configured. Then use the **pvc-bundle** command to specify the VC to be created or modified and enter bundle-vc configuration mode.

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. In this case, the attributes are ignored by the VC.

VCs in a VC bundle are subject to the following configuration inheritance guidelines (listed in order of next-highest precedence):

- VC configuration in bundle-vc mode
- Bundle configuration in bundle mode (with effect of assigned VC-class configuration)

- Subinterface configuration in subinterface mode

Examples

The following example configures the class called “five” to define parameters applicable to a VC in a bundle. If the VC goes down, traffic will be directed (bumped explicitly) to a VC mapped with precedence level 7.

```
vc-class atm five
 ubr 5000
 precedence 5
 bump explicit 7
```

The following example configures the class called “premium-class” to define parameters applicable to a VC in a bundle. Unless overridden with a bundle-vc **bump** configuration, the VC that uses this class will not allow other traffic to be bumped onto it.

```
vc-class atm premium-class
  no bump traffic
  bump explicit 7
```

Related Commands

Command	Description
class	Assigns a map-class or VC-class to a PVC or PVC bundle member.
class-vc	Assigns a VC class to an ATM PVC, SVC, or VC bundle member.
dscp (frame-relay vc-bundle-member)	Specifies the DSCP value or values for a specific Frame Relay PVC bundle member.
precedence	Configures precedence levels for a VC or PVC class that can be assigned to a VC or PVC bundle and thus applied to all members of that bundle.
protect	Configures a VC or PVC class with protected group or protected VC or PVC status for application to a VC or PVC bundle member.
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.
pvc (frame-relay vc-bundle)	Creates a PVC and PVC bundle member and enters frame-relay vc-bundle-member configuration mode.
svc-bundle	Creates or modifies a member of an SVC bundle.
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.
vbr-nrt	Configures the VBR-NRT QoS and specifies output peak cell rate, output sustainable cell rate, and output maximum burst cell size for an ATM PVC, SVC, VC class, or VC bundle member.
vc-class atm	Configures a VC class or an ATM VC or interface.

bundle

To create a bundle or modify an existing bundle to enter bundle configuration mode, use the **bundle** command in subinterface configuration mode. To remove the specified bundle, use the **no** form of this command.

bundle *bundle-name*

no bundle *bundle-name*

Syntax Description

bundle-name	Specifies the name of the bundle to be created. Limit is 16 alphanumeric characters.

Defaults

No default behavior or values

Command Modes

Subinterface configuration

Command History

Release	Modification
12.0(3)T	This command was introduced.

Usage Guidelines

From within bundle configuration mode you can configure the characteristics and attributes of the bundle and its members, such as the encapsulation type for all virtual circuits (VCs) in the bundle, the bundle management parameters, the service type, and so on. Attributes and parameters you configure in bundle configuration mode are applied to all virtual circuit (VC) members of the bundle.

VCs in a VC bundle are subject to the following configuration inheritance guidelines (listed in order of next highest precedence):

- VC configuration in bundle-vc mode
- Bundle configuration in bundle mode
- Subinterface configuration in subinterface mode

To display status on bundles, use the **show atm bundle** and **show atm bundle statistics** commands.

Examples

The following example configures a bundle called new-york. The example specifies the IP address of the subinterface and the router protocol—the router uses Intermediate System-to-Intermediate System (IS-IS) as an IP routing protocol—then configures the bundle.

```
interface a1/0.1 multipoint
  ip address 10.0.0.1 255.255.255.0
  ip router isis
  bundle new-york
```

Related Commands

Command	Description
class-bundle	Configures a VC bundle with the bundle-level commands contained in the specified VC class.
oam-bundle	Enables end-to-end F5 OAM loopback cell generation and OAM management for all VC members of a bundle, or for a VC class that can be applied to a VC bundle.
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.
show atm bundle	Displays the bundle attributes assigned to each bundle VC member and the current working status of the VC members.
show atm bundle statistics	Displays statistics on the specified bundle.

bundle svc

To create or modify a switched virtual circuit (SVC) bundle, use the **bundle svc** command in interface configuration mode. To remove the specified bundle, use the **no** form of this command.

bundle svc *bundle-name* **nsap** *nsap-address*

no bundle svc *bundle-name* **nsap** *nsap-address*

Syntax Description

bundle-name	Unique bundle name that identifies the SVC bundle in the router. The bundle names at each end of the virtual circuit (VC) must be the same. Length limit is 16 alphanumeric characters.
nsap *nsap-address*	Destination network services access point (NSAP) address of the SVC bundle.

Defaults

No SVC bundle is created or modified.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(4)T	This command was introduced.

Usage Guidelines

This command causes the system to enter SVC-bundle configuration mode. The bundle name must be the same on both sides of the VC.

From SVC-bundle configuration mode, you can configure the characteristics and attributes of the bundle and its members, such as the encapsulation type for all virtual circuits (VCs) in the bundle, the bundle management parameters, the service type, and so on. Attributes and parameters you configure in SVC-bundle configuration mode are applied to all VC members of the bundle.

VCs in a VC bundle are subject to the following configuration inheritance guidelines (listed in order of next-highest precedence):

- VC configuration in bundle-VC mode
- Bundle configuration in bundle mode
- Subinterface configuration in subinterface mode

To display the status of bundles, use the **show atm bundle svc** and **show atm bundle svc statistics** commands.

Examples

The following example configures an SVC bundle called “sanfrancisco”:

```
interface ATM1/0.1 multipoint
 ip address 170.100.9.2 255.255.255.0
 atm esi-address 111111111111.11
 bundle svc sanfrancisco nsap 47.0091810000000003E3924F01.999999999999.99
  protocol ip 170.100.9.1
broadcast
  oam retry 4 3 10
  encapsulation aal5snap
  oam-bundle manage
  svc-bundle seven
   class-vc seven
  svc-bundle six
   class-vc six
  svc-bundle five
   class-vc five
  svc-bundle four
   class-vc four
  svc-bundle three
   class-vc three
  svc-bundle two
   class-vc two
  svc-bundle one
   class-vc one
  svc-bundle zero
   class-vc zero
```

Related Commands

Command	Description
class-bundle	Configures a VC bundle with the bundle-level commands contained in the specified VC class.
oam-bundle	Enables end-to-end F5 OAM loopback cell generation and OAM management for all VC members of a bundle, or for a VC class that can be applied to a VC bundle.
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.
show atm bundle svc	Displays the bundle attributes assigned to each bundle VC member and the current working status of the VC members.
show atm bundle svc statistics	Displays statistics on the specified bundle.

class (policy-map)

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

class {*class-name* | **class-default**}

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

Syntax Description

class-name	The name of the class for which you want to configure or modify policy.
class-default	Specifies the default class so that you can configure or modify its policy.

Defaults

No default behavior or values

Command Modes

QoS policy-map configuration

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.

Usage Guidelines

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

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

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

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

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

The predefined default class called class-default is the class to which traffic is directed if that traffic does not satisfy the match criteria of other classes whose policy is defined in the policy map.

You can define a class policy to use either tail drop (by using the **queue-limit** command) or Weighted Random Early Detection (WRED) packet drop (by using the **random-detect** command). The **queue-limit** and **random-detect** commands cannot be used in the same class policy, but they can be used in two class policies in the same policy map.

You can configure the **bandwidth** command when either the **queue-limit** or the **random-detect** command is configured in a class policy. The **bandwidth** command specifies the amount of bandwidth allocated for the class.

For the default class, you can configure the **fair-queue** (class-default) command. The **fair-queue** command specifies the number of dynamic queues for the default class. The **fair-queue** command can be used in the same class policy as either the **queue-limit** or **random-detect** command. It cannot be used with the **bandwidth** command.

Examples

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

```
! The following commands create class-maps class1 and class2
! and define their match criteria:
class-map class1
 match access-group 136
class-map class2
 match input-interface ethernet101

! The following commands create the policy map, which is defined to contain policy
! specification for class1, class2, and the default class:
policy-map policy1

class class1
 bandwidth 2000
 queue-limit 40

class class2
 bandwidth 3000
 random-detect
 random-detect exponential-weighting-constant 10

class class-default
 fair-queue 16
 queue-limit 20
```

Class1 has these characteristics: A minimum of 2000 kbps of bandwidth are expected to be delivered to this class in the event of congestion, and the queue reserved for this class can enqueue 40 packets before tail drop is enacted to handle additional packets.

Class2 has these characteristics: A minimum of 3000 kbps of bandwidth are expected to be delivered to this class in the event of congestion, and a weight factor of 10 is used to calculate the average queue size. For congestion avoidance, WRED packet drop is used, not tail drop.

The default class has these characteristics: 16 dynamic queues are reserved for traffic that does not meet the match criteria of other classes whose policy is defined by the policy map called policy1, and a maximum of 20 packets per queue are enqueued before tail drop is enacted to handle additional packets.

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

The following example configures policy for the default class included in the policy map called policy2. The default class has these characteristics: 20 dynamic queues are available for traffic that does not meet the match criteria of other classes whose policy is defined by the policy map called policy2, and a weight factor of 14 is used to calculate the average queue size. For congestion avoidance, WRED packet drop is used, not tail drop.

```
policy-map policy2
class class-default
 fair-queue 20
 random-detect
 random-detect exponential-weighting-constant 14
```

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

```
policy-map policy1
class acl136
bandwidth 2000
queue-limit 40
```

The following example configures policy for a class called int101 included in the policy map called policy8. Class int101 has these characteristics: a minimum of 3000 kbps of bandwidth are expected to be delivered to this class in the event of congestion, and a weight factor of 10 is used to calculate the average queue size. For congestion avoidance, WRED packet drop is used, not tail drop. Note that when the policy map containing this class is attached to the interface to stipulate the service policy for that interface, available bandwidth is assessed.

```
policy-map policy8
class int101
bandwidth 3000
random-detect exponential-weighting-constant 10
```

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

```
policy-map policy1
class class-default
fair-queue 10
queue-limit 20
```

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

```
policy-map policy8
class class-default
fair-queue 20
random-detect exponential-weighting-constant 14
```

Related Commands

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

class-bundle

To configure a virtual circuit (VC) bundle with the bundle-level commands contained in the specified VC class, use the **class-bundle** command in bundle or SVC (switched virtual circuit)-bundle configuration mode. To remove the VC class parameters from a VC bundle, use the **no** form of this command.

class-bundle *vc-class-name*

no class-bundle *vc-class-name*

Syntax Description

vc-class-name	Name of the VC class that you are assigning to your VC bundle.

Defaults

No VC class is assigned to the VC bundle.

Command Modes

Bundle configuration

SVC-bundle configuration

Command History

Release	Modification
12.0 T	This command was introduced, replacing the **class** command for configuring ATM VC bundles.
12.2(4)T	This command was made available in SVC-bundle configuration mode.

Usage Guidelines

To use this command, you must first enter the **bundle** or **bundle svc** command to create the bundle and enter bundle or SVC-bundle configuration mode.

Use this command to assign a previously defined set of parameters (defined in a VC class) to an ATM VC bundle. Parameters set through bundle-level commands that are contained in a VC class are applied to the bundle and its VC members.

You can add the following commands to a VC class to be used to configure a VC bundle: **broadcast**, **encapsulation**, **inarp, oam-bundle**, **oam retry,** and **protocol**.

Bundle-level parameters applied through commands that are configured directly on a bundle supersede bundle-level parameters applied through a VC class by the **class-bundle** command. Some bundle-level parameters applied through a VC class or directly to the bundle can be superseded by commands that you directly apply to individual VCs in bundle-VC configuration mode.

Examples

In the following example, a class called “class1” is created and then applied to the bundle called “bundle1:”

```
! The following commands create the class class1:
vc-class atm class1
 encapsulation aal5snap
 broadcast
```

```
 protocol ip inarp
 oam-bundle manage 3
 oam 4 3 10

! The following commands apply class1 to the bundle called bundle1:
bundle bundle1
 class-bundle class1
```

With hierarchy precedence rules taken into account, VCs belonging to the bundle “bundle1” will be characterized by these parameters: aal5snap, encapsulation, broadcast on, use of Inverse Address Resolution Protocol (Inverse ARP) to resolve IP addresses, and Operation, Administration, and Maintenance (OAM) enabled.

Related Commands

Command	Description
broadcast	Configures broadcast packet duplication and transmission for an ATM VC class, PVC, SVC, or VC 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.
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 all VC members of a bundle, or for a VC class that can be applied to a VC bundle.
oam retry	Configures parameters related to OAM management for an ATM PVC, SVC, VC class, or VC bundle.
protocol (ATM)	Configures a static map for an ATM PVC, SVC, VC class, or VC bundle. Enables Inverse ARP or Inverse ARP broadcasts on an ATM PVC by configuring Inverse ARP either 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.

class-map

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

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

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

Syntax Description

class-map-name	Name of the class for the class map. The name can be a maximum of 40 alphanumeric characters. The class name is used for both the class map and to configure policy for the class in the policy map.
match-all | **match-any**	(Optional) Determines how packets are evaluated when multiple match criteria exist. Packets must either meet all of the match criteria (**match-all**) or one of the match criteria (**match-any**) in order to be considered a member of the class.

Defaults

No default behavior or values

Command Modes

Global configuration

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.

Usage Guidelines

Use this command to specify the name of the class for which you want to create or modify class map match criteria. Use of the **class-map** command enables class-map configuration mode in which you can enter one of the match commands to configure the match criteria for this class. Packets arriving at the output interface are checked against the match criteria configured for a class map to determine if the packet belongs to that class.

You can use one of the following commands in a class map:

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

If you specify more than one command in the class map, only the last command entered applies. The last command overrides the previously entered commands. For more information about match criteria and the Modular Quality of Service Command-Line Interface (CLI), refer to the *Cisco IOS Quality of Service Solutions Configuration Guide*.

Examples

The following example specifies class101 as the name of a class, and it defines a class map for this class. The class called class101 specifies policy for traffic that matches access control list 101.

```
class-map class101
  match access-group 101
```

Related Commands

Command	Description
class (policy-map)	Specifies the name of the class whose policy you want to create or change, and the default class (commonly known as the class-default class) before you configure its policy.
class class-default	Specifies the default class for a service policy map.
match access-group	Configures the match criteria for a class map on the basis of the specified ACL.
match input-interface	Configures a class map to use the specified input interface as a match criterion.
match mpls experimental	Configures a class map to use the specified EXP field value as a match criterion.
match protocol	Configures the match criteria for a class map on the basis of the specified protocol.
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.

clear ip rsvp authentication

To eliminate Resource Reservation Protocol (RSVP) security associations before their lifetimes expire, use the **clear ip rsvp authentication** command in EXEC mode.

clear ip rsvp authentication [*ip-address* | *hostname*]

Syntax Description

ip-address	(Optional) Frees security associations with a specific neighbor.
hostname	(Optional) Frees security associations with a specific host.

Note The difference between *ip-address* and *hostname* is the difference of specifying the neighbor by its ip address or by its name.

Defaults

The default behavior is to clear all security associations.

Command Modes

EXEC

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

Use the **clear ip rsvp authentication** command for the following reasons:

- To eliminate security associations before their lifetimes expire
- To free up memory
- To resolve a problem with a security association being in some indeterminate state
- To force reauthentication of neighbors

You can delete all RSVP security associations if you do not enter an IP address or a host name, or just the ones with a specific RSVP neighbor or host.

If you delete a security association, it is re-created as needed when the trusted RSVP neighbors start sending more RSVP messages.

Examples

The following command shows how to clear all security associations before they expire:

```
Router# clear ip rsvp authentication
```

Related Commands

Command	Description
ip rsvp authentication lifetime hh:mm:ss	Controls how long RSVP maintains security associations with other trusted RSVP neighbors.
show ip rsvp authentication	Displays the security associations that RSVP has established with other RSVP neighbors.

clear ip rsvp counters

To clear (set to zero) all IP Resource Reservation Protocol (RSVP) counters that are being maintained by the router, use the **clear ip rsvp counters** command in EXEC mode.

clear ip rsvp counters [**confirm**]

Syntax Description

confirm	(Optional) Requests a confirmation that all IP RSVP counters were cleared.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
12.0(14)ST	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines

Use the **clear ip rsvp counters** command to reset all IP RSVP counters to zero so that you can see changes easily.

Examples

The following command shows that all IP RSVP counters that are being maintained are cleared:

```
Router# clear ip rsvp counters

Clear rsvp counters [confirm]
```

Note The following sample outputs show how you can use the **show ip rsvp counters** and the **clear ip rsvp counters** commands together.

The following command shows the non-zero counters for the interfaces that have RSVP enabled:

```
Router# show ip rsvp counters

POS0/0                  Recv      Xmit                          Recv      Xmit
    Path                   0       300    Resv                   371         0
    PathError              0         0    ResvError                0         0
    PathTear               0       150    ResvTear                 0         0
    ResvConf               0         0    RTearConf                0         0
    Ack                   20        28    Srefresh                10        10
    DSBM_WILLING           0         0    I_AM_DSBM                0         0
    Unknown                0         0    Errors                   0         0
POS1/0                  Recv      Xmit                          Recv      Xmit
    Path                 300         0    Resv                     0       300
    PathError              0         0    ResvError                0         0
    PathTear             150         0    ResvTear                 0         0
    ResvConf               0         0    RTearConf                0         0
```

```
DSBM_WILLING            0          0     I_AM_DSBM               0          0
    Unknown                 0          0     Errors                  0          0
POS1/3                  Recv       Xmit                          Recv       Xmit
    Path                    0          0     Resv                    0          0
    PathError               0          0     ResvError               0          0
    PathTear                0          0     ResvTear                0          0
    ResvConf                0          0     RTearConf               0          0
    Ack                     0          0     Srefresh                0          0
    DSBM_WILLING            0          0     I_AM_DSBM               0          0
    Unknown                 0          0     Errors                  0          0
Loopback0               Recv       Xmit                          Recv       Xmit
    Path                    0          0     Resv                    0          0
    PathError               0          0     ResvError               0          0
    PathTear                0          0     ResvTear                0          0
    ResvConf                0          0     RTearConf               0          0
    Ack                     0          0     Srefresh                0          0
    DSBM_WILLING            0          0     I_AM_DSBM               0          0
    Unknown                 0          0     Errors                  0          0
Non RSVP i/f's          Recv       Xmit                          Recv       Xmit
    Path                    0          0     Resv                    0          0
    PathError               0          0     ResvError               0          0
    PathTear                0          0     ResvTear                0          0
    ResvConf                0          0     RTearConf               0          0
    Ack                     0          0     Srefresh                0          0
    DSBM_WILLING            0          0     I_AM_DSBM               0          0
    Unknown                 0          0     Errors                  0          0
All Interfaces          Recv       Xmit                          Recv       Xmit
    Path                    0          0     Resv                    0          0
    PathError               0          0     ResvError               0          0
    PathTear                0          0     ResvTear                0          0
    ResvConf                0          0     RTearConf               0          0
    Ack                     0          0     Srefresh                0          0
    DSBM_WILLING            0          0     I_AM_DSBM               0          0
    Unknown                 0          0     Errors                  0          0
```

Table 1 describes the fields shown in the display.

Table 1 show ip rsvp counters Command Field Descriptions

Field	Description
POS0/0, POS0/1...All Interfaces	Interface name; type of RSVP messages on a specified interface or all interfaces.
Recv	Number of messages received on the specified interface or on all interfaces.
Xmit	Number of messages transmitted from the specified interface or from all interfaces.

Related Commands

Command	Description
show ip rsvp counters	Displays the number of RSVP messages that were sent and received.

clear ip rsvp signalling rate-limit

To clear (set to zero) the number of Resource Reservation Protocol (RSVP) messages that were dropped because of a full queue, use the **clear ip rsvp signalling rate-limit** command in EXEC mode.

clear ip rsvp signalling rate-limit

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

Use the **clear ip rsvp signalling rate-limit** command to clear the counters recording dropped messages.

Examples

The following command shows how all dropped messages are cleared:

```
Router# clear ip rsvp signalling rate-limit
```

Related Commands

Command	Description
debug ip rsvp rate-limit	Displays debug messages for RSVP rate-limiting events.
ip rsvp signalling rate-limit	Controls the transmission rate for RSVP messages sent to a neighboring router during a specified amount of time.
show ip rsvp signalling rate-limit	Displays rate-limiting parameters for RSVP messages.

clear ip rsvp signalling refresh reduction

To clear (set to zero) the counters associated with the number of retransmissions and the number of out-of-order Resource Reservation Protocol (RSVP) messages, use the **clear ip rsvp signalling refresh reduction** command in EXEC mode.

clear ip rsvp signalling refresh reduction

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

Use the **clear ip rsvp signalling refresh reduction** command to clear the counters recording retransmissions and out-of-order RSVP messages.

Examples

The following command shows how all the retransmissions and out-of-order messages are cleared:

```
Router# clear ip rsvp signalling refresh reduction
```

Related Commands

Command	Description
ip rsvp signalling refresh reduction	Enables refresh reduction.
show ip rsvp signalling refresh reduction	Displays refresh-reduction parameters for RSVP messages.

compression header ip

To configure Real-Time Transport Protocol (RTP) or TCP IP header compression for a specific class, use the **compression header ip** command in policy-map class configuration mode. To remove RTP or TCP IP header compression for a specific class, use the **no** form of this command.

compression header ip [**rtp** | **tcp**]

no compression header ip

Syntax Description

rtp	(Optional) Configures RTP header compression.
tcp	(Optional) Configures TCP header compression.

Defaults

If you do not specify either RTP or TCP header compression (that is, you press the enter key after the command name) both RTP and TCP header compressions are configured. This is intended to cover the "all compressions" scenario.

Command Modes

Policy-map class configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

Using any form of the **compression header ip** command overrides any previously entered form.

The **compression header ip** command can be used at any level in the policy map hierarchy configured with the Modular Quality of Service (QoS) Command-Line Interface (CLI) (MQC) feature.

Examples

In the following example, the **compression header ip** command has been configured to use RTP header compression for a class called "class1". Class1 is part of policy map called "policy1".

```
Router(config)# policy-map policy1
Router(config-pmap)# class-map class1
Router(config-pmap-c)# compression header ip rtp
Router(config-pmap-c)# exit
```

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 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.

custom-queue-list

To assign a custom queue list to an interface, use the **custom-queue-list** command in interface configuration mode. To remove a specific list or all list assignments, use the **no** form of this command.

custom-queue-list [*list-number*]

no custom-queue-list [*list-number*]

Syntax Description

list-number	Any number from 1 to 16 for the custom queue list.

Defaults

No custom queue list is assigned.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Only one queue list can be assigned per interface. Use this command in place of the **priority-list interface** command (not in addition to it). Custom queueing allows a fairness not provided with priority queueing. With custom queueing, you can control the bandwidth available on the interface when the interface is unable to accommodate the aggregate traffic enqueued. Associated with each output queue is a configurable byte count, which specifies how many bytes of data should be delivered from the current queue by the system before the system moves on to the next queue. When a particular queue is being processed, packets are sent until the number of bytes sent exceeds the queue byte count or until the queue is empty.

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

Examples

In the following example, custom queue list number 3 is assigned to serial interface 0:

```
interface serial 0
 custom-queue-list 3
```

Related Commands

Command	Description
priority-list interface	Establishes queueing priorities on packets entering from a given interface.
queue-list default	Assigns a priority queue for those packets that do not match any other rule in the queue list.
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.
queue-list queue limit	Designates the queue length limit for a queue.
show interfaces	Displays statistics for all interfaces configured on the router or access server.
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.

disconnect qdm

To disconnect a Quality of Service Device Manager (QDM) client, use the **disconnect qdm** EXEC command in EXEC mode.

disconnect qdm [**client** *client-id*]

Syntax Description

client	(Optional) Specifies that a specific QDM client will be disconnected.
client-id	(Optional) Specifies the specific QDM identification number to disconnect. A QDM identification number can be a number from 0 to 214,748,3647.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 12.1(1)E	This command was introduced.
Release 12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.

Usage Guidelines

Use the **disconnect qdm** command to disconnect all QDM clients that are connected to the router.

Use the **disconnect qdm** [**client** *client-id*] command to disconnect a specific QDM client connected to a router. For instance, using the **disconnect qdm client 42** command will disconnect the QDM client with the ID 42.

Examples

The following example shows how to disconnect all connected QDM clients:

```
Router# disconnect qdm
```

The following example shows how to disconnect a specific QDM client with client ID 9:

```
Router# disconnect qdm client 9
```

Related Commands

Command	Description
show qdm status	Displays the status of connected QDM clients.

drop

To configure a traffic class to discard packets belonging to a specific class, use the **drop** command in policy-map class configuration mode. To disable the packet discarding action in a traffic class, use the **no** form of this command.

drop

no drop

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Policy-map class configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

Note the following points when configuring the **drop** command to unconditionally discard packets in a traffic class:

- Discarding packets is the only action that can be configured in a traffic class. That is, no other actions can be configured in the traffic class.
- When a traffic class is configured with the **drop** command, a "child" (nested) policy cannot be configured for this specific traffic class through the **service policy** command.
- Discarding packets cannot be configured for the default class known as the class-default class.

Examples

In the following example a traffic class called "class1" has been created and configured for use in a policy map called "policy1." The policy map (service policy) is attached to an output serial interface 2/0. All packets matching access-group 101 are placed in a class called "c1." Packets belonging to this class are discarded.

```
Router(config)# class-map class1
Router(config-cmap)# match access-group 101
Router(config-cmap)# policy-map policy1
Router(config-pmap)# class c1
Router(config-pmap-c)# drop
Router(config-pmap-c)# interface s2/0
Router(config-if)# service-policy output policy1
Router(config-if)# exit
```

Related Commands

Command	Description
show class-map	Displays all class maps and their matching criteria.
show policy-map	Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps.
show policy-map interface	Displays the packet statistics of all classes that are configured for all service policies either on the specified interface or subinterface or on a specific PVC on the interface.

dscp

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

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

no dscp *dscpvalue min-threshold max-threshold* [*mark-probability-denominator*]

Syntax Description

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

Defaults

If WRED is using the DSCP value to calculate the drop probability of a packet, all entries of the DSCP table are initialized with the default settings shown in Table 2 in the “Usage Guidelines” section of this command.

Command Modes

cfg-red-grp configuration

Command History

Release	Modification
12.1(5)T	This command was introduced.

Usage Guidelines

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

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

Table 2 lists the dscp default settings used by the **dscp** command. Table 2 lists the DSCP value, and its corresponding minimum threshold, maximum threshold, and mark probability. The last row of the table (the row labeled "default") shows the default settings used for any DSCP value not specifically shown in the table.

Table 2 dscp Default Settings

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

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

```
dscp af22 28 40 10
```

Related Commands

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

exponential-weighting-constant

To configure the exponential weight factor for the average queue size calculation for a Weighted Random Early Detection (WRED) parameter group, use the **exponential-weighting-constant** command in random-detect-group configuration mode. To return the exponential weight factor for the group to the default, use the **no** form of this command.

exponential-weighting-constant *exponent*

no exponential-weighting-constant

Syntax Description

exponent	Exponent from 1 to 16 used in the average queue size calculation.

Defaults

The default weight factor is 9.

Command Modes

Random-detect-group configuration

Command History

Release	Modification
11.1(22)CC	This command was introduced.

Usage Guidelines

When used, this command is issued after the **random-detect-group** command is entered.

Use this command to change the exponent used in the average queue size calculation for a WRED parameter group. The average queue size is based on the previous average and the current size of the queue. The formula is:

```
average = (old_average * (1-1/2^x)) + (current_queue_size * 1/2^x)
```

where *x* is the exponential weight factor specified in this command. Thus, the higher the factor, the more dependent the average is on the previous average.

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

For high values of *x*, the previous average becomes more important. A large factor smooths out the peaks and lows in queue length. The average queue size is unlikely to change very quickly. The WRED process will be slow to start dropping packets, but it may continue dropping packets for a time after the actual queue size has fallen below the minimum threshold. The resulting slow-moving average will accommodate temporary bursts in traffic.

If the value of *x* gets too high, WRED will not react to congestion. Packets will be sent or dropped as if WRED were not in effect.

For low values of *x*, the average queue size closely tracks the current queue size. The resulting average may fluctuate with changes in the traffic levels. In this case, the WRED process will respond quickly to long queues. Once the queue falls below the minimum threshold, the process will stop dropping packets.

If the value of *x* gets too low, WRED will overreact to temporary traffic bursts and drop traffic unnecessarily.

Examples

The following example configures the WRED group called sanjose with a weight factor of 10:

```
random-detect-group sanjose
  exponential-weighting-constant 10
```

Related Commands

Command	Description
protect	Configures a VC or PVC class with protected group or protected VC or PVC status for application to a VC or PVC bundle member.
random-detect exponential-weighting-constant	Configures the WRED and DWRED exponential weight factor for the average queue size calculation.
random-detect-group	Defines the WRED or DWRED parameter group.
show queueing	Lists all or selected configured queueing strategies.
show queueing interface	Displays the queueing statistics of an interface or VC.

fair-queue (class-default)

To specify the number of dynamic queues to be reserved for use by the class-default class as part of the default class policy, use the **fair-queue** command in policy-map class configuration mode. To delete the configured number of dynamic queues from the class-default policy, use the **no** form of this command.

fair-queue [*number-of-dynamic-queues*]

no fair-queue [*number-of-dynamic-queues*]

Syntax Description

number-of-dynamic-queues	(Optional) A power of 2 number in the range from 16 to 4096 specifying the number of dynamic queues.

Defaults

The number of dynamic queues is derived from the interface or ATM permanent virtual circuit (PVC) bandwidth. See Table 3 in the "Usage Guidelines" section of this command for the default number of dynamic queues that weighted fair queueing (WFQ) and class-based WFQ (CBWFQ) use when they are enabled on an interface. See Table 4 in the "Usage Guidelines" section of this command for the default number of dynamic queues used when WFQ or CBWFQ is enabled on an ATM PVC.

Command Modes

Policy-map class configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

This command can be used for the default class (commonly known as the class-default class) only. You can use it in conjunction with either the **queue-limit** command or the **random-detect** command.

The class-default class is the default class to which traffic is directed if that traffic does not satisfy the match criteria of other classes whose policy is defined in the policy map.

Table 3 lists the default number of dynamic queues that weighted fair queueing (WFQ) and class-based WFQ (CBWFQ) use when they are enabled on an interface.

Table 3 Default Number of Dynamic Queues As a Function of Interface Bandwidth

Bandwidth Range	Number of Dynamic Queues
Less than or equal to 64 kbps	16
More than 64 kbps and less than or equal to 128 kbps	32
More than 128 kbps and less than or equal to 256 kbps	64
More than 256 kbps and less than or equal to 512 kbps	128
More than 512 kbps	256

Table 4 lists the default number of dynamic queues used when WFQ or CBWFQ is enabled on an ATM PVC.

Table 4 Default Number of Dynamic Queues As a Function of ATM PVC Bandwidth

Bandwidth Range	Number of Dynamic Queues
Less than or equal to 128 kbps	16
More than 128 kbps and less than or equal to 512 kbps	32
More than 512 kbps and less than or equal to 2000 kbps	64
More than 2000 kbps and less than or equal to 8000 kbps	128
More than 8000 kbps	256

Examples

The following example configures policy for the default class included in the policy map called policy9. Packets that do not satisfy match criteria specified for other classes whose policies are configured in the same service policy are directed to the default class, for which 16 dynamic queues have been reserved. Because the **queue-limit** command is configured, tail drop is used for each dynamic queue when the maximum number of packets are enqueued and additional packets arrive.

```
policy-map policy9
 class class-default
 fair-queue 16
 queue-limit 20
```

The following example configures policy for the default class included in the policy map called policy8. The **fair-queue** command reserves 20 dynamic queues to be used for the default class. For congestion avoidance, Weighted Random Early Detection (WRED) packet drop is used, not tail drop.

```
policy-map policy8
class class-default
 fair-queue 20
 random-detect
```

Related Commands

Command	Description
queue-limit	Specifies or modifies the maximum number of packets the queue can hold for a class policy configured in a policy map.
random-detect (interface)	Enables WRED or DWRED.

fair-queue (DWFQ)

To enable VIP-distributed weighted fair queueing (DWFQ), use the **fair-queue** command in interface configuration mode. The command enables DWFQ on an interface using a VIP2-40 or greater interface processor. To disable DWFQ, use the **no** form of this command.

fair-queue

no fair-queue

Syntax Description

This command has no arguments or keywords.

Defaults

DWFQ is enabled by default for physical interfaces whose bandwidth is less than or equal to 2.048 Mbps.

DWFQ can be configured on interfaces but not subinterfaces. It is not supported on Fast EtherChannel, tunnel, or other logical or virtual interfaces such as Multilink PPP (MLP).

See Table 5 in the "Usage Guidelines" section of this command for a list of the default queue lengths and thresholds.

Command Modes

Interface configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

With DWFQ, packets are classified by flow. Packets with the same source IP address, destination IP address, source TCP or User Datagram Protocol (UDP) port, destination TCP or UDP port, and protocol belong to the same flow.

DWFQ allocates an equal share of the bandwidth to each flow.

Table 5 lists the default queue lengths and thresholds.

Table 5 Default Fair Queue Lengths and Thresholds

Queue or Threshold	Default
Congestive discard threshold	64 messages
Dynamic queues	256 queues
Reservable queues	0 queues

Examples

The following example enables DWFQ on the High-Speed Serial Interface (HSSI) interface 0/0/0:

```
interface Hssi0/0/0
 description 45Mbps to R2
 ip address 10.200.14.250 255.255.255.252
 fair-queue
```

Related Commands

Command	Description
fair-queue (WFQ)	Enables WFQ for an interface.
fair-queue aggregate-limit	Sets the maximum number of packets in all queues combined for DWFQ.
fair-queue individual-limit	Sets the maximum individual queue depth for DWFQ.
fair-queue limit	Sets the maximum queue depth for a specific DWFQ class.
fair-queue qos-group	Enables DWFQ and classifies packets based on the internal QoS-group number.
fair-queue tos	Enables DWFQ and classifies packets using the ToS field of packets.
show interfaces	Displays statistics for all interfaces configured on the router or access server.
show interfaces fair-queue	Displays information and statistics about WFQ for a VIP-based interface.

fair-queue (policy-map class)

To specify the number of queues to be reserved for use by a traffic class, use the **fair-queue** command in QoS policy-map class configuration mode. To delete the configured number of queues from the traffic class, use the **no** form of this command.

fair-queue [*dynamic-queues*]

no fair-queue [*dynamic-queues*]

Syntax Description

dynamic-queues	(Optional) A number specifying the number of dynamic conversation queues. The number can be in the range of 16 to 4,096.

Defaults

No default behavior or values

Command Modes

QoS policy-map class configuration

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. Support for Versatile Interface Processor (VIP)-enabled Cisco 7500 series routers was added.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T. Support for VIP-enabled Cisco 7500 series routers was added.

Usage Guidelines

On a VIP, the **fair-queue** command can be used for any traffic class (as opposed to non-VIP platforms, which can only use the **fair-queue** command in the default traffic class). The **fair-queue** command can be used in conjunction with either the **queue-limit** command or the **random-detect exponential-weighting-constant** command.

Examples

The following example configures the default traffic class for the policy map called policy9 to reserve ten queues for packets that do not satisfy match criteria specified for other traffic classes whose policy is configured in the same service policy. Because the **queue-limit** command is configured, tail drop is used for each queue when the maximum number of packets is enqueued and additional packets arrive.

```
policy-map policy9
 class class-default
 fair-queue 10
 queue-limit 20
```

The following example configures a service policy called policy8 that is associated with a user-defined traffic class called class1. The **fair-queue** command reserves 20 queues to be used for the service policy. For congestion avoidance, Weighted Random Early Detection (WRED) or distributed WRED (DWRED) packet drop is used, not tail drop.

```
policy-map policy8
 class class1
 fair-queue 20
   random-detect exponential-weighting-constant 14
```

Related Commands

Command	Description
class class-default	Specifies the default traffic class for a service policy map.
queue-limit	Specifies or modifies the maximum number of packets the queue can hold for a class policy configured in a policy map.
random-detect exponential-weighting-constant	Configures the WRED and DWRED exponential weight factor for the average queue size calculation.

fair-queue (WFQ)

To enable weighted fair queueing (WFQ) for an interface, use the **fair-queue** command in interface configuration mode. To disable WFQ for an interface, use the **no** form of this command.

fair-queue [*congestive-discard-threshold* [*dynamic-queues* [*reservable-queues*]]]

no fair-queue

Syntax Description

congestive-discard-threshold	(Optional) Number of messages allowed in each queue. The default is 64 messages, and a new threshold must be a power of 2 in the range from 16 to 4096. When a conversation reaches this threshold, new message packets are discarded.
dynamic-queues	(Optional) Number of dynamic queues used for best-effort conversations (that is, a normal conversation not requiring any special network services). Values are **16**, **32**, **64**, **128**, **256**, **512**, **1024**, **2048**, and **4096**. See Table 4 and Table 5 in the **fair-queue** (class-default) command for the default number of dynamic queues.
reservable-queues	(Optional) Number of reservable queues used for reserved conversations in the range 0 to 1000. The default is 0. Reservable queues are used for interfaces configured for features such as Resource Reservation Protocol (RSVP).

Defaults

Fair queueing is enabled by default for physical interfaces whose bandwidth is less than or equal to 2.048 Mbps and that do not use the following:

- X.25 and Synchronous Data Link Control (SDLC) encapsulations
- Link Access Procedure, Balanced (LAPB)
- Tunnels
- Loopbacks
- Dialer
- Bridges
- Virtual interfaces

Fair queueing is not an option for the protocols listed above. However, if custom queueing or priority queueing is enabled for a qualifying link, it overrides fair queueing, effectively disabling it. Additionally, fair queueing is automatically disabled if you enable the autonomous or silicon switching engine mechanisms.

Note A variety of queueing mechanisms can be configured using multilink, for example, Multichassis Multilink PPP (MMP). However, if only PPP is used on a tunneled interface—for example, virtual private dialup network (VPND), PPP over Ethernet (PPPoE), or PPP over Frame Relay (PPPoFR)—no queueing can be configured on the virtual interface.

The number of dynamic queues is derived from the interface or ATM permanent virtual circuit (PVC) bandwidth. See Table 3 in the **fair-queue** (class-default) command for the default number of dynamic queues that WFQ and class-based WFQ (CBWFQ) use when they are enabled on an interface. See Table 4 in the **fair-queue** (class-default) command for the default number of dynamic queues used when WFQ and CBWFQ are enabled on an ATM PVC.

Command Modes

Interface configuration

Command History

Release	Modification
11.0	This command was introduced.
12.2(13)T	This command was modified to remove apollo, vines, and xns from the list of protocols and traffic stream discrimination fields. These protocols were removed because Apollo Domain, Banyan VINES, and Xerox Network Systems (XNS) were removed in Release 12.2(13)T.

Usage Guidelines

This command enables WFQ. With WFQ, packets are classified by flow. For example, packets with the same source IP address, destination IP address, source TCP or User Datagram Protocol (UDP) port, destination TCP or UDP port, and protocol belong to the same flow; see Table 6 for a full list of protocols and traffic stream discrimination fields.

When enabled for an interface, WFQ provides traffic priority management that automatically sorts among individual traffic streams without requiring that you first define access lists. Enabling WFQ requires use of this command only.

When WFQ is enabled for an interface, new messages for high-bandwidth traffic streams are discarded after the configured or default congestive discard threshold has been met. However, low-bandwidth conversations, which include control message conversations, continue to enqueue data. As a result, the fair queue may occasionally contain more messages than its configured threshold number specifies.

WFQ uses a traffic data stream discrimination registry service to determine which traffic stream a message belongs to. For each forwarding protocol, Table 6 shows the attributes of a message that are used to classify traffic into data streams.

Table 6 Weighted Fair Queueing Traffic Stream Discrimination Fields

Forwarder	Fields Used
AppleTalk	• Source net, node, socket • Destination net, node, socket • Type
Connectionless Network Service (CLNS)	• Source network service access point (NSAP) • Destination NSAP
DECnet	• Source address • Destination address
Frame Relay switching	• Data-link connection identified (DLCI) value
IP	• Type of service (ToS) • IP protocol • Source IP address (if message is not fragmented) • Destination IP address (if message is not fragmented) • Source TCP/UDP port • Destination TCP/UDP port
Transparent bridging	• Unicast: source MAC, destination MAC • Ethertype Service Advertising Protocol (SAP)/Subnetwork Access Protocol (SNAP) multicast: destination MAC address
Source-route bridging	• Unicast: source MAC, destination MAC • SAP/SNAP multicast: destination MAC address
Novell NetWare	• Source/destination network/host/socket • Level 2 protocol
All others (default)	• Control protocols (one queue per protocol)

It is important to note that IP Precedence, congestion in Frame Relay switching, and discard eligible (DE) flags affect the weights used for queueing.

IP Precedence, which is set by the host or by policy maps, is a number in the range from 0 to 7. Data streams of precedence *number* are weighted so that they are given an effective bit rate of *number*+1 times as fast as a data stream of precedence 0, which is normal.

In Frame Relay switching, message flags for forward explicit congestion notification (FECN), backward explicit congestion notification (BECN), and DE message flags cause the algorithm to select weights that effectively impose reduced queue priority. The reduced queue priority provides the application with "slow down" feedback and sorts traffic, giving the best service to applications within their committed information rate (CIR).

Fair queueing is supported for all LAN and line (WAN) protocols except X.25, including LAPB and SDLC; see the notes in the section "Defaults." Because tunnels are software interfaces that are themselves routed over physical interfaces, fair queueing is not supported for tunnels. Fair queueing is on by default for interfaces with bandwidth less than or equal to 2 Mbps.

Note For Release 10.3 and earlier releases for the Cisco 7000 and 7500 routers with a Route Switch Processor (RSP) card, if you used the **tx-queue-limit** command to set the transmit limit available to an interface on a Multiport Communications Interface (MCI) or serial port communications interface (SCI) card and you configured custom queueing or priority queueing for that interface, the configured transmit limit was automatically overridden and set to 1. With Cisco IOS Release 12.0 and later releases, for WFQ, custom queueing, and priority queueing, the configured transmit limit is derived from the bandwidth value set for the interface using the **bandwidth** (interface) command. Bandwidth value divided by 512 rounded up yields the effective transmit limit. However, the derived value only applies in the absence of a **tx-queue-limit** command; that is, a configured transmit limit overrides this derivation.

When Resource Reservation Protocol (RSVP) is configured on an interface that supports fair queueing or on an interface that is configured for fair queueing with the reservable queues set to 0 (the default), the reservable queue size is automatically configured using the following method: interface bandwidth divided by 32 kbps. You can override this default by specifying a reservable queue other than 0. For more information on RSVP, refer to the chapter "Configuring RSVP" in the *Cisco IOS Quality of Service Solutions Configuration Guide*, Release 12.2.

Examples

The following example enables use of WFQ on serial interface 0, with a congestive threshold of 300. This threshold means that messages will be discarded from the queueing system only when 300 or more messages have been queued and the message is in a data stream that has more than one message in the queue. The transmit queue limit is set to 2, based on the 384-kilobit (Kb) line set by the **bandwidth** command:

```
interface serial 0
 bandwidth 384
 fair-queue 300
```

Unspecified parameters take the default values.

The following example requests a fair queue with a congestive discard threshold of 64 messages, 512 dynamic queues, and 18 RSVP queues:

```
interface Serial 3/0
 ip unnumbered Ethernet 0/0
 fair-queue 64 512 18
```

Related Commands

Command	Description
bandwidth (interface)	Sets a bandwidth value for an interface.
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 (DWFQ)	Enables DWFQ.
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.
show interfaces	Displays statistics for all interfaces configured on the router or access server.
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.
tx-queue-limit	Controls the number of transmit buffers available to a specified interface on the MCI and SCI cards.

fair-queue aggregate-limit

To set the maximum number of packets in all queues combined for VIP-distributed weighted fair queueing (DWFQ), use the **fair-queue aggregate-limit** command in interface configuration mode. To return the value to the default, use the **no** form of this command.

fair-queue aggregate-limit *aggregate-packets*

no fair-queue aggregate-limit

Syntax Description

aggregate-packets	Total number of buffered packets allowed before some packets may be dropped. Below this limit, packets will not be dropped.

Defaults

The total number of packets allowed is based on the transmission rate of the interface and the available buffer space on the Versatile Interface Processor (VIP).

Command Modes

Interface configuration

Command History

Release	Modification
11.1 CC	This command was introduced.

Usage Guidelines

In general, you should not change the maximum number of packets allows in all queues from the default. Use this command only if you have determined that you would benefit from using a different value, based on your particular situation.

DWFQ keeps track of the number of packets in each queue and the total number of packets in all queues.

When the total number of packets is below the aggregate limit, queues can buffer more packets than the individual queue limit.

When the total number of packets reaches the aggregate limit, the interface starts enforcing the individual queue limits. Any new packets that arrive for a queue that is over its individual queue limit are dropped. Packets that are already in the queue will not be dropped, even if the queue is over the individual limit.

In some cases, the total number of packets in all queues put together may exceed the aggregate limit.

Examples

The following example sets the aggregate limit to 54 packets:

```
interface Fddi9/0/0
 fair-queue tos
 fair-queue aggregate-limit 54
```

Related Commands

Command	Description
fair-queue limit	Sets the maximum queue depth for a specific DWFQ class.
fair-queue qos-group	Enables DWFQ and classifies packets based on the internal QoS-group number.
fair-queue tos	Enables DWFQ and classifies packets using the ToS field of packets.
show interfaces	Displays statistics for all interfaces configured on the router or access server.
show interfaces fair-queue	Displays information and statistics about WFQ for a VIP-based interface.

fair-queue individual-limit

To set the maximum individual queue depth for VIP-distributed weighted fair queueing (DWFQ), use the **fair-queue individual-limit** command in interface configuration mode. To return the value to the default, use the **no** form of this command.

fair-queue individual-limit *individual-packet*

no fair-queue individual-limit

Syntax Description

individual-packet	Maximum number of packets allowed in each per-flow or per-class queue during periods of congestion.

Defaults

Half of the aggregate queue limit

Command Modes

Interface configuration

Command History

Release	Modification
11.1 CC	This command was introduced.

Usage Guidelines

In general, you should not change the maximum individual queue depth from the default. Use this command only if you have determined that you would benefit from using a different value, based on your particular situation.

DWFQ keeps track of the number of packets in each queue and the total number of packets in all queues.

When the total number of packets is below the aggregate limit, queues can buffer more packets than the individual queue limit.

When the total number of packets reaches the aggregate limit, the interface starts enforcing the individual queue limits. Any new packets that arrive for a queue that is over its individual queue limit are dropped. Packets that are already in the queue will not be dropped, even if the queue is over the individual limit.

In some cases, the total number of packets in all queues put together may exceed the aggregate limit.

Examples

The following example sets the individual queue limit to 27:

```
interface Fddi9/0/0
 mac-address 0000.0c0c.2222
 ip address 10.1.1.1 255.0.0.0
 fair-queue tos
 fair-queue individual-limit 27
```

Related Commands

Command	Description
fair-queue aggregate-limit	Sets the maximum number of packets in all queues combined for DWFQ.
fair-queue limit	Sets the maximum queue depth for a specific DWFQ class.
fair-queue qos-group	Enables DWFQ and classifies packets based on the internal QoS-group number.
fair-queue tos	Enables DWFQ and classifies packets using the ToS field of packets.
show interfaces	Displays statistics for all interfaces configured on the router or access server.
show interfaces fair-queue	Displays information and statistics about WFQ for a VIP-based interface.

fair-queue limit

To set the maximum queue depth for a specific VIP-distributed weighted fair queueing (DWFQ) class, use the **fair-queue limit** command in interface configuration mode. To return the value to the default, use the **no** form of this command.

fair-queue {**qos-group** *number* | **tos** *number*} **limit** *class-packet*

no fair-queue {**qos-group** *number* | **tos** *number*} **limit** *class-packet*

Syntax Description

qos-group *number*	Number of the QoS group, as assigned by a committed access rate (CAR) policy or the Policy Propagation via Border Gateway Protocol (BGP) feature. The value can range from 1 to 99.
tos *number*	Two low-order IP Precedence bits of the type of service (ToS) field.
class-packet	Maximum number of packets allowed in the queue for the class during periods of congestion.

Defaults

The individual queue depth, as specified by the **fair-queue individual-limit** command. If the **fair-queue individual-limit** command is not configured, the default is half of the aggregate queue limit.

Command Modes

Interface configuration

Command History

Release	Modification
11.1 CC	This command was introduced.

Usage Guidelines

Use this command to specify the number queue depth for a particular class for class-based DWFQ. This command overrides the global individual limit specified by the **fair-queue individual-limit** command.

In general, you should not change this value from the default. Use this command only if you have determined that you would benefit from using a different value, based on your particular situation.

Examples

The following example sets the individual queue limit for ToS group 3 to 20:

```
interface Fddi9/0/0
 mac-address 0000.0c0c.2222
 ip address 10.1.1.1 255.0.0.0
 fair-queue tos
 fair-queue tos 3 limit 20
```

Related Commands

Command	Description
fair-queue aggregate-limit	Sets the maximum number of packets in all queues combined for DWFQ.
fair-queue qos-group	Enables DWFQ and classifies packets based on the internal QoS-group number.
fair-queue tos	Enables DWFQ and classifies packets using the ToS field of packets.
show interfaces	Displays statistics for all interfaces configured on the router or access server.
show interfaces fair-queue	Displays information and statistics about WFQ for a VIP-based interface.

fair-queue qos-group

To enable VIP-distributed weighted fair queueing (DWFQ) and classify packets based on the internal QoS-group number, use the **fair-queue qos-group** command in interface configuration mode. To disable QoS-group-based DWFQ, use the **no** form of this command.

fair-queue qos-group

no fair-queue qos-group

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
11.1 CC	This command was introduced.

Usage Guidelines

Use this command to enable QoS-group-based DWFQ, a type of class-based DWFQ. Class-based DWFQ overrides flow-based DWFQ. Therefore, this command overrides the **fair-queue** (DWFQ) command.

When this command is enabled, packets are assigned to different queues based on their QoS group. A QoS group is an internal classification of packets used by the router to determine how packets are treated by certain QoS features, such as DWFQ and committed access rate (CAR). Use a CAR policy or the QoS Policy Propagation via Border Gateway Protocol (BGP) feature to assign packets to QoS groups.

Specify a weight for each class. In periods of congestion, each group is allocated a percentage of the output bandwidth equal to the weight of the class. For example, if a class is assigned a weight of 50, packets from this class are allocated at least 50 percent of the outgoing bandwidth during periods of congestion.

Examples

The following example enables QoS-based DWFQ and allocates bandwidth for nine QoS groups (QoS groups 0 through 8):

```
interface Hssi0/0/0
 description 45Mbps to R2
 ip address 10.200.14.250 255.255.255.252
 fair-queue qos-group
 fair-queue qos-group 1 weight 5
 fair-queue qos-group 2 weight 5
 fair-queue qos-group 3 weight 10
 fair-queue qos-group 4 weight 10
 fair-queue qos-group 5 weight 10
 fair-queue qos-group 6 weight 15
 fair-queue qos-group 7 weight 20
 fair-queue qos-group 8 weight 29
```

Related Commands

Command	Description
fair-queue aggregate-limit	Sets the maximum number of packets in all queues combined for DWFQ.
fair-queue limit	Sets the maximum queue depth for a specific DWFQ class.
fair-queue tos	Enables DWFQ and classifies packets using the ToS field of packets.
fair-queue weight	Assigns a weight to a class for DWFQ.
show interfaces	Displays statistics for all interfaces configured on the router or access server.
show interfaces fair-queue	Displays information and statistics about WFQ for a VIP-based interface.

fair-queue tos

To enable VIP-distributed weighted fair queueing (DWFQ) and classify packets using the type of service (ToS) field of packets, use the **fair-queue tos** command in interface configuration command. To disable ToS-based DWFQ, use the **no** form of this command.

fair-queue tos

no fair-queue tos

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

By default, class 0 is assigned a weight of 10; class 1 is assigned a weight of 20; class 2 is assigned a weight of 30; and class 3 is assigned a weight of 40.

Command Modes

Interface configuration

Command History

Release	Modification
11.1 CC	This command was introduced.

Usage Guidelines

Use this command to enable ToS-based DWFQ, a type of class-based DWFQ. Class-based DWFQ overrides flow-based DWFQ. Therefore, this command overrides the **fair-queue** (DWFQ) command.

When this command is enabled, packets are assigned to different queues based on the two low-order IP Precedence bits in the ToS field of the packet header.

In periods of congestion, each group is allocated a percentage of the output bandwidth equal to the weight of the class. For example, if a class is assigned a weight of 50, packets from this class are allocated at least 50 percent of the outgoing bandwidth during periods of congestion.

If you wish to change the weights, use the **fair-queue weight** command.

Examples

The following example enables ToS-based DWFQ on the High-Speed Serial Interface (HSSI) interface 0/0/0:

```
interface Hssi0/0/0
 description 45Mbps to R2
 ip address 10.200.14.250 255.255.255.252
 fair-queue
 fair-queue tos
```

Related Commands

Command	Description
fair-queue aggregate-limit	Sets the maximum number of packets in all queues combined for DWFQ.
fair-queue limit	Sets the maximum queue depth for a specific DWFQ class.
fair-queue qos-group	Enables DWFQ and classifies packets based on the internal QoS-group number.
fair-queue weight	Assigns a weight to a class for DWFQ.
show interfaces	Displays statistics for all interfaces configured on the router or access server.
show interfaces fair-queue	Displays information and statistics about WFQ for a VIP-based interface.

fair-queue weight

To assign a weight to a class for VIP-distributed weighted fair queueing (DWFQ), use the **fair-queue weight** command in interface configuration mode. To remove the bandwidth allocated for the class, use the **no** form of this command.

fair-queue {**qos-group** *number* | **tos** *number*} **weight** *weight*

no fair-queue {**qos-group** *number* | **tos** *number*} **weight** *weight*

Syntax Description

qos-group *number*	Number of the QoS group, as assigned by a committed access rate (CAR) policy or the Policy Propagation via Border Gateway Protocol (BGP) feature. The value range is from 1 to 99.
tos *number*	Two low-order IP Precedence bits of the type of service (ToS) field. The value range is from 1 to 3.
weight	Percentage of the output link bandwidth allocated to this class. The sum of weights for all classes cannot exceed 99.

Defaults

For QoS DWFQ, unallocated bandwidth is assigned to QoS group 0.

For ToS-based DWFQ, class 0 is assigned a weight of 10; class 1 is assigned a weight of 20; class 2 is assigned a weight of 30; and class 3 is assigned a weight of 40.

Command Modes

Interface configuration

Command History

Release	Modification
11.1 CC	This command was introduced.

Usage Guidelines

Use this command to allocate percentages of bandwidth for specific DWFQ classes. You must also enable class-based DWFQ on the interface with either the **fair-queue qos-group** or **fair-queue tos** command.

Enter this command once for every class to allocate bandwidth to the class.

For QoS-group-based DWFQ, packets that are not assigned to any QoS groups are assigned to QoS group 0. When assigning weights to QoS group class, remember the following guidelines:

- 1 percent of the available bandwidth is automatically allocated to QoS group 0.
- The total weight for all the other QoS groups combined cannot exceed 99.
- Any unallocated bandwidth is assigned to QoS group 0.

For ToS-based DWFQ, remember the following guidelines:

- 1 percent of the available bandwidth is automatically allocated to ToS class 0.
- The total weight for all the other ToS classes combined cannot exceed 99.
- Any unallocated bandwidth is assigned to ToS class 0.

Examples

The following example allocates bandwidth to different QoS groups. The remaining bandwidth (5 percent) is allocated to QoS group 0.

```
interface Fddi9/0/0
 fair-queue qos-group
 fair-queue qos-group 1 weight 10
 fair-queue qos-group 2 weight 15
 fair-queue qos-group 3 weight 20
 fair-queue qos-group 4 weight 20
 fair-queue qos-group 5 weight 30
```

Related Commands

Command	Description
fair-queue qos-group	Enables DWFQ and classifies packets based on the internal QoS-group number.
fair-queue tos	Enables DWFQ and classifies packets using the ToS field of packets.
show interfaces	Displays statistics for all interfaces configured on the router or access server.
show interfaces fair-queue	Displays information and statistics about WFQ for a VIP-based interface.

frame-relay interface-queue priority

To enable the Frame Relay PVC Interface Priority Queueing (FR PIPQ) feature, use the **frame-relay interface-queue priority** command in interface configuration mode. To disable FR PIPQ, use the **no** form of this command.

frame-relay interface-queue priority [*high-limit medium-limit normal-limit low-limit*]

no frame-relay interface-queue priority

To assign priority to a permanent virtual circuit (PVC) within a Frame Relay map class, use the **frame-relay interface-queue priority** command in map-class configuration mode. To remove priority from a PVC within a Frame Relay map class, use the **no** form of this command.

frame-relay interface-queue priority {**high** | **medium** | **normal** | **low**}

no frame-relay interface-queue priority

Syntax Description

high-limit	(Optional) Size of the high priority queue specified in maximum number of packets.
medium-limit	(Optional) Size of the medium priority queue specified in maximum number of packets.
normal-limit	(Optional) Size of the normal priority queue specified in maximum number of packets.
low-limit	(Optional) Size of the low priority queue specified in maximum number of packets.
high	Assigns high priority to a PVC.
medium	Assigns medium priority to a PVC.
normal	Assigns normal priority to a PVC.
low	Assigns low priority to a PVC.

Defaults

The default sizes of the high, medium, normal, and low priority queues are 20, 40, 60, and 80 packets, respectively.

When FR PIPQ is enabled on the interface, the default PVC priority is normal priority.

Command Modes

Interface configuration

Map-class configuration

Command History

Release	Modification
12.1(2)T	This command was introduced.

Usage Guidelines

FR PIPQ must be enabled on the interface in order for the map-class configuration of PVC priority to be effective.

Before you configure FR PIPQ using the **frame-relay interface-queue priority** command, the following conditions must be met:

- PVCs should be configured to carry a single type of traffic.
- The network should be configured with adequate call admission control to prevent starvation of any of the priority queues.

You will not be able to configure FR PIPQ if any queueing other than first-in first out (FIFO) queueing is already configured at the interface level. You will be able to configure FR PIPQ when weighted fair queueing (WFQ) is in use, as long as WFQ is the default interface queueing method. Disabling FR PIPQ will restore the interface to dual FIFO queueing if FRF.12 is enabled, FIFO queueing if Frame Relay Traffic Shaping (FRTS) is enabled, or the default queueing method for the interface.

Examples

In the following example, FR PIPQ is enabled on serial interface 0, and the limits of the high, medium, normal, and low priority queues are set to 10, 20, 30, and 40 packets, respectively. PVC 100 is assigned high priority, so all traffic destined for PVC 100 will be sent to the high priority interface queue.

```
interface serial0
  encapsulation frame-relay
  frame-relay interface-queue priority 10 20 30 40
  frame-relay interface-dlci 100
   class high_priority_class
 !
 map-class frame-relay high_priority_class
  frame-relay interface-queue priority high
```

Related Commands

Command	Description
debug priority	Displays priority queueing events.
show frame-relay pvc	Displays statistics about PVCs for Frame Relay interfaces.
show interfaces	Displays statistics for all interfaces configured on the router or access server.
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.

frame-relay ip rtp priority

To reserve a strict priority queue on a Frame Relay permanent virtual circuit (PVC) for a set of Real-Time Transport Protocol (RTP) packet flows belonging to a range of User Datagram Protocol (UDP) destination ports, use the **frame-relay ip rtp priority** command in map-class configuration mode. To disable the strict priority queue, use the **no** form of this command.

frame-relay ip rtp priority *starting-rtp-port-number port-number-range bandwidth*

no frame-relay ip rtp priority

Syntax Description

starting-rtp-port-number	The starting UDP port number. The lowest port number to which the packets are sent. A port number can be a number from 2,000 to 65,535.
port-number-range	The range of UDP destination ports. Number, which added to the *starting-rtp-port-number* argument, yields the highest UDP port number. The range can be from 0 to 16,383.
bandwidth	Maximum allowed bandwidth, in kbps. The bandwidth can range from 0 to 2,000 kpbs.

Defaults

No default behavior or values

Command Modes

Map-class configuration

Command History

Release	Modification
12.0(7)T	This command was introduced.

Usage Guidelines

This command is most useful for voice applications, or other applications that are delay-sensitive. To use this command, you must first enter the **map-class frame-relay** command. After the Frame Relay map class has been configured, it must then be applied to a PVC.

This command extends the functionality offered by the **ip rtp priority** command by supporting Frame Relay PVCs. The command allows you to specify a range of UDP ports whose voice traffic is guaranteed strict priority service over any other queues or classes using the same output interface. Strict priority means that if packets exist in the priority queue, they are dequeued and sent first—that is, before packets in other queues are dequeued.

Frame Relay Traffic Shaping (FRTS) and Frame Relay Fragmentation (FRF.12) must be configured before the **frame-relay ip rtp priority** command is used.

Compressed RTP (CRTP) can be used to reduce the bandwidth required per voice call. When using CRTP with Frame Relay, you must use the **encapsulation frame-relay cisco** command instead of the **encapsulation frame-relay ietf** command.

Remember the following guidelines when configuring the *bandwidth* parameter:

- It is always safest to allocate to the priority queue slightly more than the known required amount of bandwidth, to allow room for network bursts.
- The IP RTP Priority admission control policy takes RTP header compression into account. Therefore, while configuring the *bandwidth* parameter of the **ip rtp priority** command you need to configure only for the bandwidth of the compressed call. Because the *bandwidth* parameter is the maximum total bandwidth, you need to allocate enough bandwidth for all calls if there will be more than one call.
- Configure a bandwidth that allows room for Layer 2 headers. The bandwidth allocation takes into account the payload plus the IP, UDP, and RTP headers but does not account for Layer 2 headers. Allowing 25 percent bandwidth for other overhead is conservative and safe.
- The sum of all bandwidth allocation for voice and data flows on an interface cannot exceed 75 percent of the total available bandwidth, unless you change the default maximum reservable bandwidth. To change the maximum reservable bandwidth, use the **max-reserved-bandwidth** command on the interface.

For more information on IP RTP Priority bandwidth allocation, refer to the section “IP RTP Priority” in the chapter “Congestion Management Overview” in the *Cisco IOS Quality of Service Solutions Configuration Guide*.

Examples

The following example first configures the Frame Relay map class called voip and then applies the map class to PVC 100 to provide strict priority service to matching RTP packets:

```
map-class frame-relay voip
 frame-relay cir 256000
 frame-relay bc 2560
 frame-relay be 600
 frame-relay mincir 256000
 no frame-relay adaptive-shaping
 frame-relay fair-queue
 frame-relay fragment 250
 frame-relay ip rtp priority 16384 16380 210

interface Serial5/0
 ip address 10.10.10.10 255.0.0.0
 no ip directed-broadcast
 encapsulation frame-relay
 no ip mroute-cache
 load-interval 30
 clockrate 1007616
 frame-relay traffic-shaping
 frame-relay interface-dlci 100
  class voip
 frame-relay ip rtp header-compression
 frame-relay intf-type dce
```

In this example, RTP packets on PVC 100 with UDP ports in the range from 16384 to 32764 (32764 = 16384 + 16380) will be matched and given strict priority service.

Related Commands

Command	Description
encapsulation frame-relay	Enables Frame Relay encapsulation.
ip rtp priority	Reserves a strict priority queue for a set of RTP packet flows belonging to a range of UDP destination ports.
map-class frame-relay	Specifies a map class to define QoS values for an SVC.
max-reserved-bandwidth	Changes the percent of interface bandwidth allocated for CBWFQ, LLQ, and IP RTP Priority.
priority	Gives priority to a class of traffic belonging to a policy map.
show frame-relay pvc	Displays statistics about PVCs for Frame Relay interfaces.
show queue	Displays the contents of packets inside a queue for a particular interface or VC.
show traffic-shape queue	Displays information about the elements queued by traffic shaping at the interface level or the DLCI level.

ip nbar pdlm

To extend or enhance the list of protocols recognized by network-based application recognition (NBAR) through a Cisco-provided Packet Description Language Module (PDLM), use the **ip nbar pdlm** command in global configuration mode. To unload a PDLM if it was previously loaded, use the **no** form of this command.

ip nbar pdlm *pdlm-name*

no ip nbar pdlm *pdlm-name*

Syntax Description

pdlm-name	URL at which the PDLM can be found on the Flash card.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)XE2	This command was introduced.
12.1(1)E	This command was integrated into Cisco IOS Release 12.1(1)E.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.1(13)E	This command was integrated into Cisco IOS Release 12.1(13)E. This command became available on Catalyst 6000 family switches without FlexWAN modules.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.

Usage Guidelines

This command is used in global configuration mode to extend the list of protocols recognized by a given version of NBAR or to enhance an existing protocol recognition capability. NBAR can be given an external PDLM at run time. In most cases, the PDLM enables NBAR to recognize new protocols without requiring a new Cisco IOS image or a router reload. Only Cisco can provide you with a new PDLM.

A list of the available PDLMs can be viewed online at Cisco.com.

Examples

The following example configures NBAR to load the citrix.pdlm PDLM from Flash memory on the router:

```
ip nbar pdlm flash://citrix.pdlm
```

Related Commands

Command	Description
show ip nbar pdlm	Displays the current PDLM in use by NBAR.

ip nbar port-map

To configure network-based application recognition (NBAR) to search for a protocol or protocol name using a port number other than the well-known port, use the **ip nbar port-map** command in global configuration mode. To look for the protocol name using only the well-known port number, use the **no** form of this command.

ip nbar port-map *protocol-name* [**tcp** | **udp**] *port-number*

no ip nbar port-map *protocol-name* [**tcp** | **udp**] *port-number*

Syntax Description

protocol-name	Name of protocol known to NBAR.
tcp	(Optional) Specifies that a TCP port will be searched for the specified *protocol-name* argument.
udp	(Optional) Specifies that a User Datagram Protocol (UDP) port will be searched for the specified *protocol-name* argument.
port-number	Assigned port for named protocol. The *port-number* argument is either a UDP or a TCP port number, depending on which protocol is specified in this command line. Up to 16 *port-number* arguments can be specified in one command line. Port number values can range from 0 to 65535.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)XE2	This command was introduced.
12.1(1)E	This command was integrated into Cisco IOS Release 12.1(1)E.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.1(13)E	This command was integrated into Cisco IOS Release 12.1(13)E. This command became available on Catalyst 6000 family switches without FlexWAN modules.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.

Usage Guidelines

This command is used in global configuration mode to tell NBAR to look for the protocol or protocol name, using a port number or numbers other than the well-known Internet Assigned Numbers Authority (IANA)-assigned) port number. For example, use this command to configure NBAR to look for Telnet on a port other than 23. Up to 16 ports can be specified with this command. Port number values can range from 0 to 65535.

Examples

The following example configures NBAR to look for the protocol Structured Query Language (SQL)*NET on port numbers 63000 and 63001 instead of on the well-known port number:

```
ip nbar port-map sqlnet tcp 63000 63001
```

Related Commands

Command	Description
show ip nbar port-map	Displays the current protocol-to-port mappings in use by NBAR.

ip nbar protocol-discovery

To configure networked-based application recognition (NBAR) to discover traffic for all protocols known to NBAR on a particular interface, use the **ip nbar protocol-discovery** command in interface configuration mode. To disable traffic discovery, use the **no** form of this command.

ip nbar protocol-discovery

no ip nbar protocol-discovery

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)XE2	This command was introduced.
12.1(1)E	This command was integrated into Cisco IOS Release 12.1(1)E.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.1(13)E	This command was integrated into Cisco IOS Release 12.1(13)E. This command became available on Catalyst 6000 family switches without FlexWAN modules.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.

Usage Guidelines

Use the **ip nbar protocol-discovery** command to configure NBAR to keep traffic statistics for all protocols known to NBAR. Protocol discovery provides an easy way to discover application protocols transiting an interface so that QoS policies can be developed and applied. The Protocol Discovery feature discovers any protocol traffic supported by NBAR. Protocol discovery can be used to monitor both input and output traffic and may be applied with or without a service policy enabled.

Examples

The following example configures protocol discovery on an Ethernet interface:

```
interface ethernet 1/3
ip nbar protocol-discovery
```

Related Commands

Command	Description
show ip nbar protocol-discovery	Displays the statistics gathered by the NBAR Protocol Discovery feature.

ip rsvp admission-control compression predict

To configure Resource Reservation Protocol (RSVP) admission control compression prediction, use the **ip rsvp admission-control compression predict** command in interface configuration mode. To disable compression prediction, use the **no** form of this command.

ip rsvp admission-control compression predict [**method** {**rtp** | **udp**} [**bytes-saved** *N*]]

no ip rsvp admission-control compression predict [**method** {**rtp** | **udp**} [**bytes-saved** *N*]]

Syntax Description

method	(Optional) Type of compression used.
rtp | **udp**	Real-Time Transport Protocol (RTP) or User Data Protocol (UDP) compression schemes.
bytes-saved *N*	(Optional) Predicted number of bytes saved per packet when RSVP predicts that compression will occur using the specified method. Values for *N* for RTP are 1 to 38; for UDP, 1 to 26.

Defaults

This command is enabled by default. The default value of bytes saved for RTP is 36; for UDP, 20.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

Use the **ip rsvp admission-control compression predict** command to disable or enable the RSVP prediction of compression for a specified method or all methods if neither **rtp** nor **udp** is selected. You can adjust the default compressibility parameter that RSVP uses to compute the compression factor for each flow.

If you use the **ip rsvp admission-control compression predict** command to change the compression method or the number of bytes saved per packet, these values affect only new flows, not existing ones.

There are two approaches to compression—conservative and aggressive. When you predict compression conservatively, you assume savings of fewer bytes per packet, but receive a higher likelihood of guaranteed quality of service (QoS). You are allowed more bandwidth per call, but each link accommodates fewer calls. When you predict compression aggressively, you assume savings of more bytes per packet, but receive a lower likelihood of guaranteed QoS. You are allowed less bandwidth per call, but each link accommodates more calls.

Examples

The following command sets the compressibility parameter for flows using the RTP method to 30 bytes saved per packet:

```
Router(config-if)# ip rsvp admission-control compression predict method rtp bytes-saved 30
```

The following command sets the compressibility parameter for flows using the UDP method to 20 bytes saved per packet:

```
Router(config-if)# ip rsvp admission-control compression predict method udp bytes-saved 20
```

The following command disables RTP header compression prediction:

```
Router(config-if)# no ip rsvp admission-control compression predict method rtp
```

The following command disables UDP header compression prediction:

```
Router(config-if)# no ip rsvp admission-control compression predict method udp
```

Note Disabling the compressibility parameter affects only those flows using the specified method.

Related Commands

Command	Description
show ip rtp header-compression	Displays statistics about RTP header compression.

ip rsvp atm-peak-rate-limit

To set a limit on the peak cell rate (PCR) of reservations for all newly created Resource Reservation Protocol (RSVP) switched virtual circuits (SVCs) established on the current interface or any of its subinterfaces, use the **ip rsvp atm-peak-rate-limit** command in interface configuration mode. To remove the current peak rate limit, in which case the reservation peak rate is limited by the line rate, use the **no** form of this command.

ip rsvp atm-peak-rate-limit *limit*

no ip rsvp atm-peak-rate-limit

Syntax Description

limit	The peak rate limit of the reservation specified, in KB. The minimum value allowed is 1 KB; the maximum value allowed is 2 GB.

Defaults

The peak rate of a reservation defaults to the line rate.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(3)T	This command was introduced.

Usage Guidelines

Each RSVP reservation corresponds to an ATM SVC with a certain PCR, sustainable cell rate (SCR), and maximum burst size. The PCR, also referred to as the peak rate, can be configured by the user or allowed to default to the line rate.

RSVP controlled-load reservations do not define any peak rate for the data. By convention, the allowable peak rate in such reservations is taken to be infinity, which is usually represented by a very large number. Under these circumstances, when a controlled-load reservation is converted to an ATM SVC, the PCR for the SVC becomes correspondingly large and may be out of range for the switch. You can use the **ip rsvp atm-peak-rate-limit** command to limit the peak rate.

The following conditions determine the peak rate limit on the RSVP SVC:

- The peak rate defaults to the line rate.
- If the peak rate is greater than the configured peak rate limiter, the peak rate is lowered to the peak rate limiter.
- The peak rate cannot be less than the reservation bandwidth. If this is the case, the peak rate is raised to the reservation bandwidth.

Note Bandwidth conversions applied to the ATM space from the RSVP space are also applied to the peak rate.

The peak rate limit is local to the router; it does not affect the normal messaging of RSVP. Only the SVC setup is affected. Large peak rates are sent to the next host without modification.

For RSVP SVCs established on subinterfaces, the peak rate limit applied to the subinterface takes effect on all SVCs created on that subinterface. If a peak rate limit is applied to the main interface, the rate limit has no effect on SVCs created on a subinterface of the main interface even if the limit value on the main interface is lower than the limit applied to the subinterface.

For a given interface or subinterface, a peak rate limit applied to that interface affects only new SVCs created on the interface, not existing SVCs.

Note This command is available only on interfaces that support the **ip rsvp svc-required** command.

Use the **show ip rsvp atm-peak-rate-limit** command to determine the peak rate limit set for an interface or subinterface, if one is configured.

Examples

The following example sets the peak rate limit for interface atm2/0/0.1 to 100 KB:

```
interface atm2/0/0.1
 ip rsvp atm-peak-rate-limit 100
```

Related Commands

Command	Description
ip flow-cache feature-accelerate	Enables the allocation of flow acceleration slots in the flow cache.
ip route-cache flow	Enables NetFlow switching for IP routing.
ip rsvp svc-required	Enables creation of an SVC to service any new RSVP reservation made on the interface or subinterface.
ip rsvp atm-peak-rate-limit	Displays the current peak rate limit set for an interface.
show ip rsvp interface	Displays RSVP-related interface information.

ip rsvp authentication

To activate Resource Reservation Protocol (RSVP) cryptographic authentication, use the **ip rsvp authentication** command in interface configuration mode. To deactivate authentication, use the **no** form of this command.

ip rsvp authentication

no ip rsvp authentication

Syntax Description

This command has no arguments or keywords.

Defaults

This command is disabled by default.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

Use the **ip rsvp authentication** command to deactivate and then reactivate RSVP authentication without reentering the other RSVP authentication configuration commands. You should not enable authentication unless you have previously configured a key. If you issue this command before the **ip rsvp authentication key** command, you get a warning message indicating that RSVP discards all messages until you specify a key. The **no ip rsvp authentication** command disables RSVP cryptographic authentication. However, the command does not automatically remove any other authentication parameters that you have configured. You must issue a specific **no ip rsvp authentication** command; for example, **no ip rsvp authentication key**, **no ip rsvp authentication type**, or **no ip rsvp authentication window-size**, if you want to remove them from the configuration.

The **ip rsvp authentication** command is similar to the **ip rsvp neighbor** command. However, the **ip rsvp authentication** command provides better authentication and performs system logging.

Examples

The following command activates authentication on an interface:

```
Router(config-if)# ip rsvp authentication
```

The following command deactivates authentication on an interface:

```
Router(config-if)# no ip rsvp authentication
```

Related Commands

Command	Description
ip rsvp authentication key	Specifies the key (string) for the RSVP authentication algorithm.
ip rsvp authentication type	Specifies the algorithm used to generate cryptographic signatures in RSVP messages.
ip rsvp authentication window-size	Specifies the maximum number of Resource Reservation Protocol (RSVP) authenticated messages that can be received out of order
ip rsvp neighbor	Enables neighbors to request a reservation.

ip rsvp authentication challenge

To make Resource Reservation Protocol (RSVP) perform a challenge-response handshake with any new RSVP neighbors on a network, use the **ip rsvp authentication challenge** command in interface configuration mode. To disable the challenge-response handshake, use the **no** form of this command.

ip rsvp authentication challenge

no ip rsvp authentication challenge

Syntax Description

This command has no arguments or keywords.

Defaults

This command is disabled by default.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

The **ip rsvp authentication challenge** command requires RSVP to perform a challenge-response handshake with any new RSVP neighbors that are discovered on a network. Such a handshake allows the router to thwart RSVP message replay attacks while booting, especially if there is a long period of inactivity from trusted RSVP neighbors following the reboot. If messages from trusted RSVP neighbors arrive very quickly after the router reboots, then challenges may not be required because the router will have reestablished its security associations with the trusted nodes before the untrusted nodes can attempt replay attacks.

If you enable RSVP authentication challenges, you should consider enabling RSVP refresh reduction by using the **ip rsvp signalling refresh reduction** command. While a challenge handshake is in progress, the receiving router initiating the handshake discards all RSVP messages from the node being challenged until the handshake-initiating router receives a valid challenge response.

Note If a neighbor does not reply to the first challenge message after 1 second, Cisco IOS sends another challenge message and waits 2 seconds. If no response is received to the second challenge, Cisco IOS sends another and waits 4 seconds. If no response to the third challenge is received, Cisco IOS sends a fourth challenge and waits 8 seconds. If there is no response to the fourth challenge, Cisco IOS stops the current challenge to that neighbor, logs a system error message, and does not create a security association for that neighbor. This kind of exponential backoff is used to recover from challenges dropped by the network or busy neighbors.

Activating refresh reduction enables the challenged node to resend dropped messages more quickly once the handshake has completed. This causes RSVP to reestablish reservation state faster when the router reboots.

Enable authentication challenges wherever possible to reduce the router's vulnerability to replay attacks.

Examples

The following command shows how to enable RSVP to perform a challenge-response handshake:

```
Router(config-if)# ip rsvp authentication challenge
```

Related Commands

Command	Description
ip rsvp signalling refresh reduction	Enables RSVP refresh reduction.

ip rsvp authentication key

To specify the key (string) for the Resource Reservation Protocol (RSVP) authentication algorithm, use the **ip rsvp authentication key** command in interface configuration mode. To disable the key, use the **no** form of this command.

ip rsvp authentication key *passphrase*

no ip rsvp authentication key

Syntax Description

passphrase	Range from 8 to 40 characters. See "Usage Guidelines" for additional information.

Defaults

This command has no default key.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

Use the **ip rsvp authentication key** command to select the key for the authentication algorithm. This key is a passphrase of 8 to 40 characters. It can include spaces; quotes are not required if spaces are used. The key can consist of more than one word. We recommend that you make the passphrase as long as possible. This key must be the same for all RSVP neighbors on this interface. As with all passwords, you should choose them carefully so that attackers cannot easily guess them.

Here are some guidelines:

- Use a mixture of upper- and lowercase letters, digits, and punctuation.
- If using just a single word, do not use a word contained in any dictionary of any language, spelling lists, or other lists of words.
- Use something easily remembered so you do not have to write it down.
- Do not let it appear in clear text in any file or script or on a piece of paper attached to a terminal.

By default, RSVP authentication keys are stored in clear text in the router configuration file, but they can optionally be stored as encrypted text in the configuration file. To enable key encryption, use the global configuration **key config-key 1** *string* command. After you enter this command, the passphrase parameter of each **ip rsvp authentication key** command is encrypted with the Data Encryption Standard (DES) algorithm when you save the configuration file. If you later issue a **no key config-key 1** *string* command, the RSVP authentication key is stored in clear text again when you save the configuration.

The *string* argument is not stored in the configuration file; it is stored only in the router's private NVRAM and will not appear in the output of a **show run** or **show config** command. Therefore, if you copy the configuration file to another router, any encrypted RSVP keys in that file will not be successfully decrypted by RSVP when the router boots and RSVP authentication will not operate correctly. To recover from this, follow these steps on the new router:

1. For each RSVP interface with an authentication key, issue a **no ip rsvp authentication key** command to clear the old key.
2. For that same set of RSVP interfaces, issue an **ip rsvp authentication key** command to reconfigure the correct clear text keys.
3. Issue a global **key config-key 1** *string* command to reencrypt the RSVP keys for the new router.
4. Save the configuration.

Examples

The following command sets the passphrase to 11223344 in clear text:

```
Router(config-if)# ip rsvp authentication key 11223344
```

To encrypt the authentication key, issue the **key config-key 1** *string* command as follows:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# key config-key 1 11223344
Router(config)# end
```

Related Commands

Command	Description
key config-key	Defines a private DEF key for the router.

ip rsvp authentication lifetime hh:mm:ss

To control how long Resource Reservation Protocol (RSVP) maintains security associations with other trusted RSVP neighbors, use the **ip rsvp authentication lifetime hh:mm:ss** command in interface configuration mode. To disable the lifetime setting, use the **no** form of this command.

ip rsvp authentication lifetime hh:mm:ss

no ip rsvp authentication lifetime hh:mm:ss

Syntax Description

This command has no arguments or keywords.

Defaults

Default security association is 30 minutes; range is 1 second to 24 hours.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

Use the **ip rsvp authentication lifetime hh:mm:ss** command to indicate when to end security associations with RSVP trusted neighbors. If an association's lifetime expires, but at least one valid, RSVP authenticated message was received in that time period, RSVP resets the security association's lifetime to this configured value. When a neighbor stops sending RSVP signaling messages (that is, the last reservation has been torn down), the memory used for the security association is freed as well as when the association's lifetime period ends. The association can be re-created if that RSVP neighbor resumes its signaling. Setting the lifetime to shorter periods allows memory to be recovered faster when the router is handling a lot of short-lived reservations. Setting the lifetime to longer periods reduces the workload on the router when establishing new authenticated reservations.

Use the **clear ip rsvp authentication** command to free security associations before their lifetimes expire.

Examples

The following command sets the lifetime period for 30 minutes and 5 seconds:

```
Router(config-if)# ip rsvp authentication lifetime 00:30:05
```

Related Commands

Command	Description
clear ip rsvp authentication	Eliminates RSVP security associations before their lifetimes expire.

ip rsvp authentication type

To specify the algorithm used to generate cryptographic signatures in Resource Reservation Protocol (RSVP) messages, use the **ip rsvp authentication type** command in interface configuration mode. To disable the type (or to use the default type, **md5**), use the **no** form of this command.

ip rsvp authentication type {**md5** | **sha-1**}

no ip rsvp authentication type

Syntax Description

md5	Rivest, Shamir, and Adelman (RSA) Message Digest 5 algorithm.
sha-1	National Institute of Standards and Technologies (NIST) Secure Hash Algorithm-1; it is newer and more secure than md5.

Defaults

The default type is **md5**.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

Use the **ip rsvp authentication type** command to specify the algorithm used to generate cryptographic signatures in RSVP messages. If you do not specify an algorithm, **md5** is used.

Examples

The following command sets the type to **sha-1**:

```
Router(config-if)# ip rsvp authentication type sha-1
```

Related Commands

Command	Description
ip rsvp authentication key	Specifies the key (string) for the RSVP authentication algorithm.

ip rsvp authentication window-size

To specify the maximum number of Resource Reservation Protocol (RSVP) authenticated messages that can be received out of order, use the **ip rsvp authentication window-size** command in interface configuration mode. To disable the window size (or to use the default value of 1), use the **no** form of this command.

ip rsvp authentication window-size [*n*]

no ip rsvp authentication window-size

Syntax Description

n	(Optional) Maximum number of authenticated messages that can be received out of order. The range is 1 to 64.

Defaults

The default value is 1.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

Use the **ip rsvp authentication window-size** command to specify the maximum number of authenticated messages that can be received out of order. All RSVP authenticated messages include a sequence number that is used to prevent replays of RSVP messages.

With a default window size of one message, RSVP rejects any duplicate authenticated messages because they are assumed to be replay attacks. However, sometimes bursts of RSVP messages become reordered between RSVP neighbors. If this occurs on a regular basis, and you can verify that the node sending the burst of messages is trusted, you can use the **window-size** option to allow for the burst size such that RSVP will not discard such reordered bursts. RSVP will still check for duplicate messages within these bursts.

Examples

The following command sets the window size to 2:

```
Router(config-if)# ip rsvp authentication window-size 2
```

Related Commands

Command	Description
ip rsvp authentication	Activates RSVP cryptographic authentication.

ip rsvp bandwidth

To enable Resource Reservation Protocol (RSVP) for IP on an interface, use the **ip rsvp bandwidth** command in interface configuration mode. To disable RSVP completely, use the **no** form of this command. To eliminate only the subpool portion of the bandwidth, use the **no** form of this command with the keyword **sub-pool**.

ip rsvp bandwidth [*interface-kbps*] [*single-flow-kbps*] [**sub-pool** *kbps*]

no ip rsvp bandwidth [*interface-kbps*] [*single-flow-kbps*] [**sub-pool** *kbps*]

Syntax Description

interface-kbps	(Optional) Maximum amount of bandwidth, in kbps, that may be allocated by RSVP flows. The range is from 1 to 10,000,000.
single-flow-kbps	(Optional) Maximum amount of bandwidth, in kbps, that may be allocated to a single flow. The range is from 1 to 10,000,000. This value is ignored by the Diff-Serv-aware MPLS Traffic Engineering feature available with Cisco IOS Release 12.2(4)T.
sub-pool *kbps*	(Optional) Amount of bandwidth in kbps on interface to be reserved to a portion of the total. The range is from 1 to the value of the *interface-kbps* argument.

Defaults

RSVP is disabled by default.

If the **ip rsvp bandwidth** command is entered but no bandwidth values are supplied (for example, **ip rsvp bandwidth** is entered followed by pressing the Enter key), a default bandwidth value (that is, 75% of the link bandwidth) is assumed for both the *interface-kbps* and *single-flow-kbps* arguments.

Command Modes

Interface configuration

Command History

Release	Modification
11.2	This command was introduced.
12.0(11)ST	The sub-pool option was added.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T. This command was implemented on the Cisco 7500 series and the ATM-permanent virtual circuit (PVC) interface.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.

Usage Guidelines

RSVP cannot be configured with distributed Cisco Express Forwarding (dCEF).

RSVP is disabled by default to allow backward compatibility with systems that do not implement RSVP.

Weighted Random Early Detection (WRED) or fair queueing must be enabled first.

Examples

The following example shows a T1 (1536 kbps) link configured to permit RSVP reservation of up to 1158 kbps, but no more than 100 kbps for any given flow on serial interface 0. Fair queueing is configured with 15 reservable queues to support those reserved flows, should they be required.

```
Router(config)# interface serial 0
Router(config-if)# fair-queue 64 256 15
Router(config-if)# ip rsvp bandwidth 1158 100
```

Related Commands

Command	Description
fair-queue (WFQ)	Enables WFQ for an interface.
ip rsvp neighbor	Enables neighbors to request a reservation.
ip rsvp reservation	Enables a router to behave like it is receiving and forwarding RSVP RESV messages.
ip rsvp sender	Enables a router to behave like it is receiving and forwarding RSVP PATH messages.
ip rsvp udp-multicasts	Instructs the router to generate UDP-encapsulated RSVP multicasts whenever it generates an IP-encapsulated multicast packet.
random-detect (interface)	Enables WRED or DWRED.
show ip rsvp installed	Displays RSVP-related installed filters and corresponding bandwidth information.
show ip rsvp interface	Displays RSVP-related interface information.
show ip rsvp neighbor	Displays current RSVP neighbors.
show ip rsvp reservation	Displays RSVP-related receiver information currently in the database.
show ip rsvp sender	Displays RSVP PATH-related sender information currently in the database.

ip rsvp burst policing

To configure a burst factor within the Resource Reservation Protocol (RSVP) token bucket policer on a per-interface basis, use the **ip rsvp burst policing** command in interface configuration mode. To return to the default value, enter the **no** form of this command.

ip rsvp burst policing [*factor*]

no ip rsvp burst policing

Syntax Description

factor	(Optional) Indicates a burst factor value as a percentage of the requested burst of the receiver.

Defaults

The default value is 200; the minimum value is 100, and the maximum value is 700.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.

Usage Guidelines

You configure the burst police factor per interface, not per flow. The burst factor controls how strictly or loosely the traffic of the sender is policed with respect to burst.

The burst factor applies to all RSVP flows installed on a specific interface. You can configure each interface independently for burst policing.

Examples

Here is an example of the **ip rsvp burst policing** command with a burst factor of 200:

```
ip rsvp burst policing 200
```

ip rsvp data-packet classification none

To turn off (disable) Resource Reservation Protocol (RSVP) data packet classification, use the **ip rsvp data-packet classification none** command in interface configuration mode. To turn on (enable) data-packet classification, use the **no** form of this command.

ip rsvp data-packet classification none

no ip rsvp data-packet classification

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

Interface configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.

Usage Guidelines

Use the **ip rsvp data-packet classification none** command when you do not want RSVP to process every packet. Configuring RSVP so that not every packet is processed eliminates overhead and improves network performance and scalability.

Examples

This section contains two examples of the **ip rsvp data-packet classification none** command. In the first example, data packet classification is turned off (disabled), as follows:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# int atm6/0
Router(config-if)# ip rsvp data-packet classification none
```

In the second example, data packet classification is turned on (enabled), as follows:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# int atm6/0
Router(config-if)# no ip rsvp data-packet classification
```

Related Commands

Command	Description
show ip rsvp interface	Displays RSVP-related interface information.

ip rsvp dsbm candidate

To configure an interface as a Designated Subnetwork Bandwidth Manager (DSBM) candidate, use the **ip rsvp dsbm candidate** command in interface configuration mode. To disable DSBM on an interface, which exempts the interface as a DSBM candidate, use the **no** form of this command.

ip rsvp dsbm candidate [*priority*]

no ip rsvp dsbm candidate

Syntax Description

priority	(Optional) A value in the range from 64 to 128. Among contenders for the DSBM, the interface with the highest priority number wins the DSBM election process.

Defaults

An interface is not configured as a DSBM contender by default. If you use this command to enable the interface as a DSBM candidate and you do not specify a priority, the default priority of 64 is assumed.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

SBM protocol entities, any one of which can manage resources on a segment, can reside in Layer 2 or Layer 3 devices. Many SBM-capable devices may be attached to a shared Layer 2 segment. When more than one SBM exists on a given segment, one of the SBMs is elected to be the DSBM. The elected DSBM is responsible for exercising admission control over requests for resource reservations on a segment, which, in the process, becomes a managed segment. A managed segment includes those interconnected parts of a shared LAN that are not separated by DSBMs. In all circumstances, only one, if any, DSBM exists for each Layer 2 segment.

You can configure an interface to have a DSBM priority in the range from 64 to 128. You can exempt an interface from participation in the DSBM election on a segment but still allow the system to interact with the DSBM if a DSBM is present on the segment. In other words, you can allow a Resource Reservation Protocol (RSVP)-enabled interface on a router connected to a managed segment to be managed by the DSBM even if you do not configure that interface to participate as a candidate in the DSBM election process. To exempt an interface from DSBM candidacy, do not issue the **ip rsvp dsbm candidate** command on that interface.

RSVP cannot be configured with VIP-distributed Cisco Express Forwarding (dCEF).

Examples

The following example configures Ethernet interface 2 as a DSBM candidate with a priority of 100:

```
interface Ethernet2
 ip rsvp dsbm candidate 100
```

Related Commands

Command	Description
debug ip rsvp	Displays information about SBM message processing, the DSBM election process, and standard RSVP enabled message processing information
debug ip rsvp detail	Displays detailed information about RSVP and SBM.
debug ip rsvp detail sbm	Display detailed information about SBM messages only, and SBM and DSBM state transitions
ip rsvp dsbm non-resv-send-limit	Configures the NonResvSendLimit object parameters.
show ip rsvp sbm	Displays information about an SBM configured for a specific RSVP-enabled interface or for all RSVP-enabled interfaces on the router.

ip rsvp dsbm non-resv-send-limit

To configure the NonResvSendLimit object parameters, use the **ip rsvp dsbm non-resv-send-limit** command in interface configuration mode. To use the default NonResvSendLimit object parameters, use the **no** form of this command.

ip rsvp dsbm non-resv-send-limit {**rate** *kbps* | **burst** *kilobytes* | **peak** *kbps* | **min-unit** *bytes* | **max-unit** *bytes*}

no ip rsvp dsbm non-resv-send-limit {**rate** *kbps* | **burst** *kilobytes* | **peak** *kbps* | **min-unit** *bytes* | **max-unit** *bytes*}

Syntax Description

rate *kbps*	The average rate, in kbps, for the Designated Subnetwork Bandwidth Manager (DSBM) candidate. The average rate is a number from 1 to 2,147,483.
burst *kilobytes*	The maximum burst size, in kb, for the DSBM candidate. The maximum burst size is a number from 1 to 2,147,483.
peak *kbps*	The peak rate, in kBps, for the DSBM candidate. The peak rate is a number from 1 to 2,147,483.
min-unit *bytes*	The minimum policed unit, in bytes, for the DSBM candidate. The minimum policed unit is a number from 1 to 2,147,483,647.
max-unit *bytes*	The maximum packet size, in bytes, for the DSBM candidate. The maximum packet size is a number from 1 to 2,147,483,647.

Defaults

The default for the **rate**, **burst**, **peak**, **min-unit**, and **max-unit** keywords is unlimited; all traffic can be sent without a valid Resource Reservation Protocol (RSVP) reservation.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(1)T	This command was introduced.

Usage Guidelines

To configure the per-flow limit on the amount of traffic that can be sent without a valid RSVP reservation, configure the **rate**, **burst**, **peak**, **min-unit**, and **max-unit** values for finite values greater than 0.

To allow all traffic to be sent without a valid RSVP reservation, configure the **rate**, **burst**, **peak**, **min-unit**, and **max-unit** values for unlimited traffic. To configure the parameters for unlimited traffic, you can either omit the command, or enter the **no** form of the command (for example, **no ip rsvp dsbm non-resv-send-limit rate**). Unlimited is the default value.

The absence of the NonResvSendLimit object allows any amount of traffic to be sent without a valid RSVP reservation.

RSVP cannot be configured with VIP-distributed Cisco Express Forwarding (dCEF).

Examples

The following example configures Ethernet interface 2 as a DSBM candidate with a priority of 100, an average rate of 500 kBps, a maximum burst size of 1000 KB, a peak rate of 500 kBps, and unlimited minimum and maximum packet sizes:

```
interface Ethernet2
 ip rsvp dsbm candidate 100
 ip rsvp dsbm non-resv-send-limit rate 500
 ip rsvp dsbm non-resv-send-limit burst 1000
 ip rsvp dsbm non-resv-send-limit peak 500
```

Related Commands

Command	Description
ip rsvp dsbm candidate	Configures an interface as a DSBM candidate.
show ip rsvp sbm	Displays information about an SBM configured for a specific RSVP-enabled interface or for all RSVP-enabled interfaces on the router.

ip rsvp flow-assist

To enable Resource Reservation Protocol (RSVP) to attach itself to NetFlow so that it can leverage NetFlow services to obtain flow classification information about packets in order to update its token bucket and set IP Precedence as required, use the **ip rsvp flow-assist** command in interface configuration mode. To detach RSVP from NetFlow, use the **no** form of this command.

ip rsvp flow-assist

no ip rsvp flow-assist

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default behavior or values. (RSVP does not use NetFlow as a packet filtering mechanism.)

Command Modes

Interface configuration

Command History

Release	Modification
12.0(3)T	This command was introduced.

Usage Guidelines

For RSVP to maintain token buckets and set IP Precedence on packets traversing the flow, it must interact with the underlying packet forwarding mechanism in order to obtain the information it needs. RSVP uses NetFlow for this purpose.

If RSVP is used on non-ATM links and RSVP must set IP Precedence without relying on traffic policing, weighted fair queueing (WFQ) cannot be used. In this case, a method of attaching RSVP to the underlying forwarding mechanism is required. The **ip rsvp flow-assist** command satisfies this requirement. It allows RSVP to attach itself to NetFlow so that it can use NetFlow to obtain information about packets, which it can then use to update its token bucket and set IP Precedence. NetFlow does not police packets or flows. For this reason, when RSVP is configured in this mode, it can only set IP Precedence and not otherwise police traffic.

In summary, you should use this command only when all of the following conditions exist:

- You want to set IP Precedence and type of service (ToS) bits using the **ip rsvp precedence** command or the **ip rsvp tos** command.
- You are not running WFQ on the interface.
- You are not running ATM or you have not specified the **ip rsvp svc-required** command.

When all of these conditions prevail, RSVP is completely detached from the data flow path and, thus, has no way to detect packets. Use of this command enables RSVP to detect packets so that it can mark them.

RSVP cannot be configured with VIP-distributed Cisco Express Forwarding (dCEF).

Use the **show ip rsvp interface** command to determine whether this command is in effect for an interface or subinterface.

Examples

The following example enables RSVP on the ATM interface 2/0/0 to attach itself to NetFlow:

```
interface atm2/0/0
 ip rsvp flow-assist
```

Related Commands

Command	Description
ip rsvp precedence	Allows you to set the IP Precedence values to be applied to packets that either conform to or exceed the RSVP flowspec.
ip rsvp tos	Allows you to set the ToS values to be applied to packets that either conform to or exceed the RSVP flowspec.
ip rsvp svc-required	Enables creation of an SVC to service any new RSVP reservation made on the interface or subinterface.
show ip rsvp interface	Displays RSVP-related interface information.

ip rsvp layer2 overhead

To control the overhead accounting performed by Resource Reservation Protocol (RSVP)/weighted fair queueing (WFQ) when a flow is admitted onto an ATM permanent virtual circuit (PVC), use the **ip rsvp layer2 overhead** command in interface configuration mode. To disable the overhead accounting, use the **no** form of this command.

ip rsvp layer2 overhead [*h c n*]

no ip rsvp layer2 overhead [*h c n*]

Syntax Description

h	(Optional) Layer 2 encapsulation header plus trailer size applied to each Layer 3 packet in bytes. Valid sizes are numbers from 0 to 65535.
c	(Optional) Layer 2 cell header size applied to each Layer 2 cell in bytes. Valid sizes are numbers from 0 to 65535.
n	(Optional) Layer 2 payload size in bytes. Valid sizes are numbers from 0 to 65534.

Defaults

This command is enabled by default on ATM interfaces that are running RSVP and WFQ. You can also use this command on non-ATM interfaces.

The default version of the command, which you specify by entering the default prefix, **default ip rsvp layer2 overhead**, or by omitting the parameters (*h*, *c*, and *n*) and entering the **ip rsvp layer2 overhead** command causes RSVP to determine the overhead values automatically, based on the interface/PVC encapsulation. (Currently, RSVP recognizes ATM Adaptation Layer 5 (AAL5) subnetwork access protocol (SNAP) and MUX (multiplexer) encapsulations.)

On non-ATM/PVC interfaces, the configured *h*, *c*, and *n* parameters determine the values that RSVP uses for its overhead.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.

Usage Guidelines

When an IP flow traverses a link, the overhead of Layer 2 encapsulation can increase the amount of bandwidth that the flow requires to exceed the advertised (Layer 3) rate.

In many cases, the additional bandwidth a flow requires because of Layer 2 overhead is negligible and can be transmitted as part of the 25 percent of the link, which is unreservable and kept for routing updates and Layer 2 overhead. This situation typically occurs when the IP flow uses large packet sizes or when the Layer 2 encapsulation allows for frames of variable size (such as in Ethernet and Frame Relay encapsulations).

However, when a flow’s packet sizes are small and the underlying Layer 2 encapsulation uses fixed-size frames, the Layer 2 encapsulation overhead can be significant, as is the case when Voice Over IP (VoIP) flows traverse ATM links.

To avoid oversubscribing ATM PVCs, which use AAL5 SNAP or AAL5 MUX encapsulations, RSVP automatically accounts for the Layer 2 overhead when admitting a flow. For each flow, RSVP determines the total amount of bandwidth required, including Layer 2 overhead, and uses this value for admission control with the WFQ bandwidth manager.

Note The **ip rsvp layer2 overhead** command does not affect bandwidth requirements of RSVP flows on ATM switched virtual circuits (SVCs).

Examples

In the following example, the total amount of bandwidth reserved with WFQ appears:

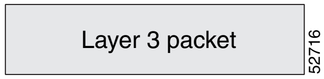
```
Router# show ip rsvp installed detail

RSVP:ATM6/0 has the following installed reservations
RSVP Reservation. Destination is 11.1.1.1, Source is 10.1.1.1,
  Protocol is UDP, Destination port is 1000, Source port is 1000
  Reserved bandwidth:50K bits/sec, Maximum burst:1K bytes, Peak rate:50K bits/sec
  Min Policed Unit:60 bytes, Max Pkt Size:60 bytes
  Resource provider for this flow:
    WFQ on ATM PVC 100/101 on AT6/0: PRIORITY queue 40.  Weight:0, BW 89 kbps
  Conversation supports 1 reservations
  Data given reserved service:0 packets (0M bytes)
  Data given best-effort service:0 packets (0 bytes)
  Reserved traffic classified for 9 seconds
  Long-term average bitrate (bits/sec):0M reserved, 0M best-effort
```

In the preceding example, the flow's advertised Layer 3 rate is 50 kbps. This value is used for admission control with the **ip rsvp bandwidth** value. The actual bandwidth required, inclusive of Layer 2 overhead, is 89 kbps. WFQ uses this value for admission control.

Typically, you should not need to configure or disable the Layer 2 overhead accounting. RSVP uses the advertised Layer 3 flow rate, minimum packet size, and maximum unit size in conjunction with the Layer 2 encapsulation characteristics of the ATM PVC to compute the required bandwidth for admission control. However, you can disable or customize the Layer 2 overhead accounting (for any link type) with the **ip rsvp layer2 overhead** command. The parameters of this command are based on the following steps that show how a Layer 3 packet is fragmented and encapsulated for Layer 2 transmission:

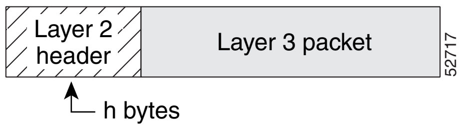
Step 1 Start with a Layer 3 packet, as shown in Figure 1, which includes an IP header and a payload.

Figure 1 Layer 3 Packet



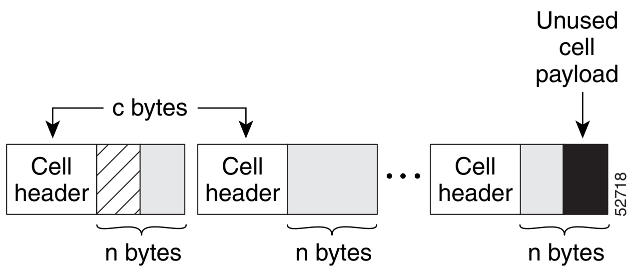
Step 2 Add an encapsulation header or trailer, as shown in Figure 2, of size *h*.

Figure 2 Layer 3 Packet with Layer 2 Header



Step 3 Segment the resulting packet into fixed-sized cells, as shown in Figure 3, with a cell header of c bytes and a cell payload of n bytes.

Figure 3 Segmented Packet



Step 4 Transmit the resulting Layer 2 cells.

More Configuration Examples

In the following example, Layer 2 overhead accounting is disabled for all reservations on the interface and its PVCs:

```
Router(config-if)# no ip rsvp layer2 overhead
```

In the following example, Layer 2 overhead accounting is configured with ATM AAL5 SNAP encapsulation:

```
Router(config-if)# no ip rsvp layer2 overhead 8 5 48
```

In the following example, Layer 2 overhead accounting is configured with ATM AAL5 MUX encapsulation:

```
Router(config-if)# ip rsvp layer2 overhead 0 5 48
```

In the following example, Layer 2 overhead accounting is configured with Ethernet V2.0 encapsulation (including 8-byte preamble, 6-byte source-active (SA) messages, 6-byte destination-active (DA) messages, 2-byte type, and 4-byte frame check sequence (FCS) trailer):

```
Router(config-if)# ip rsvp layer2 overhead 26 0 1500
```

Related Commands

Command	Description
show ip rsvp installed	Displays RSVP-related installed filters and corresponding bandwidth information.

ip rsvp listener

To configure a Resource Reservation Protocol (RSVP) router to listen for Path messages, use the **ip rsvp listener** command in global configuration mode. To disable listening, use the **no** form of this command.

ip rsvp listener *dst* {**UDP** | **TCP** | **any** | *number*} {**any** | *dst-port*} {**announce** | **reply** | **reject**}

no ip rsvp listener

Syntax Description

dst	IP address of the receiving interface.
UDP | **TCP** | **any** | *number*	User Datagram Protocol (UDP), TCP or any protocol to be used on the receiving interface and the UDP or TCP source port number. **Note** If you select *number*, the range is 0 to 255 and the protocol is IP.
any | *dst-port*	Any destination port or a port number from 0 to 65535 for the receiving interface.
announce | **reply** | **reject**	Receiver announces the arrival of the flow at its destination, or sender requests a reply when flow is received, or router sends a PathError (reject) message in response to an incoming Path message that matches specified listener parameters.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

Use the **ip rsvp listener** command to find Path messages so that the router can proxy reservations.

This command is similar to the **ip rsvp reservation** and **ip rsvp reservation-host** commands. However, they do not allow you to specify more than one port or protocol per command so that you may have to enter many commands to proxy for a set of ports and protocols. In contrast, the **ip rsvp listener** command allows you to use a wildcard for a set of ports and protocols by using just that one command.

Examples

In the following example, the sender is requesting that the receiver reply with a Resv message for the flow:

```
Router# configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.

Router(config)# ip rsvp listener 192.168.2.1 any any reply
```

Related Commands

Command	Description
ip rsvp reservation	Enables a router to simulate receiving and forwarding RSVP Resv messages.
ip rsvp reservation-host	Enables a router to simulate a host generating RSVP Resv messages.
show ip rsvp listeners	Displays configured RSVP listeners.

ip rsvp neighbor

To enable neighbors to request a reservation, use the **ip rsvp neighbor** command in interface configuration mode. To disable this feature, use the **no** form of this command.

ip rsvp neighbor *access-list-number*

no ip rsvp neighbor *access-list-number*

Syntax Description

access-list-number	Number of a standard or extended access list. It can be any number in the range from 1 to 199.

Defaults

The router accepts messages from any neighbor.

Command Modes

Interface configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

Use this command to allow only specific Resource Reservation Protocol (RSVP) neighbors to make a reservation. If no limits are specified, any neighbor can request a reservation. If an access list is specified, only neighbors meeting the specified access list requirements can make a reservation.

RSVP cannot be configured with VIP-distributed Cisco Express Forwarding (dCEF).

Examples

The following example allows neighbors meeting access list 1 requirements to request a reservation:

```
interface ethernet 0
 ip rsvp neighbor 1
```

Related Commands

Command	Description
fair-queue (WFQ)	Enables WFQ for an interface.
ip rsvp bandwidth	Enables RSVP for IP on an interface.
ip rsvp reservation	Enables a router to simulate receiving and forwarding RSVP RESV messages.
ip rsvp sender	Enables a router to simulate receiving and forwarding RSVP PATH messages.
ip rsvp udp-multicasts	Instructs the router to generate UDP-encapsulated RSVP multicasts whenever it generates an IP-encapsulated multicast packet.
random-detect (interface)	Enables WRED or DWRED.

Command	Description
show ip rsvp installed	Displays RSVP-related installed filters and corresponding bandwidth information.
show ip rsvp interface	Displays RSVP-related interface information.
show ip rsvp neighbor	Displays current RSVP neighbors.
show ip rsvp reservation	Displays RSVP-related receiver information currently in the database.
show ip rsvp sender	Displays RSVP PATH-related sender information currently in the database.

ip rsvp policy cops minimal

To lower the load of the COPS server and to improve latency times for messages on the governed router, use the **ip rsvp policy cops minimal** command in global configuration mode to restrict the COPS RSVP policy to adjudicate only PATH and RESV messages. To turn off the restriction, use the **no** form of this command.

ip rsvp policy cops minimal

no ip rsvp policy cops minimal

Syntax Description

This command has no arguments or keywords.

Defaults

The default state is OFF, causing all adjudicable RSVP messages to be processed by the configured COPS policy.

Command Modes

Global configuration

Command History

Release	Modification
12.1(1)T	This command was introduced.

Usage Guidelines

When this command is used, COPS does not attempt to adjudicate PATHERROR and RESVERROR messages. Instead, those messages are all accepted and forwarded.

Examples

In the following example, COPS authentication is restricted to PATH and RESV messages:

```
ip rsvp policy cops minimal
```

In the following example, that restriction is removed:

```
no ip rsvp policy cops minimal
```

ip rsvp policy cops report-all

To enable a router to report on its success and failure with outsourcing decisions, use the **ip rsvp policy cops report-all** command in global configuration mode. To return the router to its default, use the **no** form of this command.

ip rsvp policy cops report-all

no ip rsvp policy cops report-all

Syntax Description

This command has no arguments or keywords.

Defaults

The default state of this command is to send reports to the PDP about configuration decisions only.

Command Modes

Global configuration

Command History

Release	Modification
12.1(1)T	This command was introduced.

Usage Guidelines

In the default state, the router reports to the Policy Decision Point (PDP) when the router has succeeded or failed to implement Resource Reservation Protocol (RSVP) configuration decisions.

A *configuration decision* contains at least one of the following:

- A RESV ALLOC context (with or without additional contexts)
- A stateless or named decision object

A decision that does not contain at least one of those elements is an *outsourcing decision.*

Some brands of policy server might expect reports about RSVP messaging, which the default state of the Cisco Common Open Policy Service (COPS) for RSVP does not issue. In such cases, use the **ip rsvp policy cops report-all** command to ensure interoperability between the router and the policy server. Doing so does not adversely affect policy processing on the router.

Unicast FF reservation requests always stimulate a report from the router to the PDP, because those requests contain a RESV ALLOC context (combined with an IN CONTEXT and an OUT CONTEXT).

Examples

In order to show the Policy Enforcement Point (PEP)-to-PDP reporting process, the **debug cops** command in the following example already is enabled when a new PATH message arrives at the router:

```
router-1(config)# ip rsvp policy cops report-all

router-1(config)# 00:02:48:COPS:** SENDING MESSAGE **
Contents of router's request to PDP:
    COPS HEADER:Version 1, Flags 0, Opcode 1 (REQ), Client-type:1, Length:216
    HANDLE (1/1) object. Length:8.    00 00 02 01
    CONTEXT (2/1) object. Length:8.   R-type:5.     M-type:1
    IN_IF (3/1) object. Length:12.   Address:10.1.2.1.    If_index:4
    OUT_IF (4/1) object. Length:12.   Address:10.33.0.1.    If_index:3
    CLIENT SI (9/1) object. Length:168.   CSI data:
    [A 27-line Path message omitted here]
00:02:48:COPS:Sent 216 bytes on socket,
00:02:48:COPS:Message event!
00:02:48:COPS:State of TCP is 4
00:02:48:In read function
00:02:48:COPS:Read block of 96 bytes, num=104 (len=104)
00:02:48:COPS:** RECEIVED MESSAGE **
Contents of PDP's decision received by router:
    COPS HEADER:Version 1, Flags 1, Opcode 2 (DEC), Client-type:1, Length:104
    HANDLE (1/1) object. Length:8.    00 00 02 01
    CONTEXT (2/1) object. Length:8.   R-type:1.     M-type:1
    DECISION (6/1) object. Length:8.   COMMAND cmd:1, flags:0
    DECISION (6/3) object. Length:56.   REPLACEMENT
    [A 52-byte replacement object omitted here]
    CONTEXT (2/1) object. Length:8.   R-type:4.     M-type:1
    DECISION (6/1) object. Length:8.   COMMAND cmd:1, flags:0
00:02:48:Notifying client (callback code 2)
00:02:48:COPS:** SENDING MESSAGE **
Contents of router's report to PDP:
    COPS HEADER:Version 1, Flags 1, Opcode 3 (RPT), Client-type:1, Length:24
    HANDLE (1/1) object. Length:8.    00 00 02 01
    REPORT (12/1) object. Length:8.   REPORT type COMMIT (1)
00:02:48:COPS:Sent 24 bytes on socket,
```

ip rsvp policy cops servers

To specify that Resource Reservation Protocol (RSVP) should use Common Open Policy Service (COPS) policy for remote adjudication, use the **ip rsvp policy cops servers** command in global configuration mode. To turn off the use of COPS for RSVP, use the **no** form of this command.

ip rsvp policy cops [*acl*] **servers** *server-ip* [*server-ip*]

no ip rsvp policy cops [*acl*] **servers**

Syntax Description

acl	(Optional) Specifies the access control list (ACL) whose sessions will be governed by the COPS policy.
server-ip	Specifies the IP addresses of the servers governing the COPS policy. As many as eight servers can be specified, with the first being treated as the primary server.

Defaults

If no ACL is specified, the default behavior is for all reservations to be governed by the specified policy servers.

Command Modes

Global configuration

Command History

Release	Modification
12.1(1)T	This command was introduced.

Usage Guidelines

If more than one server is specified, the first server is treated by RSVP as the primary serer, and functions as such for *all* ACLs specified.

All servers in the list must have the same policy configuration.

If the connection of the router to the server breaks, the router tries to reconnect to that same server. If the reconnection attempt fails, the router then obeys the following algorithm:

If the connection to the Policy Decision Point (PDP) is closed (either because the PDP closed the connection, a TCP/IP error occurred, or the keepalives failed), the Policy Enforcement Point (PEP) issues a CLIENT-CLOSE message and then attempts to reconnect to the same PDP. If the PEP receives a CLIENT-CLOSE message containing a PDP redirect address, the PEP attempts to connect to the redirected PDP. Note the following points:

- If either attempt fails, the PEP attempts to connect to the PDPs previously specified in the **ip rsvp policy cops servers** configuration command, obeying the sequence of servers given in that command, always starting with the first server in that list.
- If the PEP reaches the end of the list of servers without connecting, it waits a certain time (called the *reconnect delay*) before trying again to connect to the first server in the list. This reconnect delay is initially 30 seconds, and doubles each time the PEP reaches the end of the list without having connected, until the reconnect delay becomes its maximum of 30 minutes. As soon as a connection is made, the delay is reset to 30 seconds.

The **no** form of this command need not contain any server IP addresses, but it must contain *all* the previously specified access lists (see the last example in the following section).

Examples

This first example applies the COPS policy residing on server 172.27.224.117 to all reservations passing through router-9. It also identifies the backup COPS server for this router as the one at address 172.27.229.130:

```
router-9(config)# ip rsvp policy cops servers 172.27.224.117 172.27.229.130
```

The next example applies the COPS policy residing on server 172.27.224.117 to reservations passing through router-9 only if they match access lists 40 and 160. Other reservations passing through that router will not be governed by this server. The command statement also identifies the backup COPS server for that router to be the one at address 172.27.229.130:

```
router-9(config)# ip rsvp policy cops 40 160 servers 172.27.224.117 172.27.229.130
```

The following example turns off COPS for the previously specified access lists 40 and 160 (you cannot turn off just one of the previously specified lists):

```
router-9(config)# no ip rsvp policy cops 40 160 servers
```

ip rsvp policy cops timeout

To configure the amount of time the Policy Enforcement Point (PEP) router will retain policy information after losing connection with the Common Open Policy Service (COPS) server, use the **ip rsvp policy cops timeout** command in global configuration mode. To restore the router to the default value (5 minutes), use the **no** form of this command.

ip rsvp policy cops timeout *policy-timeout*

no ip rsvp policy cops timeout

Syntax Description

policy-timeout	Duration of timeout, from 1 to 10,000 seconds.

Defaults

Timeout default is 300 seconds (5 minutes).

Command Modes

Global configuration

Command History

Release	Modification
12.1(1)T	This command was introduced.

Examples

The following example configures the router to time out all policy information relating to a lost server in 10 minutes:

```
ip rsvp policy cops timeout 600
```

The following example resets the timeout to the default value:

```
no ip rsvp policy cops timeout
```

ip rsvp policy default-reject

To reject all messages that do not match the policy access control lists (ACLs), use the **ip rsvp policy default-reject** command in global configuration mode. To restore the default behavior, which passes along all messages that do not match the ACLs, use the **no** form of this command.

ip rsvp policy default-reject

no ip rsvp policy default-reject

Syntax Description

This command has no arguments or keywords.

Defaults

Without this command, the default behavior of Resource Reservation Protocol (RSVP) is to accept, install, or forward all unmatched RSVP messages. Once this command is invoked, all unmatched RSVP messages are rejected.

Command Modes

Global configuration

Command History

Release	Modification
12.1(1)T	This command was introduced.

Usage Guidelines

If COPS is configured without an ACL, or if any policy ACL is configured to use the **permit ip any any** command, the behavior of that ACL will take precedence, and no session will go unmatched.

Note This command makes one exception to its blocking of unmatched messages. It forwards RESVERROR and PATHERROR messages that were generated by its own rejection of RESV and PATH messages. That is done to ensure that the default-reject operation does not remain totally hidden from network managers.

Caution Be extremely careful with this command. It will shut down *all* RSVP processing on the router if access lists are too narrow or if no Common Open Policy Service (COPS) server has been specified. (Use the **ip rsvp policy cops servers** command to specify a COPS server.)

Examples

The following example configures RSVP to reject all unmatched reservations:

```
ip rsvp policy default-reject
```

The following example configures RSVP to accept all unmatched reservations:

```
no ip rsvp policy default-reject
```

ip rsvp policy local

To create a local procedure that determines the use of Resource Reservation Protocol (RSVP) resources in a network, use the **ip rsvp policy local** command in global configuration mode. To disable this feature, use the **no** form of this command.

ip rsvp policy local {**default** | **acl** *acl* [*acl1...acl8*]}

no ip rsvp policy local

Syntax Description

default	Used when an RSVP message does not match any access control list (ACL).
acl *acl* [*acl1...acl8*]	Used when an ACL is specified. Values for each ACL are 1–199. **Note** You must associate at least one ACL with an ACL-based policy. However, you can associate as many as eight.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

Use the **ip rsvp policy local** command to create a local procedure that determines the use of RSVP resources in a network.

There are two types of local policies—one default local policy and one or more ACL-based local policies. The default policy is used when an RSVP message does not match any ACL-based policies. You can use local policies in the following combinations:

- A default policy and no ACL-based policies. All RSVP messages, regardless of reservation (data flow) source or destination, are subject to whatever is defined in this one policy.
- ACL-based policies and no default policy. If an RSVP message does not match the ACLs of any of these local policies, RSVP sees if there are any remote policies in place that allow the router to pass the RSVP message to a Common Open Policy Service (COPS) server for an accept/reject decision. If there are no COPS servers, the RSVP message is accepted. This final decision can be changed to a reject decision with the **ip rsvp policy default-reject** command.
- A default policy and ACL-based policies. If an RSVP message does not match the ACLs of any of these local policies, RSVP will carry out whatever decisions are in the default local policy.

An ACL-based policy must have at least one ACL associated with it, but it can optionally have up to eight ACLs. The ACLs can be standard or extended IP ACLs. They are matched against source/destination addresses/ports based on RSVP objects inside RSVP signaling messages, not on the IP headers of the RSVP messages.

CLI Submodes

After you type the **ip rsvp policy local default** or the **ip rsvp policy local acl** command, you enter local policy CLI submode where you define the properties of the default or ACL-based local policy that you are creating.

Note The local policy that you create automatically rejects all RSVP messages unless you enter a submode command that instructs RSVP on the types of messages to accept.

The submode commands are as follows:

accept—Accepts, but does not forward RSVP messages.

accept {**all** | **path** | **path-error** | **resv** | **resv-error**}

- **all**—Accepts all RSVP messages.
- **path**—Accepts incoming Path messages that match the ACL(s) of this policy. If you omit this command, incoming Path messages that match the ACL(s) are rejected and a PathError message is sent in reply. However, the PathError reply is also subject to local policy.
- **path-error**—Accepts incoming PathError messages that match the ACL(s) of this policy. If you omit this command, incoming PathError messages that match the ACL(s) are rejected.
- **resv**—Accepts incoming Resv messages that match the ACL(s) of this policy and performs any required admission control. If you omit this command, incoming Resv messages that match the ACL(s) are rejected and a ResvError message is sent in reply. However, the ResvError reply is also subject to local policy.
- **resv-error**—Accepts incoming ResvError messages that match the ACL(s) of this policy. If you omit this command, the incoming ResvError messages matching the ACL(s) are rejected.

- **default**—Sets a command to its defaults.
- **exit**—Exits local policy configuration mode.
- **forward**—Accepts and forwards RSVP messages.

  forward {**all** | **path** | **path-error** | **resv** | **resv-error**}

  - **all**—Accepts and forwards all RSVP messages.
  - **path**—Accepts and forwards Path messages that match the ACL(s) of this policy. If you omit this command, Path messages matching the ACL(s) are not forwarded to the next (downstream) hop.
  - **path-error**—Accepts and forwards PathError messages that match the ACL(s) of this policy. If you omit this command, the PathError message matching the ACL(s) are not forwarded to the previous (upstream) hop. You may want to reject outbound PathError messages if you are receiving Path messages from an untrusted node because someone could be trying to port-scan for RSVP. If you reply with a PathError message, then the untrusted node knows you support RSVP and your IP address. Such information could be used to attempt RSVP-based attacks.
  - **resv**—Accepts and forwards Resv messages that match the ACL(s) of this policy. If you omit this command, Resv messages matching the ACL(s) are not forwarded to the previous (upstream) hop.
  - **resv-error**—Accepts and forwards ResvError messages that match the ACL(s) of this policy. If you omit this command, the ResvError message matching the ACL(s) is not forwarded to the next (downstream) hop. You may want to reject outbound ResvError messages if you are receiving Resv messages from an untrusted node because it could be someone trying to port-scan for RSVP. If you reply with a ResvError message, then the untrusted node knows you support RSVP and your IP address. Such information could be used to attempt RSVP-based attacks.

- **local-override**—Overrides any remote (COPS) policy by enforcing the local policy in effect. Finalizes any decisions by this policy. If local-override is omitted, RSVP holds on to the local policy decision to see if a remote (COPS) policy exists that will make a decision on the RSVP message, and only if there is no remote policy decision will the local policy decision be enforced.
- **no**—Negates a command or sets its defaults.
- **preempt-priority** <*start-priority*> [<*hold-priority*>]—Indicates the priorities for resource requests contained in Resv messages that match the ACL(s) of this policy. The range of priority values is 0 to 65,535.

  The *start-priority* argument indicates the priority of the reservation when it is initially installed. The *hold-priority* argument indicates the priority of the reservation after it has been installed. When the *start-priority* argument is higher than the *hold-priority* argument, new reservations can steal bandwidth from longer-lived reservations; however, the start and hold priorities are often configured to be the same value. In order for reservations to be preempted in favor of reservations with higher priorities, there must be no RSVP bandwidth remaining on the interface the Resv message was received on, and a global **ip rsvp policy preempt** command must be issued. RSVP will preempt the first so many lower-priority reservations whose combined bandwidth meets (or exceeds) the amount of bandwidth required by a new, incoming, higher-priority reservation.

  Label switched path (LSP) sessions are ignored when you select reservations to be preempted, because LSP sessions have their own preemption priority scheme that is configured with the **tunnel mpls traffic-eng priority** command.

  In non-LSP sessions, RSVP reservations that are installed on a particular interface are searched in the following order to determine if they are eligible for preemption at a specific preemption priority:

  - Destination address
  - IP protocol type
  - Destination port
  - Source address (fixed-filter (FF) style reservations only)
  - Source port (FF style reservations only)
  - Downstream hop address (for shared media only; for example, Ethernet)

  The above fields are searched from lower to higher values. The source address and source port fields are not checked for shared-explicit (SE) or wildcard-filter (WF) style reservations.

Note If you exit local policy submode without entering any submode commands, the policy you have created will reject *all* RSVP messages.

Examples

In the following example, any RSVP nodes in the 192.168.101.0 subnet can initiate or respond to reservation requests, but all other nodes can respond only to reservation requests. This means that any 192.168.101.x node can send and receive Path, PathError, Resv, or ResvError messages. All other nodes can send only Resv or ResvError messages.

```
Router# configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.

Router(config)# access-list 104 permit ip 192.168.101.0 0.0.0.255 any
Router(config)# ip rsvp policy local acl 104
Router(config-rsvp-policy-local)# forward all
Router(config-rsvp-policy-local)# exit
```

```
Router(config)# ip rsvp policy local default
Router(config-rsvp-policy-local)# forward resv
Router(config-rsvp-policy-local)# forward resverror
Router(config-rsvp-policy-local)# end
```

Related Commands

Command	Description
ip rsvp policy preempt	Enables RSVP to take bandwidth from lower-priority reservations and give it to new, higher-priority reservations.
show ip rsvp policy	Displays the configured local policies.
show ip rsvp policy cops	Displays the policy server address(es), ACL IDs, and current state of the router server connection.
show ip rsvp policy local	Displays selected local policies that have been configured.
tunnel mpls traffic-eng priority	Configures the setup and reservation priority for an MPLS Traffic Engineering tunnel.

ip rsvp policy preempt

To enable Resource Reservation Protocol (RSVP) to take bandwidth from lower-priority reservations and give it to new, higher-priority reservations, use the **ip rsvp policy preempt** command in global configuration mode. To disable this feature, use the **no** form of this command.

ip rsvp policy preempt

no ip rsvp policy preempt

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

Use the **ip rsvp policy preempt** command to enable or disable the preemption parameter for all configured local and remote policies without setting the preemption parameter for each policy individually. This command allows you to give preferential quality of service (QoS) treatment to one group of RSVP hosts or applications over another.

Examples

The following example enables preemption:

```
Router(config)# ip rsvp policy preempt
```

The following example disables preemption:

```
Router(config)# no ip rsvp policy preempt
```

Related Commands

Command	Description
show ip rsvp policy	Displays the configured local policies.

ip rsvp pq-profile

To specify the criteria for Resource Reservation Protocol (RSVP) to use to determine which flows to direct into the priority queue (PQ) within weighted fair queueing (WFQ), use the **ip rsvp pq-profile** command in global configuration mode. To disable the specified criteria, use the **no** form of this command.

ip rsvp pq-profile [*voice-like* | *r'* [*b'*[*p-to-r'* | *ignore-peak-value*]]

no ip rsvp pq-profile

Syntax Description

voice-like	(Optional) Indicates pq-profile parameters sufficient for most voice flows. The default values for r', b', and p-to-r' are used. These values should cause all voice flows generated from Cisco IOS applications and most voice flows from other RSVP applications, such as Microsoft NetMeeting, to be directed into the PQ.
r'	(Optional) Indicates maximum rate of a flow in bytes per second. Valid range is from 1 to 1048576 bytes per second.
b'	(Optional) Indicates maximum burst of a flow in bytes. Valid range is from 1 to 8192 bytes.
p-to-r'	(Optional) Indicates maximum ratio of peak rate to average rate as a percentage. Valid range is from 100 to 4000 percent.
ignore-peak-value	(Optional) Indicates that the peak rate to average rate ratio of the flow is not evaluated when RSVP identifies flows.

Defaults

The default value for r' is 12288 bytes per second.

The default value for b' is 592 bytes.

The default value for p-to-r' is 110 percent.

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.

Usage Guidelines

Use this command to define the profile of RSVP flows to be placed in the PQ within the WFQ system. You can have only one profile in effect at a time. Changes to this configuration affect only new flows, not existing flows.

This command applies only on interfaces that are running RSVP and WFQ.

RSVP recognizes voice flows based upon the r, b, and p values within the flowspec of a receiver. A reserved flow is granted the PQ as long as the flowspec parameters of a receiver meet the following default criteria:

(r <= r') AND (b <= b') AND (p/r <= p-to-r')

Examples

In the following example, voice-like flows (with the default criteria for voice) are put into the PQ:

```
Router(config)# ip rsvp pq-profile
Router(config)# ip rsvp pq-profile voice-like
Router(config)# ip rsvp pq-profile 12288 592 110
Router(config)# default ip rsvp pq-profile
Router# show run | include pq-profile
```

In the following example, all flows matching the voice criteria are put into the PQ:

```
Router(config)# ip rsvp pq-profile 10240 512 100
Router# show run | include pq-profile
ip rsvp pq-profile 10240 512 100
```

In the following example, no flows are put into the PQ:

```
Router(config)# no ip rsvp pq-profile
Router# show run | include pq-profile
no ip rsvp pq-profile
```

In the following example, flows with the criteria given for r' and b' and the default value for p-to-r' are put into the PQ:

```
Router(config)# ip rsvp pq-profile 9000 300
Router# show run | include pq-profile
ip rsvp pq-profile 9000 300 110
```

In the following example, flows with the criteria given for r' and b' and ignoring the peak value of the flow are put into the PQ:

```
Router(config)# ip rsvp pq-profile 9000 300 ignore-peak-value
Router# show run | include pq-profile
ip rsvp pq-profile 9000 300 ignore-peak-value
```

In the following example, Microsoft NetMeeting voice flows with G.711 or adaptive differential pulse code modulation (ADPCM) codecs are put into the PQ:

```
Router(config)# ip rsvp pq-profile 10200 1200
```

ip rsvp precedence

To enable the router to mark the IP Precedence value of the type of service (ToS) byte for packets in a Resource Reservation Protocol (RSVP) reserved path using the specified values for packets that either conform to or exceed the RSVP flowspec, use the **ip rsvp precedence** command in interface configuration mode. To remove existing IP Precedence settings, use the **no** form of this command; if neither the **conform** nor **exceed** keyword is specified, all IP Precedence settings are removed.

ip rsvp precedence {[**conform** *precedence-value*] [**exceed** *precedence-value*]}

no ip rsvp precedence [**conform**] [**exceed**]

Syntax Description

conform *precedence-value*	(Optional) Specifies an IP Precedence value in the range from 0 to 7 for traffic that conforms to the RSVP flowspec. The IP Precedence value is written to the three high-order bits (bits 5 to 7) of the ToS byte in the IP header of a packet. Either the **conform** or **exceed** keyword is required; both keywords may be specified. When used with the **no** form of the command, the **conform** keyword is optional.
exceed *precedence-value*	(Optional) Specifies an IP Precedence value in the range from 0 to 7 for traffic that exceeds the RSVP flowspec. The IP Precedence value is written to the three high-order bits (bits 5 to 7) of the ToS byte in the IP header of a packet. Either the **conform** or **exceed** keyword is required; both keywords may be specified. When used with the **no** form of the command, the **exceed** keyword is optional.

Defaults

The IP Precedence bits of the ToS byte are left unmodified when this command is not used. The default state is equivalent to execution of the **no ip rsvp precedence** command.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(3)T	This command was introduced.

Usage Guidelines

Packets in an RSVP reserved path are divided into two classes: those that conform to the reservation flowspec and those that correspond to a reservation but that exceed, or are outside, the reservation flowspec.

The **ip rsvp precedence** command allows you to set the IP Precedence values to be applied to packets belonging to these two classes. You must specify the IP Precedence value for at least one class of traffic when you use this command. You can use a single instance of the command to specify values for both classes, in which case you can specify the **conform** and **exceed** keywords in either order.

As part of its input processing, RSVP uses the **ip rsvp precedence** command to set the IP Precedence bits on conforming and nonconforming packets. If per-VC DWRED is configured, the system uses the IP Precedence and ToS bit settings on the output interface in its packet drop process. The IP Precedence setting of a packet can also be used by interfaces on downstream routers.

Execution of the **ip rsvp precedence** command causes IP Precedence values for all preexisting reservations on the interface to be modified.

Note RSVP must be enabled on an interface before you can use this command; that is, use of the **ip rsvp bandwidth** command must precede use of the **ip rsvp precedence** command. RSVP cannot be configured with VIP-distributed Cisco Express Forwarding (dCEF).

RSVP receives packets from the underlying forwarding mechanism. Therefore, before you use the **ip rsvp precedence** command to set IP Precedence, one of the following features is required:

- Weighted fair queueing (WFQ) must be enabled on the interface.
- RSVP switched virtual circuits (SVCs) must be used.
- NetFlow must be configured to assist RSVP.

Note Use of the **no** form of this command is not equivalent to giving the **ip rsvp precedence 0** command, which sets all precedence on the packets to 0, regardless of previous precedence setting.

Examples

The following example sets the IP Precedence value to 3 for all traffic on the ATM interface 0 that conforms to the RSVP flowspec and to 2 for all traffic that exceeds the flowspec:

```
interface atm0
 ip rsvp precedence conform 3 exceed 2
```

The following example sets the IP Precedence value to 2 for all traffic on ATM interface 1 that conforms to the RSVP flowspec. The IP Precedence values of those packets that exceed the flowspec are not altered in any way.

```
interface ATM1
 ip rsvp precedence conform 2
```

Related Commands

Command	Description
ip rsvp bandwidth	Enables RSVP for IP on an interface.
ip rsvp policy cops minimal	Lowers the COPS server's load and improves latency times for messages on the governed router.
ip rsvp tos	Allows you to set the ToS values to be applied to packets that either conform to or exceed the RSVP flowspec.
show ip rsvp	Displays the IP Precedence and ToS bit values to be applied to packets that either conform to or exceed the RSVP flowspec for a given interface.

ip rsvp reservation

To enable a router to simulate receiving and forwarding Resource Reservation Protocol (RSVP) RESV messages, use the **ip rsvp reservation** command in global configuration mode. To disable this feature, use the **no** form of this command.

ip rsvp reservation *session-ip-address sender-ip-address* {**tcp** | **udp** | *ip-protocol*} *session-dport sender-sport next-hop-ip-address next-hop-interface* {**ff** | **se** | **wf**} {**rate** | **load**} *bandwidth burst-size*

no ip rsvp reservation *session-ip-address sender-ip-address* {**tcp** | **udp** | *ip-protocol*} *session-dport sender-sport next-hop-ip-address next-hop-interface* {**ff** | **se** | **wf**} {**rate** | **load**} *bandwidth burst-size*

Syntax Description

session-ip-address	For unicast sessions, this is the address of the intended receiver; for multicast sessions, this is the IP multicast address of the session.
sender-ip-address	The IP address of the sender.
tcp | **udp** | *ip-protocol*	TCP, User Datagram Protocol (UDP), or IP protocol in the range from 0 to 255.
session-dport *sender-sport*	*session-dport* is the destination port. *sender-sport* is the source port. Port numbers are specified in all cases, because the use of 16-bit ports following the IP header is not limited to UDP or TCP. If destination is zero, source must be zero, and the implication is that ports are not checked. If destination is nonzero, source must be nonzero (except for **wf** reservations, for which the source port is always ignored and can therefore be zero).
next-hop-ip-address	Host name or address of the receiver or the router closest to the receiver.
next-hop-interface	Next hop interface or subinterface type and number. Interface type can be **ethernet**, **loopback**, **null**, or **serial**.
ff | **se** | **wf**	Reservation style: • Fixed Filter (**ff**) is single reservation. • Shared Explicit (**se**) is shared reservation, limited scope. • Wild Card Filter (**wf**) is shared reservation, unlimited scope.
rate | **load**	QoS guaranteed bit rate service or controlled load service.
bandwidth	Average bit rate, in kbps, to reserve up to 75 percent of the total on the interface. The range is from 1 to 10000000.
burst-size	Maximum burst size (KB of data in queue). The range is from 1 to 65535.

Defaults

The router does not simulate receiving and processing RSVP RESV messages by default.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

Use this command to make the router simulate receiving RSVP RESV messages from a downstream host. This command can be used to proxy RSVP RESV messages for non-RSVP-capable receivers. By giving a local (loopback) next hop address and next hop interface, you can also use this command to proxy RSVP for the router you are configuring.

Note RSVP cannot be configured with VIP-distributed Cisco Express Forwarding (dCEF).

Examples

The following example specifies the use of a Shared Explicit style of reservation and the controlled load service, with token buckets of 100 or 150 kbps and 60 or 65 kbps maximum queue depth:

```
ip rsvp reservation 224.250.0.2 172.16.1.1 UDP 20 30 172.16.4.1 Et1 se load 100 60
ip rsvp reservation 224.250.0.2 172.16.2.1 TCP 20 30 172.16.4.1 Et1 se load 150 65
```

The following example specifies the use of a Wild Card Filter style of reservation and the guaranteed bit rate service, with token buckets of 300 or 350 kbps and 60 or 65 kbps maximum queue depth:

```
ip rsvp reservation 224.250.0.3 0.0.0.0 UDP 20 0 172.16.4.1 Et1 wf rate 300 60
ip rsvp reservation 226.0.0.1 0.0.0.0 UDP 20 0 172.16.4.1 Et1 wf rate 350 65
```

Note that the Wild Card Filter does not admit the specification of the sender; it accepts all senders. This action is denoted by setting the source address and port to zero. If, in any filter style, the destination port is specified to be zero, RSVP does not permit the source port to be anything else; it understands that such protocols do not use ports or that the specification applies to all ports.

Related Commands

Command	Description
fair-queue (WFQ)	Enables WFQ for an interface.
ip rsvp bandwidth	Enables RSVP for IP on an interface.
ip rsvp neighbor	Enables neighbors to request a reservation.
ip rsvp reservation-host	Enables a router to simulate a host generating RSVP RESV messages.
ip rsvp sender	Enables a router to simulate receiving and forwarding RSVP PATH messages.
ip rsvp sender-host	Enables a router to simulate a host generating RSVP PATH messages.
ip rsvp udp-multicasts	Instructs the router to generate UDP-encapsulated RSVP multicasts whenever it generates an IP-encapsulated multicast packet.
random-detect (interface)	Enables WRED or DWRED.
show ip rsvp installed	Displays RSVP-related installed filters and corresponding bandwidth information.
show ip rsvp interface	Displays RSVP-related interface information.
show ip rsvp neighbor	Displays current RSVP neighbors.
show ip rsvp reservation	Displays RSVP-related receiver information currently in the database.
show ip rsvp sender	Displays RSVP PATH-related sender information currently in the database.

ip rsvp reservation-host

To enable a router to simulate a host generating Resource Reservation Protocol (RSVP) RESV messages, use the **ip rsvp reservation-host** command in global configuration mode. To disable this feature, use the **no** form of this command.

ip rsvp reservation-host *session-ip-address sender-ip-address* {**tcp** | **udp** | *ip-protocol*} *session-dport sender-sport* {**ff** | **se** | **wf**} {**rate** | **load**} *bandwidth burst-size*

no ip rsvp reservation-host *session-ip-address sender-ip-address* {**tcp** | **udp** | *ip-protocol*} *session-dport sender-sport* {**ff** | **se** | **wf**} {**rate** | **load**} *bandwidth burst-size*

Syntax Description

session-ip-address	For unicast sessions, this is the address of the intended receiver. IP multicast addresses cannot be used with this argument. It must be a logical address configured on an interface on the router you are configuring.
sender-ip-address	The IP address of the sender.
tcp | **udp** | *ip-protocol*	TCP, User Datagram Protocol UDP, or IP protocol in the range from 0 to 255.
session-dport *sender-sport*	*session-dport* is the destination port. *sender-sport* is the source port. Port numbers are specified in all cases, because the use of 16-bit ports following the IP header is not limited to UDP or TCP. If destination is zero, source must be zero, and the implication is that ports are not checked. If destination is nonzero, source must be nonzero (except for **wf** reservations, for which the source port is always ignored and can therefore be zero).
ff | **se** | **wf**	Reservation style: • Fixed Filter (**ff**) is single reservation. • Shared Explicit (**se**) is shared reservation, limited scope. • Wild Card Filter (**wf**) is shared reservation, unlimited scope.
rate | **load**	QoS guaranteed bit rate service or controlled load service.
bandwidth	Average bit rate, in kbps, to reserve up to 75 percent of the total on the interface. The range is from 1 to 10000000.
burst-size	Maximum burst size (KB of data in queue). The range is from 1 to 65535.

Defaults

The router does not simulate a host generating RSVP RESV messages by default.

Command Modes

Global configuration

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

Use this command to make the router simulate a host generating its own RSVP RESV messages. This command is similar to the **ip rsvp reservation** command, which can cause the router to generate RESV messages on behalf of another host.

The main differences between the **ip rsvp reservation-host** and **ip rsvp reservation** commands follow:

- When you enter the **ip rsvp reservation-host** command, the *session-ip-address* argument must be a local address configured on an interface on the router. Therefore, you cannot proxy a reservation on behalf of a flow destined for another host. Also, you cannot use this command to generate reservation messages for multicast sessions.
- Because the message is assumed to originate from the router you are configuring, you do not specify a next hop or incoming interface for the RSVP RESV message when entering the **ip rsvp reservation-host** command.

Because you cannot use the command to proxy RSVP for non-RSVP-capable hosts or for multicast sessions, the **ip rsvp reservation-host** command is used mostly for debugging and testing purposes.

RSVP cannot be configured with VIP-distributed Cisco Express Forwarding (dCEF).

Examples

The following example specifies the use of a Shared Explicit style of reservation and the controlled load service, with token buckets of 100 or 150 kbps and 60 or 65 kbps maximum queue depth:

```
ip rsvp reservation-host 10.1.1.1 10.30.1.4 UDP 20 30 se load 100 60
ip rsvp reservation-host 10.40.2.2 10.22.1.1 TCP 20 30 se load 150 65
```

Related Commands

Command	Description
fair-queue (WFQ)	Enables WFQ for an interface.
ip rsvp bandwidth	Enables RSVP for IP on an interface.
ip rsvp neighbor	Enables neighbors to request a reservation.
ip rsvp reservation	Enables a router to simulate receiving and forwarding RSVP RESV messages.
ip rsvp sender	Enables a router to simulate receiving and forwarding RSVP PATH messages.
ip rsvp sender-host	Enables a router to simulate a host generating RSVP PATH messages.
ip rsvp udp-multicasts	Instructs the router to generate UDP-encapsulated RSVP multicasts whenever it generates an IP-encapsulated multicast packet.
random-detect (interface)	Enables WRED or DWRED.
show ip rsvp installed	Displays RSVP-related installed filters and corresponding bandwidth information.
show ip rsvp interface	Displays RSVP-related interface information.
show ip rsvp neighbor	Displays current RSVP neighbors.
show ip rsvp reservation	Displays RSVP-related receiver information currently in the database.
show ip rsvp sender	Displays RSVP PATH-related sender information currently in the database.

ip rsvp resource-provider

To configure a resource provider for an aggregate flow, use the **ip rsvp resource-provider** command in interface configuration mode. To disable a resource provider for an aggregate flow, use the **no** form of this command.

ip rsvp resource-provider [*none* | *wfq interface* | *wfq pvc*]

no ip rsvp resource-provider

Note Resource provider was formerly called QoS provider.

Syntax Description

none	(Optional) No resource provider specified regardless of whether one is configured on the interface.
wfq interface	(Optional) Weighted fair queueing (WFQ) specified as the resource provider on the interface.
wfq pvc	(Optional) WFQ specified as the resource provider on the permanent virtual circuit (PVC) or connection.

Defaults

The *wfq interface* is the default resource provider that Resource Reservation Protocol (RSVP) configures on the interface.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.

Usage Guidelines

Use the **ip rsvp resource-provider** command to configure the resource provider with which you want RSVP to interact when it installs a reservation.

To ensure that a flow receives quality of service (QoS) guarantees when using WFQ on a per-flow basis, configure *wfq interface* or *wfq pvc* as the resource provider. To ensure that a flow receives QoS guarantees when using class-based weighted fair queueing (CBWFQ) for data packet processing, configure *none* as the resource provider.

Examples

In the following example, the **ip rsvp resource-provider** command is configured with *wfq interface* or *wfq pvc* as the resource provider, ensuring that a flow receives QoS guarantees when using WFQ on a per-flow basis:

```
Router# configure terminal
Router(config)# int atm6/0
Router(config-if)# ip rsvp resource-provider wfq pvc
Router(config-if)#
```

In the following example, the **ip rsvp resource-provider** command is configured with *wfq interface* or *wfq pvc* as the resource provider, ensuring that a flow receives QoS guarantees when using CBWFQ for data packet processing:

```
Router# configure terminal
Router(config)# int atm6/0
Router(config-if)# ip rsvp resource-provider none
Router(config-if)#
```

Related Commands

Command	Description
show ip rsvp interface	Displays RSVP-related interface information.

ip rsvp sender

To enable a router to simulate receiving and forwarding Resource Reservation Protocol (RSVP) PATH messages, use the **ip rsvp sender** command in global configuration mode. To disable this feature, use the **no** form of this command.

ip rsvp sender *session-ip-address sender-ip-address* {**tcp** | **udp** | *ip-protocol*} *session-dport sender-sport previous-hop-ip-address previous-hop-interface bandwidth burst-size*

no ip rsvp sender *session-ip-address sender-ip-address* {**tcp** | **udp** | *ip-protocol*} *session-dport sender-sport previous-hop-ip-address previous-hop-interface bandwidth burst-size*

Syntax Description

session-ip-address	For unicast sessions, this is the address of the intended receiver; for multicast sessions, it is the IP multicast address of the session.
sender-ip-address	The IP address of the sender.
tcp | **udp** | *ip-protocol*	TCP, User Datagram Protocol (UDP), or IP protocol in the range from 0 to 255.
session-dport *sender-sport*	*session-dport* is the destination port. *sender-sport* is the source port. Port numbers are specified in all cases, because the use of 16-bit ports following the IP header is not limited to UDP or TCP. If destination is zero, source must be zero, and the implication is that ports are not checked. If destination is nonzero, source must be nonzero (except for **wf** reservations, for which the source port is always ignored and can therefore be zero).
previous-hop-ip-address	Address of the sender or the router closest to the sender.
previous-hop-interface	Address of the previous hop interface or subinterface. Interface type can be **ethernet**, **loopback**, **null**, or **serial**.
bandwidth	Average bit rate, in kbps, to reserve up to 75 percent of the total on the interface. The range is from 1 to 10000000.
burst-size	Maximum burst size (KB of data in queue). The range is from 1 to 65535.

Defaults

The router does not simulate receiving and processing RSVP PATH messages by default.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

Use this command to make the router simulate that it is receiving RSVP PATH messages from an upstream host. The command can be used to proxy RSVP PATH messages for non-RSVP-capable senders. By including a local (loopback) previous hop address and previous hop interface, you can also use this command to proxy RSVP for the router you are configuring.

RSVP cannot be configured with VIP-distributed Cisco Express Forwarding (dCEF).

Examples

The following example sets up the router to act like it is receiving RSVP PATH messages using UDP over loopback interface 1:

```
ip rsvp sender 224.250.0.1 172.16.2.1 udp 20 30 172.16.2.1 loopback 1 50 5
ip rsvp sender 224.250.0.2 172.16.2.1 udp 20 30 172.16.2.1 loopback 1 50 5
```

Related Commands

Command	Description
fair-queue (WFQ)	Enables WFQ for an interface.
ip rsvp bandwidth	Enables RSVP for IP on an interface.
ip rsvp neighbor	Enables neighbors to request a reservation.
ip rsvp reservation	Enables a router to simulate receiving and forwarding RSVP RESV messages.
ip rsvp reservation-host	Enables a router to simulate a host generating RSVP RESV messages.
ip rsvp sender-host	Enables a router to simulate a host generating RSVP PATH messages.
ip rsvp udp-multicasts	Instructs the router to generate UDP-encapsulated RSVP multicasts whenever it generates an IP-encapsulated multicast packet.
random-detect (interface)	Enables WRED or DWRED.
show ip rsvp installed	Displays RSVP-related installed filters and corresponding bandwidth information.
show ip rsvp interface	Displays RSVP-related interface information.
show ip rsvp neighbor	Displays current RSVP neighbors.
show ip rsvp reservation	Displays RSVP-related receiver information currently in the database.
show ip rsvp sender	Displays RSVP PATH-related sender information currently in the database.

ip rsvp sender-host

To enable a router to simulate a host generating a Resource Reservation Protocol (RSVP) PATH message, use the **ip rsvp sender-host** command in global configuration mode. To disable this feature, use the **no** form of this command.

ip rsvp sender-host *session-ip-address sender-ip-address* {**tcp** | **udp** | *ip-protocol*} *session-dport sender-sport bandwidth burst-size*

no ip rsvp sender-host *session-ip-address sender-ip-address* {**tcp** | **udp** | *ip-protocol*} *session-dport sender-sport bandwidth burst-size*

Syntax Description

session-ip-address	For unicast sessions, this is the address of the intended receiver; for multicast sessions, it is the IP multicast address of the session.
sender-ip-address	The IP address of the sender. It must be a logical address configured on an interface on the router you are configuring.
tcp | **udp** | *ip-protocol*	TCP, User Datagram Protocol (UDP), or IP protocol in the range from 0 to 255.
session-dport *sender-sport*	*session-dport* is the destination port. *sender-sport* is the source port. Port numbers are specified in all cases, because the use of 16-bit ports following the IP header is not limited to UDP or TCP. If destination is zero, source must be zero, and the implication is that ports are not checked. If destination is nonzero, source must be nonzero (except for **wf** reservations, for which the source port is always ignored and can therefore be zero).
bandwidth	Average bit rate, in kbps, to reserve up to 75 percent of the total on the interface. The range is from 1 to 10000000.
burst-size	Maximum burst size (KB of data in queue). The range is from 1 to 65535.

Defaults

The router does not simulate RSVP PATH message generation by default.

Command Modes

Global configuration

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

Use this command to make the router simulate a host generating its own RSVP PATH messages. This command is similar to the **ip rsvp sender** command, which can cause the router to generate RSVP PATH messages on behalf of another host.

The main differences between the **ip rsvp sender-host** and **ip rsvp sender** commands follow:

- When you enter the **ip rsvp sender-host** command, the *sender-ip-address* argument must be a local address configured on an interface on the router.
- Because the message is assumed to originate from the router you are configuring, you do not specify a previous hop or incoming interface for the RSVP PATH message when entering the **ip rsvp sender-host** command.

Because you cannot use the command to proxy RSVP for non-RSVP-capable hosts, the **ip rsvp sender-host** command is used mostly for debugging and testing purposes.

RSVP cannot be configured with VIP-distributed Cisco Express Forwarding (dCEF).

Examples

The following example sets up the router to act like a host that will send traffic to the given multicast address:

```
ip rsvp sender-host 224.250.0.1 10.24.2.1 udp 20 30 50 5
ip rsvp sender-host 227.0.0.1 10.24.2.1 udp 20 30 50 5
```

Related Commands

Command	Description
fair-queue (WFQ)	Enables WFQ for an interface.
ip rsvp bandwidth	Enables RSVP for IP on an interface.
ip rsvp neighbor	Enables neighbors to request a reservation.
ip rsvp reservation	Enables a router to simulate receiving and forwarding RSVP RESV messages.
ip rsvp reservation-host	Enables a router to simulate a host generating RSVP RESV messages.
ip rsvp sender	Enables a router to simulate receiving and forwarding RSVP PATH messages.
ip rsvp udp-multicasts	Instructs the router to generate UDP-encapsulated RSVP multicasts whenever it generates an IP-encapsulated multicast packet.
random-detect (interface)	Enables WRED or DWRED.
show ip rsvp installed	Displays RSVP-related installed filters and corresponding bandwidth information.
show ip rsvp interface	Displays RSVP-related interface information.
show ip rsvp neighbor	Displays current RSVP neighbors.
show ip rsvp reservation	Displays RSVP-related receiver information currently in the database.
show ip rsvp sender	Displays RSVP PATH-related sender information currently in the database.

ip rsvp signalling dscp

To specify the differentiated services code point (DSCP) value to be used on all RSVP messages transmitted on an interface, use the **ip rsvp signalling dscp** command in interface configuration mode. To disable the **ip rsvp signalling dscp** interface configuration command, use the **no** form of this command.

ip rsvp signalling dscp [*value*]

no ip rsvp signalling dscp

Syntax Description

value	Indicates a DSCP value. A DSCP value can be a number from 0 to 63.

Defaults

The default value is 0, and the maximum value is 63.

Command Modes

Interface configuration

Command History

Release	Modification
12.1	This command was introduced
12.1(2)T	This command was introduced.

Usage Guidelines

You configure the DSCP per interface, not per flow. The DSCP determines the priority that a packet receives from various hops as it travels to its destination.

The DSCP applies to all RSVP flows installed on a specific interface. You can configure each interface independently for DSCP.

Examples

Here is an example of the **ip rsvp signalling dscp** command with a DSCP value of 6:

```
Router(config-if)# ip rsvp signalling dscp 6
Router# show ip rsvp interface detail s2/0

 Se2/0:
   Bandwidth:
     Curr allocated:10K bits/sec
     Max. allowed (total):1536K bits/sec
     Max. allowed (per flow):1536K bits/sec
   Neighbors:
     Using IP enacp:1.  Using UDP encaps:0
   DSCP value used in Path/Resv msgs:0x6
   Burst Police Factor:300%
   RSVP:Data Packet Classification provided by: none
Router#
```

ip rsvp signalling initial-retransmit-delay

To configure the minimum amount of time that a Resource Reservation Protocol (RSVP)-configured router waits for an acknowledgment (ACK) message before retransmitting the same message, use the **ip rsvp signalling initial-retransmit-delay** command in global configuration mode. To reset the delay value to its default (1.0 sec), use the **no** form of this command.

ip rsvp signalling initial-retransmit-delay *delay value*

no ip rsvp signalling initial-retransmit-delay

Syntax Description

delay value	Minimum amount of time that a router waits for an ACK message before the first retransmission of the same message. The delay value ranges from 500 to 30,000 milliseconds (ms).

Defaults

The default value is 1000 ms (1.0 sec).

Command Modes

Global configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

Use the **ip rsvp signalling initial-retransmit-delay** command to configure the minimum amount of time that a router waits for an ACK message before retransmitting the same message.

If an ACK is not received for a state, the first retransmit occurs after the initial retransmit interval. If no ACK is received after the first retransmit, a second retransmit occurs. The message continues to be retransmitted, with the gap between successive retransmits being twice the previous interval, until an ACK is received. Then the message drops into normal refresh schedule if it needs to be refreshed (Path and Resv messages), or is processed (Error or Tear messages). If no ACK is received after five retransmits, the message is discarded as required.

Examples

The following command shows how to set the initial-retransmit-delay to 2 seconds:

```
Router(config)# ip rsvp signalling initial-retransmit-delay 2000
```

The following command shows how to reset the initial-retransmit-delay to the default (1.0 sec):

```
Router(config)# no ip rsvp signalling initial-retransmit-delay
```

ip rsvp signalling patherr state-removal

To reduce the amount of Resource Reservation Protocol (RSVP) traffic messages in a network, use the **ip rsvp signalling patherr state-removal** command in global configuration mode. To disable this feature, use the **no** form of this command.

ip rsvp signalling patherr state-removal [**neighbor** *acl*]

no ip rsvp signalling patherr state-removal

Syntax Description

neighbor	(Optional) Adjacent routers that are part of a particular traffic engineering tunnel.
acl	(Optional) A simple access list with values of 1 to 99.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

Use the **ip rsvp signalling patherr state-removal** command to allow routers to delete Path state automatically when forwarding a PathError message, thereby eliminating the need for a subsequent PathTear message.

This command is most effective when all network nodes support this feature. All nodes need to have the latest version of Cisco IOS software configured.

This command applies only to label-switched path (LSP) flows.

Examples

The following command shows how to enable **ip rsvp signalling patherr state-removal**:

```
Router(config)# ip rsvp signalling patherr state-removal
```

The following command shows how to disable **ip rsvp signalling patherr state-removal**:

```
Router(config)# no ip rsvp signalling patherr state-removal
```

The following command shows how to enable **ip rsvp signalling patherr state-removal** based on an access control list (ACL):

```
Router(config)# ip rsvp signalling patherr state-removal neighbor 98
```

The following command shows how to disable **ip rsvp signalling patherr state-removal** based on an ACL:

```
Router(config)# no ip rsvp signalling patherr state-removal neighbor 98
```

ip rsvp signalling rate-limit

To control the transmission rate for Resource Reservation Protocol (RSVP) messages sent to a neighboring router during a specified amount of time, use the **ip rsvp signalling rate-limit** command in global configuration mode. To disable this feature, use the **no** form of this command.

ip rsvp signalling rate-limit [*burst*][*maxsize*][*period*]

no ip rsvp signalling rate-limit

Syntax Description

burst	(Optional) Maximum number of RSVP messages allowed to be sent to a neighboring router during this interval. Range is 1 to 5000 messages. Default is 4 messages.
maxsize	(Optional) Maximum size of the message queue in bytes. Range is 1 to 5000 bytes. Default is 500 bytes.
period	(Optional) Length of the interval (timeframe) in milliseconds (ms). Range is 10 to 5000 ms. Default is 20 ms.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

Use the **ip rsvp signalling rate-limit** command to prevent a burst of RSVP traffic engineering signalling messages from overflowing the input queue of a receiving router, which would cause the router to drop some messages. Dropped messages substantially delay the completion of signalling.

Examples

The following command shows how every 10 ms 6 messages with a message queue of 500 bytes are sent to any neighboring router:

```
Router(config)# ip rsvp signalling rate-limit 10 6 500
```

Related Commands

Command	Description
debug ip rsvp rate-limit	Displays debug messages for RSVP rate-limiting events.

ip rsvp signalling refresh reduction

To enable Resource Reservation Protocol (RSVP) refresh reduction, use the **ip rsvp signalling refresh reduction** command in global configuration mode. To disable refresh reduction, use the **no** form of this command.

ip rsvp signalling refresh reduction

no ip rsvp signalling refresh reduction

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

RSVP refresh reduction is a set of extensions to reduce the messaging load imposed by RSVP and to help it scale to support larger numbers of flows.

The following features of the refresh reduction standard (RFC 2961) are supported and will be turned on with this command:

- Setting the refresh-reduction-capable bit in message headers
- Message-Identifier (ID) usage
- Reliable messaging with rapid retransmit, acknowledgement (ACK) messages, and MESSAGE_ID objects
- Summary refresh extension
- Bundle messages (reception only)

Refresh reduction requires the cooperation of the neighbor to operate; for this purpose, the neighbor must also support the standard. If the router detects that a directly connected neighbor is not supporting the refresh reduction standard (either through observing the refresh-reduction-capable bit in messages received from the next hop, or by sending a MESSAGE_ID object to the next hop and receiving an error), refresh reduction will not be used on this link irrespective of this command.

Examples

The following command shows how to enable RSVP refresh reduction:

```
Router(config)# ip rsvp signalling refresh reduction
```

The following command shows how to disable RSVP refresh reduction:

```
Router(config)# no ip rsvp signalling refresh reduction
```

Related Commands

Command	Description
show ip rsvp interface	Displays RSVP-related interface information.
show ip rsvp signalling refresh reduction	Displays refresh-reduction parameters for RSVP messages.

ip rsvp signalling refresh reduction ack-delay

To configure the maximum amount of time that a Resource Reservation Protocol (RSVP)-configured router holds on to an acknowledgment (ACK) message before sending it, use the **ip rsvp signalling refresh reduction ack-delay** command in global configuration mode. To reset the ack-delay value to its default (0.25 sec), use the **no** form of this command.

ip rsvp signalling refresh reduction ack-delay *delay-value*

no ip rsvp signalling refresh reduction ack-delay

Syntax Description

delay-value	Maximum amount of time that a router holds on to an ACK message before sending it. Values range from 100 to 10,000 milliseconds (ms).

Defaults

The default value is 250 ms (0.25 sec).

Command Modes

Global configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

Use the **ip rsvp signalling refresh reduction ack-delay** command to configure the maximum amount of time that an RSVP-configured router keeps an ACK message before sending it.

Examples

The following command shows how to set the ack-delay value to 1 second:

```
Router(config)# ip rsvp signalling refresh reduction ack-delay 1000
```

The following command shows how to set the ack-delay value to the default (0.25 sec) value:

```
Router(config)# no ip rsvp signalling refresh reduction ack-delay
```

ip rsvp svc-required

To enable creation of a switched virtual circuit (SVC) to service any new Resource Reservation Protocol (RSVP) reservation made on the interface or subinterface of an Enhanced ATM port adapter (PA-A3), use the **ip rsvp svc-required** command in interface configuration mode. To disable SVC creation for RSVP reservations, use the **no** form of this command.

ip rsvp svc-required

no ip rsvp svc-required

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled. This command applies exclusively to the RSVP-ATM QoS Interworking feature.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(3)T	This command was introduced.

Usage Guidelines

Usually reservations are serviced when RSVP classifies packets and a queueing mechanism schedules them for transmission to manage congestion. Traditionally, RSVP is used with weighted fair queueing (WFQ). When RSVP is coupled with WFQ, all of the packets visible to WFQ are also visible to RSVP, which allows RSVP to identify and take action on packets important to it. In this case, WFQ provides bandwidth guarantees.

However, when the **ip rsvp svc-required** command is used to configure an interface or subinterface, a new SVC is established and used to service each new reservation on the interface. ATM SVCs are used to provide bandwidth guarantees and NetFlow is used on input interfaces to make data packets visible to RSVP.

Note When RSVP is enabled, all packets are processed by the Route Switch Processor (RSP).

This command must be executed on both ends of an SVC driven by RSVP. This command is supported only for the Enhanced ATM port adapter (PA-A3) and its subinterfaces.

Note For this command to take effect, NetFlow must be enabled. Therefore, the **ip route-cache flow** command must precede this command in the configuration.

Use the **show ip rsvp interface** command to determine whether this command is in effect for any interface or subinterface.

Examples

The following example signals RSVP that reservations made on ATM interface 2/0/0 will be serviced by creation of an SVC:

```
interface atm2/0/0
 ip rsvp svc-required
```

Related Commands

Command	Description
ip route-cache flow	Enables NetFlow switching for IP routing.
ip rsvp atm-peak-rate-limit	Sets a limit on the peak cell rate of reservations for all newly created RSVP SVCs established on the current interface or any of its subinterfaces.
ip rsvp precedence	Allows you to set the IP Precedence values to be applied to packets that either conform to or exceed the RSVP flowspec.
show ip rsvp interface	Displays RSVP-related interface information.

ip rsvp tos

To enable the router to mark the five low-order type of service (ToS) bits of the IP header ToS byte for packets in a Resource Reservation Protocol (RSVP) reserved path using the specified values for traffic that either conforms to or exceeds the RSVP flowspec, use the **ip rsvp tos** command in interface configuration mode. To remove existing settings for the ToS bits, use the **no** form of this command; if neither the **conform** nor **exceed** keyword is specified, all settings for the ToS bits are removed.

ip rsvp tos {[**conform** *tos-value*] [**exceed** *tos-value*]}

no ip rsvp tos [**conform**] [**exceed**]

Syntax Description

conform *tos-value*	(Optional) Specifies a ToS value in the range from 0 to 31 for traffic that conforms to the RSVP flowspec. The ToS value is written to the five low-order bits (bits 0 to 4) of the ToS byte in the IP header of a packet. Either the **conform** or **exceed** keyword is required; both keywords may be specified. When used with the **no** form of the command, the **conform** keyword is optional.
exceed *tos-value*	(Optional) Specifies a ToS value in the range from 0 to 31 for traffic that exceeds the RSVP flowspec. The ToS byte value is written to the five low-order bits (bits 0 to 4) of the ToS byte in the IP header of a packet. Either the **conform** or **exceed** keyword is required; both keywords may be specified. When used with the **no** form of the command, the **exceed** keyword is optional.

Defaults

The ToS bits of the ToS byte are left unmodified when this command is not used. (The default behavior is equivalent to use of the **no ip rsvp tos** command.)

Command Modes

Interface configuration

Command History

Release	Modification
12.0(3)T	This command was introduced.

Usage Guidelines

Packets in an RSVP reserved path are divided into two classes: those that conform to the reservation flowspec and those that correspond to a reservation but that exceed, or are outside, the reservation flowspec.

The **ip rsvp tos** command allows you to set the ToS values to be applied to packets belonging to these two classes. You must specify the ToS value for at least one class of traffic when you use this command. You can use a single instance of the command to specify values for both classes, in which case you can specify the **conform** and **exceed** keywords in either order.

As part of its input processing, RSVP uses the **ip rsvp tos** command configuration to set the ToS bits of the ToS byte on conforming and nonconforming packets. If per-virtual circuit (VC) VIP-distributed Weighted Random Early Detection (DWRED) is configured, the system uses the ToS bit and IP Precedence bit settings on the output interface in its packet drop process. The ToS bit and IP Precedence bit settings of a packet can also be used by interfaces on downstream routers.

Execution of the **ip rsvp tos** command causes ToS bit values for all preexisting reservations on the interface to be modified.

Note RSVP must be enabled on an interface before you can use this command; that is, use of the **ip rsvp bandwidth** command must precede use of the **ip rsvp tos** command. RSVP cannot be configured with VIP-distributed Cisco Express Forwarding (dCEF).

Note The **ip rsvp tos** command sets bits 0 to 4 so that in combination with the IP Precedence bit settings every bit in the ToS byte is set. Use of these bits is made with full knowledge of the fact that certain canonical texts that address the ToS byte specify that only bits 1 to 4 are used as the ToS bits.

RSVP receives packets from the underlying forwarding mechanism. Therefore, to use the **ip rsvp tos** command to set the ToS bits, one of the following features is required:

- Weighted fair queueing (WFQ) must be enabled on the interface.
- RSVP switched virtual circuits (SVCs) must be used.
- NetFlow must be configured to assist RSVP.

Note Use of the **no** form of this command is not equivalent to giving the **ip rsvp tos 0** command, which sets all precedence on the packets to 0, regardless of previous precedence setting.

Examples

The following example sets the ToS bits value to 4 for all traffic on ATM interface 1 that conforms to the RSVP flowspec. ToS bits on packets exceeding the flowspec are not altered.

```
interface atm1
 ip rsvp tos conform 4
```

Related Commands

Command	Description
ip rsvp bandwidth	Enables RSVP for IP on an interface.
ip rsvp flow-assist	Enables RSVP to attach itself to NetFlow so that it can leverage NetFlow services.
ip rsvp policy cops minimal	Lowers the COPS server’s load and improves latency times for messages on the governed router.
show ip rsvp	Displays the IP Precedence and ToS bit values to be applied to packets that either conform to or exceed the RSVP flowspec for a given interface.

ip rsvp udp-multicasts

To instruct the router to generate User Datagram Protocol (UDP)-encapsulated Resource Reservation Protocol (RSVP) multicasts whenever it generates an IP-encapsulated multicast packet, use the **ip rsvp udp-multicasts** command in interface configuration mode. To disable this feature, use the **no** form of this command.

ip rsvp udp-multicasts [*multicast-address*]

no ip rsvp udp-multicasts [*multicast-address*]

Syntax Description

multicast-address	(Optional) Host name or UDP multicast address of router.

Defaults

The generation of UDP multicasts is disabled. If a system sends a UDP-encapsulated RSVP message to the router, the router begins using UDP for contact with the neighboring system. The router uses multicast address 224.0.0.14 and starts sending to UDP port 1699. If the command is entered with no specifying multicast address, the router uses the same multicast address.

Command Modes

Interface configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

Use this command to instruct a router to generate UDP-encapsulated RSVP multicasts whenever it generates an IP-encapsulated multicast packet. Some hosts require this trigger from the router.

RSVP cannot be configured with VIP-distributed Cisco Express Forwarding (dCEF).

Examples

The following example reserves up to 7500 kbps on Ethernet interface 2, with up to 1 Mbps per flow. The router is configured to use UDP encapsulation with the multicast address 224.0.0.14.

```
interface ethernet 2
 ip rsvp bandwidth 7500 1000
 ip rsvp udp-multicasts 224.0.0.14
```

Related Commands

Command	Description
ip rsvp bandwidth	Enables RSVP for IP on an interface.
ip rsvp neighbor	Enables neighbors to request a reservation.
ip rsvp reservation	Enables a router to simulate receiving and forwarding RSVP RESV messages.
ip rsvp sender	Enables a router to simulate receiving and forwarding RSVP PATH messages.

ip rtp priority

To reserve a strict priority queue for a set of Real-Time Transport Protocol (RTP) packet flows belonging to a range of User Datagram Protocol (UDP) destination ports, use the **ip rtp priority** command in interface configuration mode. To disable the strict priority queue, use the **no** form of this command.

ip rtp priority *starting-rtp-port-number port-number-range bandwidth*

no ip rtp priority

Syntax Description

starting-rtp-port-number	The starting RTP port number. The lowest port number to which the packets are sent. The port number can be a number from 2000 to 65,535.
port-number-range	The range of UDP destination ports. Number, when added to the *starting-rtp-port-number* argument, that yields the highest UDP port number. The range of UDP destination ports is from 0 to 16,383.
bandwidth	Maximum allowed bandwidth, in kbps. The maximum allowed bandwidth is from 0 to 2,000.

Defaults

No default behavior or values

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

This command is most useful for voice applications, or other applications that are delay-sensitive.

This command extends and improves on the functionality offered by the **ip rtp reserve** command by allowing you to specify a range of UDP/RTP ports whose voice traffic is guaranteed strict priority service over any other queues or classes using the same output interface. Strict priority means that if packets exist in the priority queue, they are dequeued and sent first—that is, before packets in other queues are dequeued. We recommend that you use the **ip rtp priority** command instead of the **ip rtp reserve** command for voice configurations.

This command can be used in conjunction with either weighted fair queueing (WFQ) or class-based WFQ (CBWFQ) on the same outgoing interface. In either case, traffic matching the range of ports specified for the priority queue is guaranteed strict priority over other CBWFQ classes or WFQ flows; voice packets in the priority queue are always serviced first.

Remember the following guidelines when using the **ip rtp priority** command:

- When used in conjunction with WFQ, the **ip rtp priority** command provides strict priority to voice, and WFQ scheduling is applied to the remaining queues.
- When used in conjunction with CBWFQ, the **ip rtp priority** command provides strict priority to voice. CBWFQ can be used to set up classes for other types of traffic (such as Systems Network Architecture [SNA]) that need dedicated bandwidth and need to be treated better than best effort and not as strict priority; the nonvoice traffic is serviced fairly based on the weights assigned to the enqueued packets. CBWFQ can also support flow-based WFQ within the default CBWFQ class if so configured.

Remember the following guidelines when configuring the *bandwidth* argument:

- It is always safest to allocate to the priority queue slightly more than the known required amount of bandwidth, to allow room for network bursts.
- The IP RTP Priority admission control policy takes RTP header compression into account. Therefore, while configuring the *bandwidth* argument of the **ip rtp priority** command you need to configure only for the bandwidth of the compressed call. Because the *bandwidth* argument is the maximum total bandwidth, you need to allocate enough bandwidth for all calls if there will be more than one call.
- Configure a bandwidth that allows room for Layer 2 headers. The bandwidth allocation takes into account the payload plus the IP, UDP, and RTP headers but does not account for Layer 2 headers. Allowing 25 percent bandwidth for other overhead is conservative and safe.
- The sum of all bandwidth allocation for voice and data flows on an interface cannot exceed 75 percent of the total available bandwidth, unless you change the default maximum reservable bandwidth. To change the maximum reservable bandwidth, use the **max-reserved-bandwidth** command on the interface.

For more information on IP RTP Priority bandwidth allocation, refer to the section "IP RTP Priority" in the chapter "Congestion Management Overview" in the *Cisco IOS Quality of Service Solutions Configuration Guide*.

Examples

The following example first defines a CBWFQ configuration and then reserves a strict priority queue with the following values: a starting RTP port number of 16384, a range of 16383 UDP ports, and a maximum bandwidth of 40 kbps:

```
! The following commands define a class map:
class-map class1
 match access-group 101
 exit

! The following commands create and attach a policy map:
policy-map policy1
class class1
 bandwidth 3000
 queue-limit 30
 random-detect
 random-detect precedence 0 32 256 100
 exit
interface Serial1
 service-policy output policy1

! The following command reserves a strict priority queue:
 ip rtp priority 16384 16383 40
```

Related Commands

Command	Description
bandwidth (policy-map class)	Specifies or modifies the bandwidth allocated for a class belonging to a policy map.
fair queue (WFQ)	Enables WFQ for an interface.
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.
ip rtp reserve	Reserves a special queue for a set of RTP packet flows belonging to a range of UDP destination ports.
max-reserved-bandwidth	Changes the percent of interface bandwidth allocated for CBWFQ, LLQ, and IP RTP Priority.
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
ppp multilink	Enables MLP on an interface and, optionally, enables dynamic bandwidth allocation.
ppp multilink fragment-delay	Configures a maximum delay allowed for transmission of a packet fragment on an MLP bundle.
ppp multilink interleave	Enables interleaving of RTP packets among the fragments of larger packets on an MLP bundle.
priority	Gives priority to a class of traffic belonging to a policy map.
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 queue	Displays the contents of packets inside a queue for a particular interface or VC.

match access-group

To configure the match criteria for a class map on the basis of the specified access control list (ACL), use the **match access-group** command in class-map configuration mode. To remove ACL match criteria from a class map, use the **no** form of this command.

match access-group {*access-group* | **name** *access-group-name*}

no match access-group *access-group*

Syntax Description

access-group	A numbered ACL whose contents are used as the match criteria against which packets are checked to determine if they belong to this class. An ACL number can be a number from 1 to 2699.
name *access-group-name*	A named ACL whose contents are used as the match criteria against which packets are checked to determine if they belong to this class. The name can be a maximum of 40 alphanumeric characters

Defaults

No default behavior or values

Command Modes

Class-map configuration

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.

Usage Guidelines

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

The **match access-group** command specifies a numbered or named ACL whose contents are used as the match criteria against which packets are checked to determine if they belong to the class specified by the class map.

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

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

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

Examples

The following example specifies a class map called acl144 and configures the ACL numbered 144 to be used as the match criteria for this class:

```
class-map acl144
 match access-group 144
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class.
match input-interface	Configures a class map to use the specified input interface as a match criterion.
match mpls experimental	Configures a class map to use the specified EXP field value as a match criterion.
match protocol	Configures the match criteria for a class map on the basis of the specified protocol.

match any

To configure the match criteria for a class map to be successful match criteria for all packets, use the **match any** command in class-map configuration mode. To remove all criteria as successful match criteria, use the **no** form of this command.

match any

no match any

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

Class-map configuration

Command History

Release	Modification
12.0(5)XE	This command was introduced.
12.0(5)T	This command was integrated into Cisco IOS Release 12.0(5)T.
12.1(1)E	This command was integrated into Cisco IOS Release 12.1(1)E.

Examples

In the following configuration, all packets leaving Ethernet interface 1/1 will be policed based on the parameters specified in policy-map class configuration mode.

```
Router(config)# class-map matchany
Router(config-cmap)# match any
Router(config-cmap)# exit

Router(config)# policy-map policy1
Router(config-pmap)# class class4
Router(config-pmap-c)# police 8100 1500 2504 conform-action transmit exceed-action
set-qos-transmit 4
Router(config-pmap-c)# exit

Router(config)# interface e1/1
Router(config-if)# service-policy output policy1
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class.
match input-interface	Configures a class map to use the specified input interface as a match criterion.
match protocol	Configures the match criteria for a class map on the basis of the specified protocol.

match class-map

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

match class-map *class-map-name*

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

Syntax Description

class-map-name	Specifies the name of the traffic class to use as a match criterion.

Defaults

No default behavior or values

Command Modes

Class-map configuration

Command History

Release	Modification
12.0(5)XE	This command was introduced.
12.1(1)E	This command was integrated into Cisco IOS Release 12.1(1)E.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.

Usage Guidelines

The only method of including both match-any and match-all characteristics in a single traffic class is to use the **match class-map** command. To combine match-any and match-all characteristics into a single class, a traffic class created with the match-any instruction must use a class configured with the match-all instruction as a match criterion (through the **match class-map** command), or vice versa.

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

Examples

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

```
Router(config)# class-map match-any class2
Router(config-cmap)# match protocol ip
Router(config-cmap)# match qos-group 3
Router(config-cmap)# match access-group 2
Router(config-cmap)# exit
```

```
Router(config)# class-map match-all class1
Router(config-cmap)# match class-map class2
Router(config-cmap)# match destination-address mac 1.1.1
Router(config-cmap)# exit
```

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

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

```
Router(config)# class-map match-all class3
Router(config-cmap)# match protocol ip
Router(config-cmap)# match qos-group 4
Router(config-cmap)# exit

Router(config)# class-map match-any class4
Router(config-cmap)# match class-map class3
Router(config-cmap)# match destination-address mac 1.1.1
Router(config-cmap)# match access-group 2
Router(config-cmap)# exit

Router(config)# policy-map policy1
Router(config-pmap)# class class4
Router(config-pmap-c)# police 8100 1500 2504 conform-action transmit exceed-action
set-qos-transmit 4
Router(config-pmap-c)# exit
```

Related Commands

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

match cos

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

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

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

Syntax Description

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

Defaults

Disabled

Command Modes

Class-map configuration

Command History

Release	Modification
12.1(5)T	This command was introduced.

Examples

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

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

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

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

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

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

```
Router(config)# interface fa0/0.1
Router(config-if)# service-policy output cos-based-treatment
```

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

Related Commands

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

match destination-address mac

To use the destination MAC address as a match criterion, use the **match destination-address mac** command in class-map configuration mode. To remove a previously specified destination MAC address as a match criterion, use the **no** form of this command.

match destination-address mac *address*

no match destination-address mac *address*

Syntax Description

address	Specifies the specific destination MAC address to be used as a match criterion.

Defaults

No default behavior or values

Command Modes

Class-map configuration

Command History

Release	Modification
12.0(5)XE	This command was introduced.
12.1(1)E	This command was integrated into Cisco IOS Release 12.1(1)E.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.

Examples

The following example specifies a class map called macaddress and specifies the destination MAC address to be used as the match criterion for this class.

```
class-map macaddress
match destination-address mac 00:00:00:00:00:00
```

Related Commands

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

match discard-class

To match packets of a certain discard class, use the **match discard-class** command in class-map configuration mode.

match discard-class *class-number*

Syntax Description

class-number	Number of the discard class being matched. Valid values are 0 to 7.

Defaults

Packets will not be classified as expected.

Command Modes

Class-map configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.

Examples

The following example shows that packets in discard class 2 are matched:

```
match discard-class 2
```

Related Commands

Command	Description
set discard-class	Marks a packet with a discard-class value.

match dscp

To identify a specific IP differentiated service code point (DSCP) value as a match criterion, use the **match dscp** command in class-map configuration mode. To remove a specific DSCP value from a class map, use the **no** form of this command.

match [**ip**] **dscp** *dscp-value* [*dscp-value dscp-value dscp-value dscp-value dscp-value dscp-value dscp-value*]

no match [**ip**] **dscp** *dscp-value* [*dscp-value dscp-value dscp-value dscp-value dscp-value dscp-value dscp-value*]

Syntax Description

ip	(Optional) Specifies that the match is for IPv4 packets only. If not used, the match is on both IPv4 and IPv6 packets.
dscp-value	Specifies the exact value from 0 to 63 used to identify an IP DSCP value.

Defaults

Matching on both IPv4 and IPv6 packets is the default.

Command Modes

Class-map configuration

Command History

Release	Modification
12.2(13)T	This command was introduced. This command replaces the **match ip dscp** command.

Usage Guidelines

DSCP Values

Up to eight DSCP values can be matched in one match statement. For example, if you wanted the DCSP values of 0, 1, 2, 3, 4, 5, 6, or 7 (note that only one of the IP DSCP values must be a successful match criterion, not all of the specified DSCP values), enter the **match dscp 0 1 2 3 4 5 6 7** command.

This command is used by the class map to identify a specific DSCP value marking on a packet. In this context, *dscp-value* arguments are used as markings only and have no mathematical significance. For instance, the *dscp-value* of 2 is not greater than 1. The value simply indicates that a packet marked with the *dscp-value* of 2 is different from a packet marked with the *dscp-value* of 1. The treatment of these marked packets is defined by the user through the setting of QoS policies in policy-map class configuration mode.

Match IPv6 Packets on DSCP Values

To match DSCP values for IPv6 packets only, the **match protocol ipv6** command must also be used. Without that command, the DSCP match defaults to match both IPv4 and IPv6 packets.

Match IPv4 Packets on DSCP Values

To match DSCP values for IPv4 packets only, use the **ip** keyword. Without the **ip** keyword, the match occurs on both IPv4 and IPv6 packets. Alternatively, the **match protocol ip** command can be used with the **match dscp** command to classify only IPv4 packets.

Examples

Priority50 Service Policy Matching DSCP Value

The following example shows how to configure the service policy called "priority50" and attach service policy "priority50" to an interface. In this example, the class map called "ipdscp15" will evaluate all packets entering interface Fast Ethernet 1/0/0 for an IP DSCP value of 15. If the incoming packet has been marked with the IP DSCP value of 15, the packet will be treated as priority traffic and will be allocated with bandwidth of 50 kbps.

```
Router(config)# class-map ipdscp15
Router(config-cmap)# match ip dscp 15
Router(config)# exit
Router(config)# policy-map priority50
Router(config-pmap)# class ipdscp15
Router(config-pmap-c)# priority 50
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface fa1/0/0
Router(config-if)# service-policy output priority50
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class.
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
service-policy	Attaches a policy map to an input interface or VC, or an output interface or VC, to be used as the service policy for that interface or VC.
set dscp	Marks the DSCP value for packets within a traffic class.
show class-map	Displays all class maps and their matching criteria.

match fr-dlci

To specify the Frame Relay data-link connection identifier (DLCI) number as a match criterion in a class map, use the **match fr-dlci** command in class-map configuration mode. To remove a previously specified DLCI number as a match criterion, use the **no** form of this command.

match fr-dlci *dlci-number*

no match fr-dlci *dlci-number*

Syntax Description

dlci-number	Number of the DLCI associated with the packet.

Defaults

No default behavior or values

Command Modes

Class-map configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

This match criterion can be used in main interfaces and point-to-multipoint subinterfaces in Frame Relay networks, and it can also be used in hierarchical policy maps.

Examples

In the following example a class map called "class1" has been created and the Frame Relay DLCI number of 500 has been specified as a match criterion. Packets matching this criterion are placed in class1.

```
Router(config)# class-map class1
Router(config-cmap)# match fr-dlci 500
Router(config-cmap)# end
```

Related Commands

Command	Description
show class-map	Displays all class maps and their matching criteria.
show policy-map interface	Displays the packet statistics of all classes that are configured for all service policies either on the specified interface or subinterface or on a specific PVC on the interface.

match input-interface

To configure a class map to use the specified input interface as a match criterion, use the **match input-interface** command in class-map configuration mode. To remove the input interface match criterion from a class map, use the **no** form of this command.

match input-interface *interface-name*

no match input-interface *interface-name*

Syntax Description

interface-name	Name of the input interface to be used as match criteria.

Defaults

No default behavior or values

Command Modes

Class-map configuration

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.

Usage Guidelines

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

The **match input-interface** command specifies the name of an input interface to be used as the match criterion against which packets are checked to determine if they belong to the class specified by the class map.

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

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

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

Examples

The following example specifies a class map called eth1 and configures the input interface named ethernet1to be used as the match criterion for this class:

```
class-map eth1
 match input-interface ethernet1
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class.
match access-group	Configures the match criteria for a class map based on the specified ACL.
match mpls experimental	Configures a class map to use the specified EXP field value as a match criterion.
match protocol	Configures the match criteria for a class map on the basis of the specified protocol.

match ip dscp

Note Effective with Release 12.2(13)T, the **match ip dscp** command is replaced by the **match dscp** command. See the **match dscp** command for more information.

To identify a specific IP differentiated service code point (DSCP) value as a match criterion, use the **match ip dscp** class-map configuration command. To remove a specific IP DSCP value from a class map, use the **no** form of this command.

match ip dscp *ip-dscp-value* [*ip-dscp-value ip-dscp-value ip-dscp-value ip-dscp-value ip-dscp-value ip-dscp-value ip-dscp-value*]

no match ip dscp *ip-dscp-value* [*ip-dscp-value ip-dscp-value ip-dscp-value ip-dscp-value ip-dscp-value ip-dscp-value ip-dscp-value*]

Syntax Description

ip-dscp-value	Specifies the exact value from 0 to 63 used to identify an IP DSCP value.

Defaults

This command has no default behavior or values.

Command Modes

Class-map configuration

Command History

Release	Modification
12.0(5)XE	This command was introduced.
12.0(9)S	This command was integrated in Cisco IOS Release 12.0(9)S.
12.1(2)T	This command was integrated in Cisco IOS Release 12.1(2)T.
12.2(13)T	This command was replaced by the **match dscp** command.

Usage Guidelines

Up to eight IP DSCP values can be matched in one match statement. For example, if you wanted the IP DCSP values of 0, 1, 2, 3, 4, 5, 6, or 7 (note that only one of the IP DSCP values must be a successful match criterion, not all of the specified IP DSCP values), enter the **match ip dscp 0 1 2 3 4 5 6 7** command.

This command is used by the class map to identify a specific IP DSCP value marking on a packet. The *ip-dscp-value* arguments are used as markings only. The IP DSCP values have no mathematical significance. For instance, the *ip-dscp-value* of 2 is not greater than 1. The value simply indicates that a packet marked with the *ip-dscp-value* of 2 is different than a packet marked with the *ip-dscp-value* of 1. The treatment of these marked packets is defined by the user through the setting of QoS policies in policy-map class configuration mode.

Examples

The following example shows how to configure the service policy called priority50 and attach service policy priority50 to an interface. In this example, the class map called ipdscp15 will evaluate all packets entering interface Fast Ethernet 1/0/0 for an IP DSCP value of 15. If the incoming packet has been marked with the IP DSCP value of 15, the packet will be treated with a priority level of 55.

```
Router(config)# class-map ipdscp15
Router(config-cmap)# match ip dscp 15
Router(config)# exit
Router(config)# policy-map priority55
Router(config-pmap)# class ipdscp15
Router(config-pmap-c)# priority 55
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface fa1/0/0
Router(config-if)# service-policy input priority55
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class.
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
service-policy	Attaches a policy map to an input interface or VC, or an output interface or VC, to be used as the service policy for that interface or VC.
set ip dscp	Marks the IP DSCP value for packets within a traffic class.
show class-map	Displays all class maps and their matching criteria.

match ip precedence

Note Effective with Release 12.2(13)T, the **match ip precedence** command is replaced by the **match precedence** command. See the **match precedence** command for more information.

To identify IP precedence values as match criteria, use the **match ip precedence** command in class-map configuration mode. To remove IP precedence values from a class map, use the **no** form of this command.

match ip precedence *ip-precedence-value* [*ip-precedence-value ip-precedence-value ip-precedence-value*]

no match ip precedence *ip-precedence value* [*ip-precedence-value ip-precedence-value ip-precedence-value*]

Syntax Description

ip-precedence-value	Specifies the exact value from 0 to 7 used to identify an IP precedence value.

Defaults

This command has no default behavior or values.

Command Modes

Class-map configuration

Command History

Release	Modification
12.0(5)XE	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(13)T	This command was replaced by the **match precedence** command.

Usage Guidelines

Up to four precedence values can be matched in one match statement. For example, if you wanted the IP precedence values of 0, 1, 2, or 3 (note that only one of the IP precedence values must be a successful match criterion, not all of the specified IP precedence values), enter the **match ip precedence 0 1 2 3** command.

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

Examples

The following example shows how to configure the service policy called priority50 and attach service policy priority50 to an interface. In this example, the class map called ipprec5 will evaluate all packets entering Fast Ethernet interface 1/0/0 for an IP precedence value of 5. If the incoming packet has been marked with the IP precedence value of 5, the packet will be treated with a priority level of 50.

```
Router(config)# class-map ipprec5
Router(config-cmap)# match ip precedence 5
Router(config)# exit
Router(config)# policy-map priority50
Router(config-pmap)# class ipprec5
Router(config-pmap-c)# priority 50
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface fa1/0/0
Router(config-if)# service-policy input priority50
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class.
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
set ip precedence	Sets the precedence value in the IP header.
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 class-map	Displays all class maps and their matching criteria, or a specified class map and its matching criteria.

match ip rtp

To configure a class map to use the Real-Time Protocol (RTP) protocol port as the match criterion, use the **match ip rtp** command in class-map configuration mode. To remove the RTP protocol port match criterion, use the **no** form of this command.

match ip rtp *starting-port-number port-range*

no match ip rtp

Syntax Description

starting-port-number	The starting RTP port number. Values range from 2000 to 65535.
port-range	The RTP port number range. Values range from 0 to 16383.

Defaults

No default behavior or values

Command Modes

Class-map configuration

Command History

Release	Modification
12.1(2)T	This command was introduced.

Usage Guidelines

This command is used to match IP RTP packets that fall within the specified port range. It matches packets destined to all even User Datagram Port (UDP) port numbers in the range <starting port range> <starting port range + port range>.

Use of an RTP port range as the match criterion is particularly effective for applications that use RTP, such as voice or video.

Examples

The following example specifies a class map called eth1 and configures the RTP port number 2024 and range 1000 to be used as the match criteria for this class:

```
class-map eth1
 match ip rtp 2024 1000
```

Related Commands

Command	Description
ip rtp priority	Reserves a strict priority queue for a set of RTP packet flows belonging to a range of UDP destination ports.
match access-group	Configures the match criteria for a class map based on the specified ACL number.

match mpls experimental

To configure a class map to use the specified value of the experimental (EXP) field as a match criterion, use the **match mpls experimental** command in class-map configuration mode. To remove the EXP field match criterion from a class map, use the **no** form of this command.

match mpls experimental *number*

no match mpls experimental *number*

Syntax Description

number	EXP field value (any number from 0 through 7) to be used as a match criterion. Numbers can be space delimited (for example, 3 4 7).

Defaults

No default behavior or values

Command Modes

Class-map configuration

Command History

Release	Modification
12.0(7)XE1	This command was introduced.
12.1(1)E	This command was integrated into Cisco IOS Release 12.1 E.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1 T.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(4)T	This command was implemented on the Cisco MGX 8850 switch and the MGX 8950 switch with a Cisco MGX RPM-PR card.
12.2(4)T2	This command was implemented on the Cisco 7500 series.

Usage Guidelines

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

The **match mpls experimental** command specifies the name of an EXP field value to be used as the match criterion against which packets are checked to determine if they belong to the class specified by the class map.

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

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

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

Examples

The following example specifies a class map called eth1 and configures the Multiprotocol Label Switching (MPLS) experimental values of 1 and 2 to be used as the match criterion for this class:

```
Router(config)# class-map eth1
Router(config-cmap)# match mpls experimental 1 2
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class.
match access-group	Configures the match criteria for a class map based on the specified ACL.
match input-interface	Configures a class map to use the specified input interface as a match criterion.
match protocol	Matches traffic by a particular protocol.
match qos-group	Configures the match criteria for a class map based on the specified protocol.

match mpls experimental topmost

To match the experimental (EXP) value in the topmost label, use the **match mpls experimental topmost** command in class-map configuration mode.

match mpls experimental topmost *value*

Syntax Description

value	Value of the Multiprotocol Label Switching (MPLS) EXP field in the topmost label header. Valid values are 0 to 7.

Defaults

Packets will not be classified as expected.

Command Modes

Class-map configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

You can enter this command on the input and the output interfaces. It will match only on MPLS packets.

Examples

The following example shows that the EXP value 3 in the topmost label is matched:

```
match mpls experimental topmost 3
```

Related Commands

Command	Description
set mpls experimental topmost	Sets the MPLS EXP field value in the topmost MPLS label header at the input and/or output interfaces.

match not

To specify the single match criterion value to use as an unsuccessful match criterion, use the **match not** command in class-map configuration mode. To remove a previously specified source value to not use as a match criterion, use the **no** form of this command.

match not *match-criteria*

no match not *match-criteria*

Syntax Description

match-criteria	(Required) Specifies the match criterion value that is an unsuccessful match criterion. All other values of the specified match criterion will be considered successful match criteria.

Defaults

No default behavior or values

Command Modes

Class-map configuration

Command History

Release	Modification
12.0(5)XE	This command was introduced.
12.0(5)T	This command was integrated into Cisco IOS Release 12.0(5)T.
12.1(1)E	This command was integrated into Cisco IOS Release 12.1(1)E.

Usage Guidelines

The **match not** command is used to specify a QoS policy value that is not used as a match criterion. When the **match not** command is used, all other values of that QoS policy become successful match criteria.

For instance, if the **match not qos-group 4** command is issued in class-map configuration mode, the specified class will accept all QoS group values except 4 as successful match criteria.

Examples

In the following traffic class, all protocols except IP are considered successful match criteria:

```
Router(config)# class-map noip
Router(config-cmap)# match not protocol ip
Router(config-cmap)# exit
```

Related Commands

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

match packet length (class-map)

To specify the Layer 3 packet length in the IP header as a match criterion in a class map, use the **match packet length** command in class-map configuration mode. To remove a previously specified Layer 3 packet length as a match criterion, use the **no** form of this command.

match packet length {**max** *maximum-length-value* [**min** *minimum-length-value*] | **min** *minimum-length-value* [**max** *maximum-length-value*]}

no match packet length {**max** *maximum-length-value* [**min** *minimum-length-value*] | **min** *minimum-length-value* [**max** *maximum-length-value*]}

Syntax Description

max	Maximum. Indicates that a maximum value for the Layer 3 packet length is to be specified.
maximum-length-value	Specifies the maximum length value of the Layer 3 packet length, in bytes. The range is from 1 to 2000.
min	Minimum. Indicates that a minimum value for the Layer 3 packet length is to be specified.
minimum-length-value	Specifies the minimum length value of the Layer 3 packet length, in bytes. The range is from 1 to 2000.

Defaults

If only the minimum value is specified, a packet with a Layer 3 length greater than the minimum is viewed as matching the criterion.

If only the maximum value is specified, a packet with a Layer 3 length less than the maximum is viewed as matching the criterion.

Command Modes

Class-map configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

This command considers only the Layer 3 packet length in the IP header. It does not consider the Layer 2 packet length in the IP header.

When using this command, you must at least specify the maximum or minimum value. However, you do have the option of entering both values.

Examples

In the following example a class map called “class 1” has been created, and the Layer 3 packet length has been specified as a match criterion. In this example, packets with a minimum Layer 3 packet length of 100 and a maximum Layer 3 packet length of 300 are viewed as meeting the match criteria.

```
Router(config)# class map match-all class1
Router(config-cmap)# match packet length min 100 max 300
```

Related Commands

Command	Description
show class-map	Displays all class maps and their matching criteria.
show policy-map interface	Displays the packet statistics of all classes that are configured for all service policies either on the specified interface or subinterface or on a specific PVC on the interface.

match precedence

To identify IP precedence values as match criteria, use the **match precedence** command in class-map configuration mode. To remove IP precedence values from a class map, use the **no** form of this command.

match [**ip**] **precedence** *precedence-value* [*precedence-value precedence-value precedence-value*]

no match [**ip**] **precedence** *precedence value* [*precedence-value precedence-value precedence-value*]

Syntax Description

ip	(Optional) Specifies that the match is for IPv4 packets only. If not used, the match is on both the IPv4 and IPv6 packets.
precedence-value	Specifies the exact value from 0 to 7 used to identify a precedence value.

Defaults

Matching on both IPv4 and IPv6 packets is the default.

Command Modes

Class-map configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

Precedence Value Arguments

Up to four precedence values can be matched in one match statement. For example, if you wanted the precedence values of 0, 1, 2, or 3 (note that only one of the precedence values must be a successful match criterion, not all of the specified precedence values), enter the **match ip precedence 0 1 2 3** command.

The *precedence-value* arguments are used as markings only. In this context, the IP precedence values have no mathematical significance. For instance, the *precedence-value* of 2 is not greater than 1. The value simply indicates that a packet marked with the *precedence-value* of 2 is different from a packet marked with the *precedence-value* of 1. The treatment of these different packets is defined by the user through the setting of QoS policies in policy-map class configuration mode.

Match on Precedence for IPv6 Only

To match on precedence values for IPv6 packets only, the **match protocol ipv6** command must also be used. Without that command, the precedence match defaults to match both IPv4 and IPv6 packets.

Match on Precedence for IPv4 Packets Only

To match on precedence values for IPv4 packets only, use the **ip** keyword. Without the **ip** keyword, the match occurs on both IPv4 and IPv6 packets.

Examples

IPv4-Specific Traffic Match

The following example shows how to configure the service policy called "priority50" and attach service policy "priority50" to an interface, matching for IPv4 traffic only. In a network where both IPv4 and IPv6 are running, you might find it necessary to distinguish between the protocols for matching and traffic segregation. In this example, the class map called "ipprec5" will evaluate all IPv4 packets entering Fast Ethernet interface 1/0/0 for a precedence value of 5. If the incoming IPv4 packet has been marked with the precedence value of 5, the packet will be treated as priority traffic and will be allocated with bandwidth of 50 kbps.

```
Router(config)# class-map ipprec5
Router(config-cmap)# match ip precedence 5
Router(config)# exit
Router(config)# policy-map priority50
Router(config-pmap)# class ipprec5
Router(config-pmap-c)# priority 50
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface fa1/0/0
Router(config-if)# service-policy input priority50
```

IPv6-Specific Traffic Match

The following example shows the same service policy matching on precedence for IPv6 traffic only. Notice that the **match protocol** command with the **ipv6** keyword precedes the **match precedence** command. The **match protocol** command is required to perform matches on IPv6 traffic alone.

```
Router(config)# class-map ipprec5
Router(config-cmap)# match protocol ipv6
Router(config-cmap)# match precedence 5
Router(config)# exit
Router(config)# policy-map priority50
Router(config-pmap)# class ipprec5
Router(config-pmap-c)# priority 50
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface fa1/0/0
Router(config-if)# service-policy input priority50
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class.
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
service-policy	Attaches a policy map to an input interface or VC, or an output interface or VC, to be used as the service policy for that interface or VC.
set ip precedence	Sets the precedence value in the IP header.
show class-map	Displays all class maps and their matching criteria, or a specified class map and its matching criteria.

match protocol

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

match protocol *protocol-name*

no match protocol *protocol-name*

Syntax Description

protocol-name	Name of the protocol used as a matching criterion. Supported protocols include the following: • **aarp**—AppleTalk Address Resolution Protocol • **arp**—IP Address Resolution Protocol (ARP) • **bridge**—bridging • **bstun**—Block Serial Tunneling • **cdp**—Cisco Discovery Protocol • **clns**—ISO Connectionless Network Service • **clns_es**—ISO CLNS End System • **clns_is**—ISO CLNS Intermediate System • **cmns**—ISO Connection-Mode Network Service • **compressedtcp**—compressed TCP • **decnet**—DECnet • **decnet_node**—DECnet Node • **decnet_router-I1**—DECnet Router L1 • **decnet_router-I2**—DECnet Router L2 • **dlsw**—data-link switching • **ip**—IP • **ipv6**—IPv6 • **ipx**—Novell IPX • **llc2**—llc2 • **pad**—packet assembler/disassembler links • **qllc**—Qualified Logical Link Control protocol • **rsrb**—remote source-route bridging • **snapshot**—snapshot routing support • **stun**—serial tunnel

Defaults

No default behavior or values

Command Modes

Class-map configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(5)XE	This command was integrated into Cisco IOS Release 12.0(5)XE.
12.0(7)S	This command was integrated into Cisco IOS Release 12.0(7)S.
12.1(1)E	This command was integrated into Cisco IOS Release 12.1(1)E.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.1(13)E	This command was integrated into Cisco IOS Release 12.1(13)E. This command became available on Catalyst 6000 family switches without FlexWAN modules.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(13)T	This command was modified to remove apollo, vines, and xns from the list of protocols used as matching criteria. These protocols were removed because Apollo Domain, Banyan VINES, and Xerox Network Systems (XNS) were removed in Release 12.2(13)T. In addition, the **ipv6** keyword was added to support protocol matching on IPv6 packets.

Usage Guidelines

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

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

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

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

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

This command can be used to match protocols that are known to the network-based application recognition (NBAR) feature. For a list of protocols currently supported by NBAR, refer to the "Classification" section of the *Cisco IOS Quality of Service Solutions Configuration Guide*, Release 12.2.

Examples

The following example specifies a class map called ipx and configures the Internetwork Packet Exchange (IPX) protocol as a match criterion for it:

```
class-map ipx
  match protocol ipx
```

The following example configures NBAR to match FTP traffic:

```
match protocol ftp
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class.
match access-group	Configures the match criteria for a class map based on the specified ACL.
match input-interface	Configures a class map to use the specified input interface as a match criterion.
match qos-group	Configures a class map to use the specified EXP field value as a match criterion.

match protocol citrix

To configure network-based application recognition (NBAR) to match Citrix traffic, use the **match protocol citrix** command in class-map configuration mode. To disable NBAR from matching Citrix traffic, use the **no** form of this command.

match protocol citrix [**app** *application-name-string*]

no match protocol citrix [**app** *application-name-string*]

Syntax Description

app	(Optional) Specifies matching of an application name string.
application-name-string	(Optional) Specifies string to be used as the subprotocol parameter.

Defaults

No default behavior or values

Command Modes

Class-map configuration

Command History

Release	Modification
12.1(2)E	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.1(13)E	This command was integrated into Cisco IOS Release 12.1(13)E. This command became available on Catalyst 6000 family switches without FlexWAN modules.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.

Usage Guidelines

Entering the **match protocol citrix** command without the **app** keyword establishes all Citrix traffic as successful match criteria.

Examples

The following example configures NBAR to match all Citrix traffic:

```
match protocol citrix
```

The following example configures NBAR to match Citrix traffic with the application name of packet1:

```
match protocol citrix app packet1
```

match protocol http

To configure network-based application recognition (NBAR) to match HTTP traffic by URL, HOST, or Multipurpose Internet Mail Extension (MIME)-type, use the **match protocol http** command in class-map configuration mode. To disable NBAR from matching HTTP traffic by URL, HOST, or MIME-type, use the **no** form of this command.

match protocol http [**url** *url-string* | **host** *hostname-string* | **mime** *MIME-type*]

no match protocol http [**url** *url-string* | **host** *hostname-string* | **mime** *MIME-type*]

Syntax Description

url	(Optional) Specifies matching by a URL.
url-string	(Optional) User-specified URL of HTTP traffic to be matched.
host	(Optional) Specifies matching by a host name.
hostname-string	(Optional) User-specified host name to be matched.
mime	(Optional) Specifies matching by MIME text string.
MIME-type	(Optional) User-specified MIME text string to be matched.

Defaults

No default behavior or values

Command Modes

Class-map configuration

Command History

Release	Modification
12.0(5)XE2	This command was introduced.
12.1(1)E	This command was integrated into Cisco IOS Release 12.1(1)E.
12.1(2)E	The *hostname-string* argument was added.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.1(13)E	This command was integrated into Cisco IOS Release 12.1(13)E. This command became available on Catalyst 6000 family switches without FlexWAN modules.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.

Usage Guidelines

When matching by MIME-type, the MIME-type can contain any user-specified text string. Refer to the the Internet Assigned Numbers Authority (IANA) web page (*www.iana.com*) for a list of the IANA-registered MIME types.

When matching by MIME-type is performed, NBAR matches a packet containing the MIME-type and all subsequent packets until the next HTTP transaction.

When matching by HOST is performed, NBAR performs a regular expression match on the host field contents inside an HTTP GET packet and classifies all packets from that host.

HTTP URL matching supports GET, PUT, HEAD, POST, DELETE, and TRACE. When matching by URL, NBAR recognizes the HTTP packets containing the URL, and then matches all packets that are part of the HTTP request. When specifying a URL for classification, include only the portion of the URL following www.hostname.domain in the match statement. For example, in the URL www.anydomain.com/latest/whatsnew.html include only /latest/whatsnew.html.

To match the www.anydomain.com portion, use the host name matching feature. The URL or host specification strings can take the form of a regular expression with options shown in Table 7.

Table 7 URL or HOST Specification String Options

Options	Description
*	Match any zero or more characters in this position.
?	Match any one character in this position.
|	Match one of a choice of characters.
(|)	Match one of a choice of characters in a range. For example, xyz.(gif | jpg) matches either xyz.gif or xyz.jpg.
[ ]	Match any character in the range specified, or one of the special characters. For example, [0-9] is all of the digits; [*] is the "*" character, and [[] is the "[" character.

Examples

The following example classifies, within the class map called "class1," HTTP packets based on any URL containing the string "whatsnew/latest" followed by zero or more characters:

```
class-map class1
match protocol http url whatsnew/latest*
```

The following example classifies, within the class map called "class2," packets based on any host name containing the string "cisco" followed by zero or more characters:

```
class-map class2
match protocol http host cisco*
```

The following example classifies, within the class map called "class3," packets based on the Joint Photographics Expert Group (JPEG) MIME type:

```
class-map class3
match protocol http mime "*jpeg"
```

match protocol rtp

To configure network-based application recognition (NBAR) to match Real-Time Transfer Protocol (RTP) traffic, use the **match protocol rtp** command in class-map configuration mode. To disable NBAR from matching RTP traffic, use the **no** form of this command.

match protocol rtp [**audio** | **video** | **payload-type** *payload-string*]

no match protocol rtp [**audio** | **video** | **payload-type** *payload-string*]

Syntax Description

audio	(Optional) Specifies matching by audio payload-type values in the range of 0 to 23. These payload-type values are reserved for audio traffic.
video	(Optional) Specifies matching by video payload-type values in the range of 24 to 33. These payload-type values are reserved for video traffic.
payload-type	(Optional) Specifies matching by a specific payload-type value, providing more granularity than is available with the **audio** or **video** keywords.
payload-string	(Optional) User-specified string that contains the specific payload-type values. A *payload-string* argument can contain commas to separate payload-type values and hyphens to indicate a range of payload-type values. A *payload-string* argument can be specified in hexadecimal (prepend 0x to the value) and binary (prepend b to the value) notation in addition to standard number values.

Defaults

No default behavior or values

Command Modes

Class-map configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.1(11b)E	This command was incorporated into the Cisco IOS Release 12.1 E train.
12.1(13)E	This command was integrated into Cisco IOS Release 12.1(13)E. This command became available on Catalyst 6000 family switches without FlexWAN modules.

Usage Guidelines

Entering the **match protocol rtp** command without any other keywords establishes all RTP traffic as successful match criteria.

RTP is a packet format for multimedia data streams. It can be used for media-on-demand as well as interactive services such as Internet telephony. RTP consists of a data and a control part. The control part is called Real-Time Transport Control Protocol (RTCP). It is important to note that the NBAR RTP Payload Classification feature does not identify RTCP packets and that RTCP packets run on odd-numbered ports while RTP packets run on even-numbered ports.

The payload type field of an RTP packet identifies the format of the RTP payload and is represented by a number. NBAR matches RTP traffic on the basis of this field in the RTP packet. A working knowledge of RTP and RTP payload types is helpful if you want to configure NBAR to match RTP traffic. For more information about RTP and RTP payload types, refer to RFC 1889, *RTP: A Transport Protocol for Real-Time Applications.*

Examples

The following example configures NBAR to match all RTP traffic:

```
class-map class1
match protocol rtp
```

The following example configures NBAR to match RTP traffic with the payload-types 0, 1, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, and 64:

```
class-map class2
match protocol rtp payload-type "0, 1, 4-0x10, 10001b-10010b, 64"
```

match qos-group

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

match qos-group *qos-group-value*

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

Syntax Description

qos-group-value	Specifies the exact value from 0 to 99 used to identify a QoS group value.

Defaults

No default behavior or values

Command Modes

Class-map configuration

Command History

Release	Modification
11.1 CC	This command was introduced.
12.05(XE)	This command was incorporated into Cisco IOS Release 12.0(5)XE.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T. This command can be used with the **random-detect discard-class-based** command.

Usage Guidelines

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

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

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

Examples

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

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

```
Router(config)# exit
Router(config)# policy-map priority50
Router(config-pmap)# class qosgroup5
Router(config-pmap-c)# priority 50
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface fa1/0/0
Router(config-if)# service-policy output priority50
```

The following example shows that the packet "qos-group 1" belongs to a particular class:

```
match qos-group 1
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class.
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
service-policy	Attaches a policy map to an input interface or VC, or an output interface or VC, to be used as the service policy for that interface or VC.
set precedence	Specifies an IP precedence value for packets within a traffic class.
set qos-group	Sets a group ID that can be used later to classify packets.

match source-address mac

To use the source MAC address as a match criterion, use the **match source-address mac** command in class-map configuration mode. To remove a previously specified source MAC address as a match criterion in class map configuration mode, use the **no** form of this command.

match source-address mac *address-destination*

no match source-address mac *address-destination*

Syntax Description

address-destination	Specifies the source destination MAC address to be used as a match criterion.

Defaults

No default behavior or values

Command Modes

Class-map configuration

Command History

Release	Modification
12.0(5)XE	This command was introduced.
12.1(1)E	This command was integrated into Cisco IOS Release 12.1(1)E.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.

Usage Guidelines

This command can be used only on an input interface with a MAC address. These interfaces include Fast Ethernet and Ethernet interfaces.

This command cannot be used on output interfaces with no MAC address, such as serial and ATM interfaces.

Examples

The following example uses the mac address mac 0.0.0 as a match criterion:

```
class-map matchsrcmac
match source-address mac 0.0.0
```

Related Commands

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

max-reserved-bandwidth

To change the percent of interface bandwidth allocated for Resource Reservation Protocol (RSVP), class-based weighted fair queueing (CBWFQ), low latency queueing (LLQ), IP RTP Priority, Frame Relay IP RTP Priority, and Frame Relay PVC Interface Priority Queueing (PIPQ), use the **max-reserved bandwidth** command in interface configuration mode. To restore the default value, use the **no** form of this command.

max-reserved-bandwidth *percent*

no max-reserved-bandwidth

Syntax Description

percent	Percent of interface bandwidth allocated for RSVP, CBWFQ, LLQ, IP RTP Priority, Frame Relay IP RTP Priority, and Frame Relay PIPQ.

Defaults

75 percent

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

The sum of all bandwidth allocation on an interface should not exceed 75 percent of the available bandwidth on an interface. The remaining 25 percent of bandwidth is used for overhead, including Layer 2 overhead, control traffic, and best-effort traffic.

If you need to allocate more than 75 percent for RSVP, CBWFQ, LLQ, IP RTP Priority, Frame Relay IP RTP Priority, and Frame Relay PIPQ, you can use the **max-reserved-bandwidth** command. The *percent* argument specifies the maximum percentage of the total interface bandwidth that can be used.

If you do use the **max-reserved-bandwidth** command, make sure that not too much bandwidth is taken away from best-effort and control traffic.

The **max-reserved-bandwidth** command is intended for use on main interfaces only; it has no effect on virtual circuits (VCs) or ATM permanent virtual circuits (PVCs).

Examples

In the following example, the policy map called policy1 is configured for three classes with a total of 8 Mbps configured bandwidth, as shown in the output from the **show policy-map** command:

```
Router# show policy-map policy1

 Policy Map policy1
  Weighted Fair Queueing
    Class class1
      Bandwidth 2500 (kbps) Max Threshold 64 (packets)
    Class class2
      Bandwidth 2500 (kbps) Max Threshold 64 (packets)
```

```
    Class class3
      Bandwidth 3000 (kbps) Max Threshold 64 (packets)
```

When you enter the **service-policy** command in an attempt to attach the policy map on a 10-Mbps Ethernet interface, an error message such as the following is produced:

```
I/f Ethernet1/1 class class3 requested bandwidth 3000 (kbps) Available only 2500 (kbps)
```

The error message is produced because the default maximum configurable bandwidth is 75 percent of the available interface bandwidth, which in this example is 7.5 Mbps. To change the maximum configurable bandwidth to 80 percent, use the **max-reserved-bandwidth** command in interface configuration mode, as follows:

```
max-reserved-bandwidth 80
service output policy1
end
```

To verify that the policy map was attached, enter the **show policy-map interface** command:

```
Router# show policy-map interface e1/1

 Ethernet1/1  output :policy1
  Weighted Fair Queueing
    Class class1
      Output Queue:Conversation 265
        Bandwidth 2500 (kbps) Packets Matched 0 Max Threshold 64 (packets)
        (discards/tail drops) 0/0
    Class class2
      Output Queue:Conversation 266
        Bandwidth 2500 (kbps) Packets Matched 0 Max Threshold 64 (packets)
        (discards/tail drops) 0/0
    Class class3
      Output Queue:Conversation 267
        Bandwidth 3000 (kbps) Packets Matched 0 Max Threshold 64 (packets)
        (discards/tail drops) 0/0
```

Virtual Template Configuration Example

The following example configures a strict priority queue in a virtual template configuration with CBWFQ. The **max-reserved-bandwidth** command changes the maximum bandwidth allocated between CBWFQ and IP RTP Priority from the default (75 percent) to 80 percent.

```
multilink virtual-template 1
interface virtual-template 1
 ip address 172.16.1.1 255.255.255.0
 no ip directed-broadcast
 ip rtp priority 16384 16383 25
 service-policy output policy1
 ppp multilink
 ppp multilink fragment-delay 20
 ppp multilink interleave
 max-reserved-bandwidth 80
 end

interface Serial0/1
 bandwidth 64
 ip address 10.1.1.2 255.255.255.0
 no ip directed-broadcast
 encapsulation ppp
 ppp multilink
 end
```

Note To make the virtual access interface function properly, do not configure the **bandwidth** command on the virtual template. Configure it on the actual interface, as shown in the example.

Related Commands

Command	Description
bandwidth (policy-map class)	Specifies or modifies the bandwidth allocated for a class belonging to a policy map.
ip rtp priority	Reserves a strict priority queue for a set of RTP packet flows belonging to a range of UDP destination ports.
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 comprising the 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.

mpls experimental

To configure Multiprotocol Label Switching (MPLS) experimental (EXP) levels for a virtual circuit (VC) class that can be assigned to a VC bundle and thus applied to all VC members of that bundle, use the **mpls experimental** command in vc-class configuration mode. To remove the MPLS EXP levels from the VC class, use the **no** form of this command.

To configure the MPLS EXP levels for a VC member of a bundle, use the **mpls experimental** command in bundle-vc configuration mode. To remove the MPLS EXP levels from the VC, use the **no** form of this command.

mpls experimental [**other** | *range*]

no mpls experimental

Syntax Description

other	(Optional) Any MPLS EXP levels that are not explicitly configured.
range	(Optional) A single MPLS EXP level specified as a number from 0 to 7, or a range of levels, specified as a hyphenated range.

Defaults

Defaults to **other**, that is, any MPLS EXP levels that are not explicitly configured.

Command Modes

VC-class configuration (for a VC class)

Bundle-vc configuration (for ATM VC bundle members)

Command History

Release	Modification
12.2(8)T	This command was introduced.

Usage Guidelines

Assignment of MPLS EXP levels to VC bundle members allows you to create differentiated service because you can distribute the MPLS EXP levels over the different VC bundle members. You can map a single level or a range of levels to each discrete VC in the bundle, thereby enabling VCs in the bundle to carry packets marked with different levels. Alternatively, you can configure a VC with the **mpls experimental other** command to indicate that it can carry traffic marked with levels not specifically configured for it. Only one VC in the bundle can be configured with the **mpls experimental other** command to carry all levels not specified. This VC is considered the default one.

To use this command in vc-class configuration mode, enter the **vc-class atm** global configuration command before you enter this 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 to configure an individual bundle member in bundle-vc configuration mode, first enter the **bundle** command to enact bundle configuration mode for the bundle to which you want to add or modify the VC member to be configured. Then, use the **pvc-bundle** command to specify the VC to be created or modified and enter bundle-vc configuration mode.

VCs in a VC bundle are subject to the following configuration inheritance guidelines (listed in order of next highest MPLS EXP level):

- VC configuration in bundle-vc mode
- Bundle configuration in bundle mode (with the effect of assigned vc-class configuration)
- Subinterface configuration in subinterface mode

Note If you are using an ATM interface, you must configure all MPLS EXP levels (ranging from 0 to 7) for the bundle. To do this, Cisco recommends configuring one member of the bundle with the **mpls experimental other** command. The **other** keyword defaults to any MPLS EXP levels in the range from 0 to 7 that are not explicitly configured.

Examples

The following example configures a class called "control-class" that includes the **mpls experimental** command that, when applied to a bundle, configures all VC members of that bundle to carry MPLS EXP level 7 traffic. Note, however, that VC members of that bundle can be individually configured with the **mpls experimental** command at the bundle-vc level, which would supervene.

```
vc-class atm control-class
 mpls experimental 7
```

The following example configures permanent virtual circuit (PVC) 401 (with the name "control-class") to carry traffic with MPLS EXP levels in the range of 4 to 2, overriding the level mapping set for the VC through vc-class configuration:

```
pvc-bundle control-class 401
 mpls experimental 4-2
```

Related Commands

Command	Description
bump	Configures the bumping rules for a VC class that can be assigned to a VC bundle.
bundle	Creates a bundle or modifies an existing bundle to enter bundle configuration mode.
class-vc	Assigns a VC class to an ATM PVC, SVC, or VC bundle member.
protect	Configures a VC or PVC class with protected group or protected VC/PVC status for application to a VC/PVC bundle member.
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 PCR for an ATM PVC, PVC range, SVC, VC class, or VC bundle member.
vbr-nrt	Configures the VBR-NRT QoS and specifies output peak cell rate, output sustainable cell rate, and output maximum burst cell size for an ATM PVC, SVC, VC class, or VC bundle member.
vc-class atm	Configures a VC class for an ATM VC or interface.

oam-bundle

To enable end-to-end F5 Operation, Administration, and Maintenance (OAM) loopback cell generation and OAM management for all virtual circuit (VC) members of a bundle or a VC class that can be applied to a VC bundle, use the **oam-bundle** command in switched virtual circuit (SVC)-bundle configuration mode or VC-class configuration mode. To remove OAM management from the bundle or class configuration, use the **no** form of this command.

To enable end-to-end F5 OAM loopback cell generation and OAM management for all VC members of a bundle, use the **oam-bundle** command in bundle configuration mode. To remove OAM management from the bundle, use the **no** form of this command.

oam-bundle [**manage**] [*frequency*]

no oam-bundle [**manage**] [*frequency*]

Syntax Description

manage	(Optional) Enables OAM management. If this keyword is omitted, loopback cells are sent, but the bundle is not managed.
frequency	(Optional) Number of seconds between transmitted OAM loopback cells. Values range from 0 to 600 seconds. The default value for the *frequency* argument is 10 seconds.

Defaults

End-to-end F5 OAM loopback cell generation and OAM management are disabled, but if OAM cells are received, they are looped back.

Command Modes

SVC-bundle configuration (for an SVC bundle)

VC-class configuration (for a VC class)

Bundle configuration (for an ATM VC bundle)

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.2(4)T	This command was made available in SVC-bundle configuration mode.

Usage Guidelines

This command defines whether a VC bundle is OAM managed. If this command is configured for a bundle, every VC member of the bundle is OAM managed. If OAM management is enabled, further control of OAM management is configured using the **oam retry** 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. In this case, the attributes are ignored by the VC.

To use this command in VC-class configuration mode, first enter the **vc-class atm** global configuration command.

To use this command in bundle configuration mode, enter the **bundle** subinterface configuration command to create the bundle or to specify an existing bundle before you enter this command.

VCs in a VC bundle are subject to the following configuration inheritance rules (listed in order of next-highest precedence):

- VC configuration in bundle-VC mode
- Bundle configuration in bundle mode (with effect of assigned VC-class configuration)

Examples

The following example enables OAM management for a bundle called “chicago”:

```
bundle chicago
 oam-bundle manage
```

Related Commands

Command	Description
broadcast	Configures broadcast packet duplication and transmission for an ATM VC class, PVC, SVC, or VC bundle.
class-bundle	Configures a VC bundle with the bundle-level commands contained in the specified VC class.
encapsulation	Sets the encapsulation method used by the interface.
inarp	Configures the Inverse ARP time period for an ATM PVC, VC class, or VC bundle.
oam retry	Configures parameters related to OAM management for an ATM PVC, SVC, VC class, or VC bundle.
protocol (ATM)	Configures a static map for an ATM PVC, SVC, VC class, or VC bundle. Enables Inverse ARP or Inverse ARP broadcasts on an ATM PVC by configuring Inverse ARP either directly on the PVC, on the VC bundle, or in a VC class (applies to IP and IPX protocols only).

police

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

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

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

Syntax Description

bps	Average rate in bits per second. Valid values are 8,000 to 200,000,000.
burst-normal	(Optional) Normal burst size in bytes. Valid values are 1,000 to 51,200,000. The default normal burst size is 1500 bytes.
burst-max	(Optional) Excess burst size in bytes. Valid values are 1,000 to 51,200,000.
conform-action *action*	Action to take on packets that conform to the rate limit.
exceed-action *action*	Action to take on packets that exceed the rate limit.
violate-action *action*	(Optional) Action to take on packets that violate the normal and maximum burst sizes.
action	Action to take on packets. Specify one of the following keywords: • **drop**—Drops the packet. • **set-clp-transmit** *value*—Sets the ATM Cell Loss Priority (CLP) bit from 0 to 1 on the ATM cell and transmits the packet with the ATM CLP bit set to 1. • **set-discard-class-transmit**—Sets the discard class attribute of a packet and transmits the packet with the new discard class setting. • **set-dscp-transmit** *value*—Sets the IP differentiated services code point (DSCP) value and transmits the packet with the new IP DSCP value setting. • **set-frde-transmit** *value*—Sets the Frame Relay Discard Eligibility (DE) bit from 0 to 1 on the frame relay frame and transmits the packet with the DE bit set to 1. • **set-mpls-experimental-imposition-transmit** *value*—Sets the Multiprotocol Label Switching (MPLS) experimental (EXP) bits (0 to 7) in the imposed label headers and transmits the packet with the new MPLS EXP bit value setting. • **set-mpls-experimental-topmost-transmit** *value*—Sets the MPLS EXP field value in the topmost MPLS label header at the input and/or output interfaces. • **set-prec-transmit** *value*—Sets the IP precedence and transmits the packet with the new IP precedence value setting. • **set-qos-transmit** *value*—Sets the qos-group value and transmits the packet with the new qos-group value setting. • **transmit**—Transmits the packet. The packet is not altered.

Defaults

Disabled

Command Modes

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

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

Command History

Release	Modification
11.1 CC	The **rate-limit** command was introduced.
12.0(5)XE	This **police** command, which was closely related to the **rate-limit** command, was introduced.
12.1(1)E	This command was introduced in Cisco IOS Release 12.1 E.
12.1(5)T	This command was introduced in Cisco IOS Release 12.1 T. The **violate-action** option became available.
12.2(2)T	The **set-clp-transmit** option for the *action* argument was added to the **police** command. The **set-frde-transmit** option for the *action* argument was added to the **police** command. The **set-mpls-exp-transmit** option for the *action* argument was added to the **police** command.
12.2(8)T	The command was modified for the Policer Enhancement — Multiple Actions feature. This command can now accommodate multiple actions for packets marked as conforming to, exceeding, or violating a specific rate.
12.2(13)T	In the *action* field, the **set-mpls-experimental-transmit** option was renamed to **set-mpls-experimental-imposition-transmit**.

Usage Guidelines

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

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

Specifying Multiple Actions

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

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

Using the Police Command with the Traffic Policing Feature

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

The token bucket algorithm for the **police** command that was introduced in Cisco IOS Release 12.0(5)XE is different from the token bucket algorithm for the **police** command introduced in Cisco IOS Release 12.1(5)T. For information on the token bucket algorithm introduced in

Release 12.0(5)XE, refer to the *Traffic Policing* document for Release 12.0(5)XE. This document is available on the *New Features for 12.0(5)XE* feature documentation index (under Modular QoS CLI-related feature modules) at www.cisco.com.

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

Token Bucket Algorithm with One Token Bucket

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

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

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

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

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

Token Bucket Algorithm with Two Token Buckets

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

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

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

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

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

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

  The token arrival rate is calculated as follows:

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

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

Examples

Token Bucket Algorithm with One Token Bucket Example

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

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

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

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

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

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

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

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

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

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

Token Bucket Algorithm with Two Token Buckets Example

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Conforming to the MPLS EXP Value Example

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

```
policy-map input-IP-dscp
  class dscp24
   police 8000 1500 1000
     conform-action set-mpls-experimental-imposition-transmit 5
     exceed-action set-mpls-experimental-imposition-transmit 3
     violate-action drop
```

Related Commands

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

police (percent)

To configure traffic policing on the basis of a percentage of bandwidth available on an interface, use the **police** (percent) command in policy-map class configuration mode. To remove traffic policing from the configuration, use the **no** form of this command.

police cir percent *percent* [**bc** *conform-burst-in-msec*] [**pir percent** *percent*]
[**be** *peak-burst-in-msec*]

no police cir percent *percent* [**bc** *conform-burst-in-msec*] [**pir percent** *percent*]
[**be** *peak-burst-in-msec*]

Syntax Description

cir	Committed information rate (CIR). Indicates that the CIR will be used for policing traffic.
percent	Specifies that percent of bandwidth will be used for calculating the CIR.
percent	Specifies the bandwidth percentage. Valid range is a number from 1 to 100.
bc	(Optional) Conform burst (bc) size used by the first token bucket for policing traffic.
conform-burst-in-msec	(Optional) Specifies the bc value in milliseconds (ms). Valid range is a number from 1 to 2000.
pir	(Optional) Peak information rate (PIR). Indicates that the PIR will be used for policing traffic.
percent	(Optional) Specifies that a percentage of bandwidth will be used for calculating the PIR.
percent	(Optional) Specifies the bandwidth percentage. Valid range is a number from 1 to 100.
be	(Optional) Peak burst (be) size used by the second token bucket for policing traffic.
peak-burst-in-msec	(Optional) Specifies the be size in ms. Valid range is a number from 1 to 2000.

Defaults

Disabled

Command Modes

Policy-map class configuration

Command History

Release	Modification
11.1 CC	The **rate-limit** command was introduced.
12.0(5)XE	This **police** command, which was closely related to the **rate-limit** command, was introduced.
12.1(1)E	This command was integrated into Cisco IOS Release 12.2(1)E.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T. This command was modified for the Percentage-Based Policing and Shaping feature.

Usage Guidelines

This command calculates the CIR and PIR based on a percentage of the maximum amount of bandwidth available on the interface. When a policy map is attached to the interface, the equivalent CIR and PIR values in bits per second (bps) are calculated based on the interface bandwidth and the percent value entered with this command. The **show policy-map interface** command can then be used to verify the bps rate calculated.

The calculated CIR and PIR bps rates must be in the range of 8000 and 2000000000 bps. If the rates are outside this range, the associated policy map cannot be attached to the interface. If the interface bandwidth changes (for example, more is added), the bps values of the CIR and the PIR are recalculated based on the revised amount of bandwidth. If the CIR and PIR percentages are changed after the policy map is attached to the interface, the bps values of the CIR and PIR are recalculated.

This command also allows you to specify the values for the conform burst size and the peak burst size in milliseconds. If you want bandwidth to be calculated as a percentage, the conform burst size and the peak burst size must be specified in milliseconds (ms).

Policy maps can be configured in two-level (nested) hierarchies; a primary (or “parent”) level and a secondary (or “child”) level. The **police** (percent) command can be configured for use in either a parent or child policy map.

The **police** (percent) command uses the maximum rate of bandwidth available as the reference point for calculating the bandwidth percentage. When the **police** (percent) command is configured in a child policy map, the **police** (percent) command uses the bandwidth amount specified in the next higher-level policy (in this case, the parent policy map). If the parent policy map does not specify the maximum bandwidth rate available, the **police** (percent) command uses the maximum bandwidth rate available on the next higher level (in this case, the physical interface, the highest point in the hierarchy) as the reference point. The **police** (percent) command always looks to the next higher level for the bandwidth reference point. The following sample configuration illustrates this point:

```
Policymap parent_policy
 class parent
  shape average 512000
  service-policy child_policy

Policymap child_policy
 class normal_type
  police cir percent 30
```

In this sample configuration, there are two hierarchical policies; one called “parent_policy” and one called “child_policy.” In the policy map called “child_policy,” the **police** (percent) command has been configured in the class called “normal_type.” In this class, the percentage specified by for the **police** (percent) command is 30 percent. The command will use 512 kbps, the peak rate, as the bandwidth reference point for “class parent” in “parent policy.” The **police** (percent) command will use 512 kbps as the basis for calculating the CIR rate (512 kbps * 30 percent).

```
interface serial 4/0
 service-policy output parent_policy

Policymap parent_policy
 class parent
  bandwidth 512
  service-policy child_policy
```

In the above example, there is one policy map called "parent_policy." In this policy map, a peak rate has not been specified. The **bandwidth** (policy-map class) command has been used, but this command does not represent the maximum rate of bandwidth available. Therefore, the **police** (percent) command will look to the next higher level (in this case Serial interface 4/0) to get the bandwidth reference point. Assuming the bandwidth of the Series interface s4/0 is 1.5 Mbps, the **police** (percent) command will use 1.5 Mbps as the basis for calculating the CIR rate (1500000 * 30 percent).

How Bandwidth Is Calculated

The **police** (percent) command is often used in conjunction with the **bandwidth** (policy-map class) and **priority** commands. The **bandwidth** (policy-map class) and **priority** commands can be used to calculate the total amount of bandwidth available on an entity (for example, a physical interface). When the **bandwidth** (policy-map class) and **priority** commands calculate the total amount of bandwidth available on an entity, the following guidelines are invoked:

- If the entity is a physical interface, the total bandwidth is the bandwidth on the physical interface.
- If the entity is a shaped ATM permanent virtual circuit (PVC), the total bandwidth is calculated as follows:
  - For a variable bit rate (VBR) virtual circuit (VC), the sustained cell rate (SCR) is used in the calculation.
  - For an available bit rate (ABR) VC, the minimum cell rate (MCR) is used in the calculation.

For more information on bandwidth allocation, refer to the chapter "Congestion Management Overview" in the *Cisco IOS Quality of Service Solutions Configuration Guide*, Release 12.2.

Examples

The following example configures traffic policing using a CIR and a PIR based on a percentage of bandwidth. In this example, a CIR of 20 percent and a PIR of 40 percent have been specified. Additionally, an optional bc value and be value (300 ms and 400 ms, respectively) have been specified.

```
Router(config)# policy-map policy1
Router(config-pmap)# class-map class1
Router(config-pmap-c)# police cir percent 20 bc 300 ms pir percent 40 be 400 ms
Router(config-pmap-c)# service-policy child-policy1
Router(config-pmap-c)# exit
Router(config-pmap-c)# interface serial 3/1
Router(config-if)# service-policy output policy1
```

Related Commands

Command	Description
bandwidth (policy-map class)	Specifies or modifies the bandwidth allocated for a class belonging to a policy map.
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.
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.
shape (percent)	Specifies average or peak rate traffic shaping based on a percentage of bandwidth available on an interface.
show policy-map	Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps.
show policy-map interface	Displays the packet statistics of all classes that are configured for all service policies either on the specified interface or subinterface or on a specific PVC on the interface.

police (two rates)

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

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

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

Syntax Description

cir	Committed information rate (CIR) at which the first token bucket is updated.
cir	Specifies the CIR value in bits per second. The value is a number from 8,000 to 200,000,000.
bc	(Optional) Conform burst (bc) size used by the first token bucket for policing.
conform-burst	(Optional) Specifies the bc value in bytes. The value is a number from 1,000 to 51,200,000.
pir	Peak information rate (PIR) at which the second token bucket is updated.
pir	Specifies the PIR value in bits per second. The value is a number from 8,000 to 200,000,000.
be	(Optional) Peak burst (be) size used by the second taken bucket for policing.
peak-burst	(Optional) Specifies the peak burst (be) size in bytes. The size varies according to the interface and platform in use.
conform-action	(Optional) Action to take on packets that conform to the CIR and PIR.
exceed-action	(Optional) Action to take on packets that conform to the PIR but not the CIR.
violate-action	(Optional) Action to take on packets exceed the PIR.
action	(Optional) Action to take on packets. Specify one of the following keywords: • **drop**—Drops the packet. • **set-clp-transmit**—Sets the ATM Cell Loss Priority (CLP) bit from 0 to 1 on the ATM cell and sends the packet with the ATM CLP bit set to 1. • **set-dscp-transmit** *new-dscp*—Sets the IP differentiated services code point (DSCP) value and sends the packet with the new IP DSCP value setting. • **set-frde-transmit**—Sets the Frame Relay discard eligible (DE) bit from 0 to 1 on the Frame Relay frame and sends the packet with the DE bit set to 1. • **set-mpls-exp-transmit**—Sets the Multiprotocol Label Switching (MPLS) experimental bits from 0 to 7 and sends the packet with the new MPLS experimental bit value setting. • **set-prec-transmit** *new-prec*—Sets the IP precedence and sends the packet with the new IP precedence value setting. • **set-qos-transmit** *new-qos*—Sets the quality of service (QoS) group value and sends the packet with the new QoS group value setting. • **transmit**—Sends the packet with no alteration.

Defaults

Disabled

Command Modes

Policy-map configuration

Command History

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

Usage Guidelines

Two-rate traffic policing uses two token buckets—Tc and Tp—for policing traffic at two independent rates. Note the following points about the two token buckets:

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

Updating Token Buckets

The following scenario illustrates how the token buckets are updated:

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

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

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

Marking Traffic

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

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

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

Tp(t) = Tp(t) – B

Tc(t) = Tc(t) – B

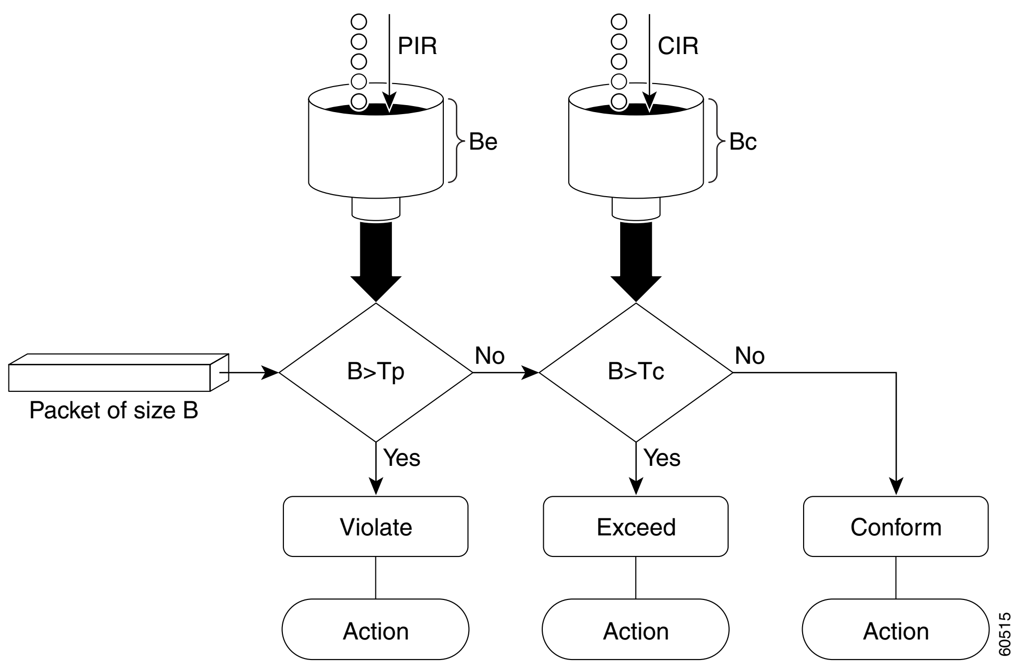
For example, if the CIR is 100 kbps, the PIR is 200 kbps, and a data stream with a rate of 250 kbps arrives at the two-rate policer, the packet would be marked as follows:

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

Marking Packets and Assigning Actions Flowchart

The flowchart in Figure 1 illustrates how the two-rate policer marks packets and assigns a corresponding action (that is, violate, exceed, or conform) to the packet.

Figure 4 Marking Packets and Assigning Actions with the Two-Rate Policer



Examples

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

```
Router(config)# class-map police
Router(config-cmap)# match access-group 101
Router(config-cmap)# policy-map policy1
Router(config-pmap)# class police
Router(config-pmap-c)# police cir 500000 bc 10000 pir 1000000 be 10000 conform-action
transmit exceed-action set-prec-transmit 2 violate-action drop
Router(config-pmap-c)# interface s3/0
Router(config-if)# service-policy output policy1
Router(config-if)# end
Router# show policy-map policy1

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

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

In the following example, 1.25 Mbps of traffic is sent ("offered") to a policer class:

```
Router# show policy-map interface s3/0

 Serial3/0

  Service-policy output: policy1

   Class-map: police (match all)
    148803 packets, 36605538 bytes
    30 second offered rate 1249000 bps, drop rate 249000 bps
    Match: access-group 101
    police:
     cir 500000 bps, conform-burst 10000, pir 1000000, peak-burst 100000
     conformed 59538 packets, 14646348 bytes; action: transmit
     exceeded 59538 packets, 14646348 bytes; action: set-prec-transmit 2
     violated 29731 packets, 7313826 bytes; action: drop
     conformed 499000 bps, exceed 500000 bps violate 249000 bps

   Class-map: class-default (match-any)
    19 packets, 1990 bytes
    30 seconds offered rate 0 bps, drop rate 0 bps
    Match: any
```

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

Related Commands

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

policy-map

To 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 command. To delete a policy map, use the **no** form of this command.

policy-map *policy-map-name*

no policy-map *policy-map-name*

Syntax Description

policy-map-name	Name of the policy map. The name can be a maximum of 40 alphanumeric characters.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

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

You can configure class policies in a policy map only if the classes have match criteria defined for them. You use the **class-map** and **match** commands to configure the match criteria for a class. Because you can configure a maximum of 64 class maps, no policy map can contain more than 64 class policies.

A single policy map can be attached to multiple interfaces concurrently. 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 comprising the policy map. In this case, if the policy map is already attached to other interfaces, it is removed from them.

Whenever you modify class policy in an attached policy map, CBWFQ is notified and the new classes are installed as part of the policy map in the CBWFQ system.

Examples

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

```
! The following commands create class-map class1 and defines 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 creates a policy map called policy9 and configures three class policies to belong to that map. Of these classes, two specify policy for classes with class maps that specify match criteria based on either a numbered ACL or an interface name, and one specifies policy for the default class called **class-default** to which packets that do not satisfy 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 20Related Commands
```

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 the default class (commonly known as the class-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.
queue-limit	Specifies or modifies the maximum number of packets the queue can hold for a class policy configured in a policy map.
random-detect (interface)	Enables WRED or DWRED.
random-detect exponential-weighting-constant	Configures the WRED and DWRED exponential weight factor for the average queue size calculation.
random-detect precedence	Configures WRED and DWRED parameters for a particular IP Precedence.
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.

precedence

To configure precedence levels for a virtual circuit (VC) class that can be assigned to a VC bundle and thus applied to all VC members of that bundle, use the **precedence** command in vc-class configuration mode. To remove the precedence levels from the VC class, use the **no** form of this command.

To configure the precedence levels for a VC or permanent virtual circuit (PVC) member of a bundle, use the **precedence** command in bundle-vc configuration mode for ATM VC bundle members, or in switched virtual circuit (SVC)-bundle-member configuration mode for an ATM SVC. To remove the precedence levels from the VC or PVC, use the **no** form of this command.

precedence [**other** | *range*]

no precedence

Syntax Description

other	(Optional) Any precedence levels in the range from 0 to 7 that are not explicitly configured.
range	(Optional) A single precedence level specified either as a number from 0 to 7 or a range of precedence levels, specified as a hyphenated range.

Defaults

Defaults to **other**—that is, any precedence levels in the range from 0 to 7 that are not explicitly configured.

Command Modes

VC-class configuration (for a VC class)

Bundle-vc configuration (for ATM VC bundle members)

SVC-bundle-member configuration (for an ATM SVC)

Command History

Release	Modification
11.1(22)CC	This command was introduced.
12.0(3)T	This command was integrated into Cisco IOS Release 12.0(3)T. This command was extended to configure precedence levels for a VC member of a bundle.
12.2(4)T	This command was made available in SVC-bundle-member configuration mode.
12.0(23)S	This command was made available in vc-class and bundle-vc configuration modes on the 8-port OC-3 STM-1 ATM line card for Cisco 12000 series Internet routers.

Usage Guidelines

Assignment of precedence levels to VC or PVC bundle members allows you to create differentiated service because you can distribute the IP precedence levels over the various VC/PVC bundle members. You can map a single precedence level or a range of levels to each discrete VC/PVC in the bundle, thereby enabling VCs/PVCs in the bundle to carry packets marked with different precedence levels. Alternatively, you can use the **precedence other** command to indicate that a VC/PVC can carry traffic marked with precedence levels not specifically configured for other VCs/PVCs. Only one VC/PVC in the bundle can be configured using the **precedence other** command. This VC/PVC is considered the default one.

To use this command in vc-class configuration mode, first enter the **vc-class atm** command in global configuration mode. The **precedence** 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 the **precedence** command to configure an individual bundle member in bundle-VC configuration mode, first enter the **bundle** command to enact bundle configuration mode for the bundle to which you want to add or modify the VC member to be configured. Then use the **pvc-bundle** command to specify the VC to be created or modified and enter bundle-VC configuration mode.

VCs in a VC bundle are subject to the following configuration inheritance guidelines (listed in order of next-highest precedence):

- VC configuration in bundle-vc mode
- Bundle configuration in bundle mode (with effect of assigned vc-class configuration)
- Subinterface configuration in subinterface mode

Examples

The following example configures a class called "control-class" that includes a **precedence** command that, when applied to a bundle, configures all VC members of that bundle to carry IP precedence level 7 traffic. Note, however, that VC members of that bundle can be individually configured with the **precedence** command at the bundle-vc level, which would supervene.

```
vc-class atm control-class
 precedence 7
```

The following example configures PVC 401 (with the name of "control-class") to carry traffic with IP precedence levels in the range of 4–2, overriding the precedence level mapping set for the VC through vc-class configuration:

```
pvc-bundle control-class 401
 precedence 4-2
```

Related Commands

Command	Description
bump	Configures the bumping rules for a VC class that can be assigned to a VC bundle.
bundle	Creates a bundle or modifies an existing bundle to enter bundle configuration mode.
class-vc	Assigns a VC class to an ATM PVC, SVC, or VC bundle member.
dscp (frame-relay vc-bundle-member)	Specifies the DSCP value or values for a specific Frame Relay PVC bundle member.
match precedence	Identifies IP precedence values as match criteria.
mpls experimental	Configures the MPLS experimental bit values for a VC class that can be mapped to a VC bundle and thus applied to all VC members of that bundle.
protect	Configures a VC class with protected group or protected VC status for application to a VC bundle member.
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.
pvc	Creates or assigns a name to an ATM PVC, specifies the encapsulation type on an ATM PVC, and enters interface-ATM-VC configuration mode.
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.
vbr-nrt	Configures the VBR-NRT QoS and specifies output peak cell rate, output sustainable cell rate, and output maximum burst cell size for an ATM PVC, SVC, VC class, or VC bundle member.
vc-class atm	Configures a VC class for an ATM VC or interface.

precedence (WRED group)

To configure a Weighted Random Early Detection (WRED) or VIP-distributed WRED (DWRED) group for a particular IP Precedence, use the **precedence** command in random-detect-group configuration mode. To return the values for each IP Precedence for the group to the default values, use the **no** form of this command.

precedence *precedence min-threshold max-threshold mark-probability-denominator*

no precedence *precedence min-threshold max-threshold mark-probability-denominator*

Syntax Description

precedence	IP Precedence number. Values range from 0 to 7.
min-threshold	Minimum threshold in number of packets. Value range from 1 to 4096. When the average queue length reaches this number, WRED or DWRED begins to drop packets with the specified IP Precedence.
max-threshold	Maximum threshold in number of packets. The value range is *min-threshold* to 4096. When the average queue length exceeds this number, WRED or DWRED drops all packets with the specified IP Precedence.
mark-probability-denominator	Denominator for the fraction of packets dropped when the average queue depth is *max-threshold*. For example, if the denominator is 512, 1 out of every 512 packets is dropped when the average queue is at the *max-threshold*. The value is 1 to 65536. The default is 10; 1 out of every 10 packets is dropped at the *max-threshold*.

Defaults

For all IP Precedences, the *mark-probability-denominator* argument is 10, and the *max-threshold* argument is based on the output buffering capacity and the transmission speed for the interface.

The default *min-threshold* argument depends on the IP Precedence. The *min-threshold* argument for IP Precedence 0 corresponds to half of the *max-threshold* argument. The values for the remaining IP Precedences fall between half the *max-threshold* argument and the *max-threshold* argument at evenly spaced intervals. See Table 8 in the "Usage Guidelines" section of this command for a list of the default minimum value for each IP Precedence.

Command Modes

Random-detect-group configuration

Command History

Release	Modification
11.1(22)CC	This command was introduced.

Usage Guidelines

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

If used, this command is issued after the **random-detect-group** command.

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

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

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

Table 8 lists the default minimum value for each IP Precedence.

Table 8 Default WRED Minimum Threshold Values

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

Examples

The following example specifies parameters for the WRED parameter group called sanjose for the different IP Precedences:

```
random-detect-group sanjose
  precedence 0 32 256 100
  precedence 1 64 256 100
  precedence 2 96 256 100
  precedence 3 128 256 100
  precedence 4 160 256 100
  precedence 5 192 256 100
  precedence 6 224 256 100
  precedence 7 256 256 100
```

Related Commands

Command	Description
exponential-weighting-constant	Configures the exponential weight factor for the average queue size calculation for a WRED parameter group.
random-detect (per VC)	Enables per-VC WRED or per-VC DWRED.
random-detect-group	Defines the WRED or DWRED parameter group.
random-detect precedence	Configures WRED and DWRED parameters for a particular IP Precedence.
show queueing	Lists all or selected configured queueing strategies.
show queueing interface	Displays the queueing statistics of an interface or VC.

priority

To give priority to a class of traffic belonging to a policy map, use the **priority** command in policy-map class configuration mode. To remove a previously specified priority for a class, use the **no** form of this command.

priority {*bandwidth-kbps* | **percent** *percentage*} [*burst*]

no priority {*bandwidth-kbps* | **percent** *percentage*} [*burst*]

Syntax Description

bandwidth-kbps	Guaranteed allowed bandwidth, in kbps, for the priority traffic. The amount of guaranteed bandwidth varies according to the interface and platform in use. Beyond the guaranteed bandwidth, the priority traffic will be dropped in the event of congestion to ensure that the nonpriority traffic is not starved.
percent	Specifies that the amount of guaranteed bandwidth will be specified by the percent of available bandwidth.
percentage	Used in conjunction with the **percent** keyword, specifies the percentage of the total available bandwidth to be set aside for the priority class. The percentage can be a number from 1 to 100.
burst	(Optional) Specifies the burst size in bytes. The burst size configures the network to accommodate temporary bursts of traffic. The default burst value, which is computed as 200 milliseconds of traffic at the configured bandwidth rate, is used when the burst argument is not specified. The range of the burst is from 32 to 2,000,000 bytes.

Defaults

No default behavior or values

Command Modes

Policy-map class configuration

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.0(5)XE5	This command was introduced for the Versatile Interface Processor (VIP) as part of the Distributed Low Latency Queueing (Low Latency Queueing for the VIP) feature.
12.0(9)S	This command was introduced for the VIP as part of the Distributed Low Latency Queueing (Low Latency Queueing for the VIP) feature.
12.1(2)E	The *burst* argument was added.
12.1(3)T	The *burst* argument was added.
12.1(5)T	This command was introduced for the VIP as part of the Distributed Low Latency Queueing (Low Latency Queueing for the VIP) feature.
12.2(2)T	The **percent** keyword and the *percentage* argument were added.

Usage Guidelines

This command configures low latency queueing (LLQ), providing strict priority queueing (PQ) for class-based weighted fair queueing (CBWFQ). Strict PQ allows delay-sensitive data such as voice to be dequeued and sent before packets in other queues are dequeued.

The **priority** command allows you to set up classes based on a variety of criteria (not just User Datagram Ports (UDP) ports) and assign priority to them, and is available for use on serial interfaces and ATM permanent virtual circuits (PVCs). A similar command, the **ip rtp priority** command, allows you to stipulate priority flows based only on UDP port numbers and is not available for ATM PVCs.

When the device is not congested, the priority class traffic is allowed to exceed its allocated bandwidth. When the device is congested, the priority class traffic above the allocated bandwidth is discarded.

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

Within a policy map, you can give one or more classes priority status. When multiple classes within a single policy map are configured as priority classes, all traffic from these classes is queued to the same, single, priority queue.

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

For more information on bandwidth allocation, refer to the chapter "Congestion Management Overview" in the *Cisco IOS Quality of Service Solutions Configuration Guide,* Release 12.2.

Examples

The following example configures PQ with a guaranteed bandwidth of 50 kbps and a one-time allowable burst size of 60 bytes for the policy map called policy1:

```
Router(config)# policy-map policy1
Router(config-pmap)# class voice
Router(config-pmap-c)# priority 50 60
```

In the following example, 10 percent of the available bandwidth is reserved for the class called voice on interfaces to which the policy map called policy1 has been attached:

```
Router(config)# policy-map policy1
Router(config-pmap)# class voice
Router(config-pmap-c)# priority percent 10
```

Related Commands

Command	Description
bandwidth	Specifies or modifies the bandwidth allocated for a class belonging to a policy map.
ip rtp priority	Reserves a strict priority queue for a set of RTP packet flows belonging to a range of UDP destination ports.
ip rtp reserve	Reserves a special queue for a set of RTP packet flows belonging to a range of UDP destination ports.
max-reserved-bandwidth	Changes the percent of interface bandwidth allocated for CBWFQ, LLQ, and IP RTP Priority.
show interfaces fair-queue	Displays information and statistics about WFQ for a VIP-based interface.
show policy-map	Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps.
show policy-map interface	Displays the packet statistics of all classes that are configured for all service policies either on the specified interface or subinterface or on a specific PVC on the interface.
show queue	Displays the contents of packets inside a queue for a particular interface or VC.

priority-group

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

priority-group *list-number*

no priority-group *list-number*

Syntax Description

list-number	Priority list number assigned to the interface. Any number from 1 to 16.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

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

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

Examples

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

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

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

```
stun peer-name 131.108.254.6
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 131.108.254.8 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.
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 default

To assign a priority queue for those packets that do not match any other rule in the priority list, use the **priority-list default** 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.

Defaults

This command is not enabled by default.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

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

Examples

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

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

Related Commands

Command	Description
priority-group	Assigns the specified priority list to an interface.
priority-list interface	Establishes queueing priorities on packets entering from a given interface.
priority-list protocol	Establishes queueing priorities based on the protocol type.
priority-list queue-limit	Specifies the maximum number of packets that can be waiting in each of the priority queues.
show queue	Displays the contents of packets inside a queue for a particular interface or VC.
show queueing	Lists all or selected configured queueing strategies.

priority-list interface

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

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

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

Syntax Description

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.

Defaults

No queueing priorities are established by default.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

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

Examples

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

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

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

Related Commands

Command	Description
priority-group	Assigns the specified priority list to an interface.
priority-list default	Assigns a priority queue for those packets that do not match any other rule in the priority list.
priority-list protocol	Establishes queueing priorities based on the protocol type.
priority-list queue-limit	Specifies the maximum number of packets that can be waiting in each of the priority queues.
show queue	Displays the contents of packets inside a queue for a particular interface or VC.
show queueing	Lists all or selected configured queueing strategies.

priority-list protocol

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

priority-list *list-number* **protocol** *protocol-name* {**high** | **medium** | **normal** | **low**} *queue-keyword keyword-value*

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

Syntax Description

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 9 in the "Usage Guidelines" section of this command.

Defaults

No queueing priorities are established.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(13)T	This command was modified to remove apollo, vines, and xns 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.

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 Table 9, Table 10, and Table 11 to configure the queueing priorities for your system.

Table 9 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.
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 10 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 11 lists common UDP services and their port numbers.

Table 10 Common TCP Services and Their Port Numbers

Service	Port
FTP data	20
FTP	21

Table 10 Common TCP Services and Their Port Numbers (continued)

Service	Port
Simple Mail Transfer Protocol (SMTP)	25
Telnet	23

Table 11 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
TFTP	69

Note Table 10 and Table 11 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 assigns 1 as the arbitrary priority list number, specifies DECnet as the protocol type, and assigns a high-priority level to the DECnet packets sent on this interface:

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

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

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

The following example assigns a medium-priority level to Telnet packets:

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

The following example assigns a medium-priority level to UDP DNS packets:

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

The following example assigns 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 assigns 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 assigns 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-list queue-limit** command in global configuration mode. To select the normal queue, use the **no** form of this command.

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

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

Syntax Description

list-number	Any number from 1 to 16 that identifies the priority list.
high-limit *medium-limit* *normal-limit* *low-limit*	(Optional) 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 Table 12.

Defaults

This command is not enabled by default.

See Table 12 in the "Usage Guidelines" section of this command for a list of the default queue limit arguments.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

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 arguments are listed in Table 12.

Table 12 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 ISDN (Integrated Services Digital Network) call in the queue, changing the configuration of the **priority-list queue-limit** command drops the call from the queue. For more information about priority queueing, refer to the *Quality of Service Configuration Guide,* Release 12.2.

Examples

The following example sets the maximum packets in the priority queue to 10:

```
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.

protect

To configure a virtual circuit (VC) class with protected group or protected VC status for application to a VC bundle member, use the **protect** command in vc-class configuration mode. To remove the protected status from the VC class, use the **no** form of this command.

To configure a specific VC or permanent virtual circuit (PVC) as part of a protected group of the bundle or to configure it as an individually protected VC or PVC bundle member, use the **protect** command in bundle-vc configuration mode. To remove the protected status from the VC or PVC, use the **no** form of this command.

protect {**group** | **vc**}

no protect {**group** | **vc**}

Syntax Description

group	Configures the VC or PVC bundle member as part of the protected group of the bundle.
vc	Configures the VC or PVC member as individually protected.

Defaults

The VC or PVC neither belongs to the protected group nor is it an individually protected VC or PVC.

Command Modes

VC-class configuration (for a VC class)

Bundle-vc configuration (for ATM VC bundle members)

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.0(23)S	This command was made available in vc-class and bundle-vc configuration modes on the 8-port OC-3 STM-1 ATM line card for Cisco 12000 series Internet routers.

Usage Guidelines

Use the **protect** command in vc-class configuration mode to configure a VC class to contain protected group or individual protected VC status. When the class is applied to the VC bundle member, that VC is characterized by the protected status. You can also apply this command directly to a VC in bundle-vc configuration mode.

When a protected VC goes down, it takes the bundle down. When all members of a protected group go down, the bundle goes down.

To use the **protect** command in vc-class configuration mode, first enter the **vc-class atm** global configuration command.

The **protect** 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 the **protect** command in bundle-vc configuration mode, first enter the **bundle** command to enact bundle configuration mode for the bundle containing the VC member to be configured. Then enter the **pvc-bundle** configuration command to add the VC to the bundle as a member of it.

VCs in a VC bundle are subject to the following configuration inheritance guidelines (listed in order of next highest precedence):

- VC configuration in bundle-vc mode
- Bundle configuration in bundle mode (with effect of assigned vc-class configuration)
- Subinterface configuration in subinterface mode

Examples

The following example configures a class called "control-class" to include a **protect** command, which, when applied to a VC bundle member, configures the VC as an individually protected VC bundle member. When this protected VC goes down, it takes the bundle down.

```
vc-class atm control-class
 protect vc
```

Related Commands

Command	Description
bump	Configures the bumping rules for a VC class that can be assigned to a VC bundle.
bundle	Creates a bundle or modifies an existing bundle to enter bundle configuration mode.
class-vc	Assigns a VC class to an ATM PVC, SVC, or VC bundle member.
precedence	Configures precedence levels for a VC class that can be assigned to a VC bundle and thus applied to all VC members of that bundle; configures precedence levels for an individual VC or PVC bundle member.
pvc	Creates or assigns a name to an ATM PVC, specifies the encapsulation type on an ATM PVC, and enters interface-ATM-VC configuration mode.
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.
vbr-nrt	Configures the VBR-NRT QoS and specifies output peak cell rate, output sustainable cell rate, and output maximum burst cell size for an ATM PVC, SVC, VC class, or VC bundle member.
vc-class atm	Configures a VC class for an ATM VC or interface.

pvc-bundle

To add a virtual circuit (VC) to a bundle as a member of the bundle and enter bundle-vc configuration mode in order to configure that VC bundle member, use the **pvc-bundle** command in bundle configuration mode. To remove the VC from the bundle, use the **no** form of this command.

pvc-bundle *pvc-name* [*vpi/*] [*vci*]

no pvc-bundle *pvc-name* [*vpi/*] [*vci*]

Syntax Description

pvc-name	The name of the permanent virtual circuit (PVC) bundle.
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 7500 series routers, the value range is from 0 to 255; on the Cisco 4500 and 4700 routers, the value range is from 0 to 1 less than the quotient of 8192 divided by the value set by the **atm vc-per-vp** command. The *vpi* and *vci* arguments cannot both be set to 0; if one is 0, the other cannot be 0.
vci	(Optional) ATM network virtual channel identifier (VCI) for this PVC. The value range is from 0 to 1 less than the maximum value set for this interface by the **atm vc-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.

Defaults

No default behavior or values

Command Modes

Bundle configuration

Command History

Release	Modification
12.0(3)T	This command was introduced.

Usage Guidelines

Each bundle can contain multiple VCs having different QoS attributes. This command associates a VC with a bundle, making it a member of that bundle. Before you can add a VC to a bundle, the bundle must exist. Use the **bundle** command to create a bundle. You can also use this command to configure a VC that already belongs to a bundle. You enter the command in the same way, giving the name of the VC bundle member.

The **pvc-bundle** command enters bundle-vc configuration mode, in which you can specify VC-specific and VC class attributes for the VC.

Examples

The following example specifies an existing bundle called chicago and enters bundle configuration mode. Then it adds two VCs to the bundle. For each added VC, bundle-vc mode is entered and a VC class is attached to the VC to configure it.

```
bundle chicago
 pvc-bundle chicago-control 207
  class control-class
 pvc-bundle chicago-premium 206
  class premium-class
```

The following example configures the PVC called chicago-control, an existing member of the bundle called chicago, to use class-based weighted fair queueing (CBWFQ). The example configuration attaches the policy map called policy1 to the PVC. Once the policy map is attached, the classes comprising policy1 determine the service policy for the PVC chicago-control.

```
bundle chicago
 pvc-bundle chicago-control 207
  class control-class
  service-policy output policy1
```

Related Commands

Command	Description
atm vc-per-vp	Sets the maximum number of VCIs to support per VPI.
bump	Configures the bumping rules for a VC class that can be assigned to a VC bundle.
class-bundle	Configures a VC bundle with the bundle-level commands contained in the specified VC class.
class-vc	Assigns a VC class to an ATM PVC, SVC, or VC bundle member.
precedence	Configures precedence levels for a VC member of a bundle, or for a VC class that can be assigned to a VC bundle.
protect	Configures a VC class with protected group or protected VC status for application to a VC bundle member.
pvc	Creates or assigns a name to an ATM PVC, specifies the encapsulation type on an ATM PVC, and enters interface-ATM-VC configuration mode.
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.
vbr-nrt	Configures the VBR-NRT QoS and specifies output peak cell rate, output sustainable cell rate, and output maximum burst cell size for an ATM PVC, SVC, VC class, or VC bundle member.

qos pre-classify

To enable quality of service (QoS) preclassification, use the **qos pre-classify** command in interface configuration mode. To disable the QoS preclassification feature, use the **no** form of this command.

qos pre-classify

no qos pre-classify

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)XE3	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(2)T	This command was implemented on the following platforms: Cisco 2600 and Cisco 3600 series routers.

Usage Guidelines

This command is restricted to tunnel interfaces, virtual templates, and crypto maps. The **qos pre-classify** command is unavailable on all other interface types.

The **qos pre-classify** command can be enabled for IP packets only.

Examples

The following example enables the QoS for Virtual Private Networks (VPNs) feature on tunnel interfaces and virtual templates:

```
Router(config-if)# qos pre-classify
```

The following example enables the QoS for VPNs feature on crypto maps:

```
Router(config-crypto-map)# qos pre-classify
```

Related Commands

Command	Description
show interfaces	Displays statistics for the interfaces configured on a router or access server.
show queue	Displays the contents of packets inside a queue for a particular interface or VC.

queue-limit

To specify or modify the maximum number of packets the queue can hold for a class policy configured in a policy map, use the **queue-limit** command in policy-map class configuration mode. To remove the queue packet limit from a class, use the **no** form of this command.

queue-limit *number-of-packets*

no queue-limit *number-of-packets*

Syntax Description

number-of-packets	A number in the range from 1 to 64 specifying the maximum number of packets that the queue for this class can accumulate.

Defaults

On the Versatile Interface Processor (VIP)-based platforms, the default value is chosen as a function of the bandwidth assigned to the traffic class. The default value is also based on available buffer memory. If sufficient buffer memory is available, the default **queue-limit** value is equal to the number of 250-byte packets that would lead to a latency of 500 milliseconds (ms) when the packets are delivered at the configured rate. For example, if two 250-byte packets are required to lead to a latency of 500 ms, the default *number-of-packets* value would be 2.

On all other platforms, the default is 64.

Command Modes

Policy-map class configuration

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. Support for VIP-enabled Cisco 7500 series routers was added.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T. Support for VIP-enabled Cisco 7500 series routers was added.

Usage Guidelines

Weighted fair queueing (WFQ) creates a queue for every class for which a class map is defined. Packets satisfying the match criteria for a class accumulate in the queue reserved for the class until they are sent, which occurs when the queue is serviced by the fair queueing process. When the maximum packet threshold you defined for the class is reached, enqueueing of any further packets to the class queue causes tail drop or, if Weighted Random Early Detection (WRED) is configured for the class policy, packet drop to take effect.

Examples

The following example configures a policy map called policy11 to contain policy for a class called acl203. Policy for this class is set so that the queue reserved for it has a maximum packet limit of 40.

```
policy-map policy11
 class acl203
  bandwidth 2000
  queue-limit 40
```

Related Commands

Command	Description
class (policy-map)	Specifies the name of the class whose policy you want to create or change, and the default class (commonly known as the class-default class) before you configure its policy.
class class-default	Specifies the default traffic class whose bandwidth is to be configured or modified.
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.

queue-list default

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

queue-list *list-number* **default** *queue-number*

no queue-list *list-number* **default** *queue-number*

Syntax Description

list-number	Number of the queue list. Any number from 1 to 16 that identifies the queue list.
queue-number	Number of the queue. Any number from 1 to 16.

Defaults

Disabled

The default number of the queue list is queue number 1.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

When you use multiple rules, remember that the system reads the **queue-list** commands in order of appearance. When classifying a packet, the system searches the list of rules specified by **queue-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.

Queue number 0 is a system queue. It is emptied before any of the other queues are processed. The system enqueues high-priority packets, such as keepalives, to this queue.

Use the **show interfaces** command to display the current status of the output queues.

Examples

In the following example, the default queue for list 10 is set to queue number 2:

```
queue-list 10 default 2
```

Related Commands

Command	Description
custom-queue-list	Assigns a custom queue list to an interface.
queue-list interface	Establishes queueing priorities on packets entering on an interface.
queue-list protocol	Establishes queueing priority based on the protocol type.
queue-list queue byte-count	Specifies how many bytes the system allows to be delivered from a given queue during a particular cycle.
queue-list queue limit	Designates the queue length limit for a queue.
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.

queue-list interface

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

queue-list *list-number* **interface** *interface-type interface-number queue-number*

no queue-list *list-number* **interface** *interface-type interface-number queue-number*

Syntax Description

list-number	Number of the queue list. Any number from 1 to 16 that identifies the queue list.
interface-type	Type of the interface.
interface-number	Number of the interface.
queue-number	Number of the queue. Any number from 1 to 16.

Defaults

No queueing priorities are established.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

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

Examples

In the following example, queue list 4 establishes queueing priorities for packets entering on interface tunnel 3. The queue number assigned is 10.

```
queue-list 4 interface tunnel 3 10
```

Related Commands

Command	Description
custom-queue-list	Assigns a custom queue list to an interface.
queue-list default	Assigns a priority queue for those packets that do not match any other rule in the queue list.
queue-list protocol	Establishes queueing priority based on the protocol type.
queue-list queue byte-count	Specifies how many bytes the system allows to be delivered from a given queue during a particular cycle.
queue-list queue limit	Designates the queue length limit for a queue.
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.

queue-list protocol

To establish queueing priority based upon the protocol type, use the **queue-list protocol** command in global configuration mode. To remove an entry from the list, use the **no** form of this command.

queue-list *list-number* **protocol** *protocol-name queue-number queue-keyword keyword-value*

no queue-list *list-number* **protocol** *protocol-name queue-number queue-keyword keyword-value*

Syntax Description

list-number	Number of the queue list. Any number from 1 to 16.
protocol-name	Protocol type: **aarp**, **appletalk**, **arp**, **bridge** (transparent), **clns**, **clns_es**, **clns_is**, **cmns**, **compressedtcp**, **decnet**, **decnet_node**, **decnet_routerl1**, **decnet_routerl2**, **dlsw**, **ip**, **ipx**, **pad**, **rsrb**, **stun** and **x25**.
queue-number	Number of the queue. Any number from 1 to 16.
queue-keyword keyword-value	Possible keywords are **fragments, gt, list, lt, tcp**, and **udp**. See Table 9 from the **priority-list protocol** command.

Defaults

No queueing priorities are established.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(13)	This command was modified to remove apollo, vines, and xns 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.

Usage Guidelines

When you use multiple rules for a single protocol, remember that the system reads the **queue-list** commands in order of appearance. When classifying a packet, the system searches the list of rules specified by **queue-list** commands for a matching protocol. 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 Table 9, Table 10, and Table 11 in the **priority-list protocol** command section to configure the queueing priorities for your system.

Examples

The following example assigns 1 as the custom queue list, specifies DECnet as the protocol type, and assigns 3 as a queue number to the packets sent on this interface:

```
queue-list 1 protocol decnet 3
```

The following example assigns DECnet packets with a size greater than 200 bytes to queue number 2:

```
queue-list 2 protocol decnet 2 gt 200
```

The following example assigns DECnet packets with a size less than 200 bytes to queue number 2:

```
queue-list 4 protocol decnet 2 lt 200
```

The following example assigns traffic that matches IP access list 10 to queue number 1:

```
queue-list 1 protocol ip 1 list 10
```

The following example assigns Telnet packets to queue number 2:

```
queue-list 4 protocol ip 2 tcp 23
```

The following example assigns User Datagram Protocol (UDP) Domain Name Service packets to queue number 2:

```
queue-list 4 protocol ip 2 udp 53
```

The following example assigns traffic that matches Ethernet type code access list 201 to queue number 1:

```
queue-list 1 protocol bridge 1 list 201
```

Related Commands

Command	Description
custom-queue-list	Assigns a custom queue list to an interface.
queue-list default	Assigns a priority queue for those packets that do not match any other rule in the queue list.
queue-list queue byte-count	Specifies how many bytes the system allows to be delivered from a given queue during a particular cycle.
queue-list queue limit	Designates the queue length limit for a queue.
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.

queue-list queue byte-count

To specify how many bytes the system allows to be delivered from a given queue during a particular cycle, use the **queue-list queue byte-count** command in global configuration mode. To return the byte count to the default value, use the **no** form of this command.

queue-list *list-number* **queue** *queue-number* **byte-count** *byte-count-number*

no queue-list *list-number* **queue** *queue-number* **byte-count** *byte-count-number*

Syntax Description

list-number	Number of the queue list. Any number from 1 to 16.
queue-number	Number of the queue. Any number from 1 to 16.
byte-count-number	The average number of bytes the system allows to be delivered from a given queue during a particular cycle.

Defaults

This command is disabled by default. The default byte count is 1500 bytes.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Examples

In the following example, queue list 9 establishes the byte count as 1400 for queue number 10:

```
queue-list 9 queue 10 byte-count 1400
```

Related Commands

Command	Description
custom-queue-list	Assigns a custom queue list to an interface.
queue-list default	Assigns a priority queue for those packets that do not match any other rule in the queue list.
queue-list interface	Establishes queueing priorities on packets entering on an interface.
queue-list protocol	Establishes queueing priority based on the protocol type.
queue-list queue byte-count	Specifies how many bytes the system allows to be delivered from a given queue during a particular cycle.
queue-list queue limit	Designates the queue length limit for a queue.
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.

queue-list queue limit

To designate the queue length limit for a queue, use the **queue-list queue limit** command in global configuration mode. To return the queue length to the default value, use the **no** form of this command.

queue-list *list-number* **queue** *queue-number* **limit** *limit-number*

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

Syntax Description

list-number	Number of the queue list. Any number from 1 to 16.
queue-number	Number of the queue. Any number from 1 to 16.
limit-number	Maximum number of packets that can be enqueued at any time. The range is from 0 to 32767 queue entries. A value of 0 means that the queue can be of unlimited size.

Defaults

The default queue length limit is 20 entries.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Examples

In the following example, the queue length of queue 10 is increased to 40:

```
queue-list 5 queue 10 limit 40
```

Related Commands

Command	Description
custom-queue-list	Assigns a custom queue list to an interface.
queue-list default	Assigns a priority queue for those packets that do not match any other rule in the queue list.
queue-list interface	Establishes queueing priorities on packets entering on an interface.
queue-list protocol	Establishes queueing priority based on the protocol type.
queue-list queue byte-count	Specifies how many bytes the system allows to be delivered from a given queue during a particular cycle.
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.

random-detect discard-class

To configure the weighted random early detection (WRED) parameters for a discard-class value for a class policy in a policy map, use the **random-detect discard-class** command in policy-map configuration mode. To disable this feature, use the **no** form of this command.

random-detect discard-class *value min-threshold max-threshold mark-prob-denominator*

no random-detect discard-class *value min-threshold max-threshold mark-prob-denominator*

Syntax Description

value	Discard class. Valid values are 0 to 7.
min-threshold	Minimum threshold in number of packets. Valid values are 1 to 4096. When the average queue length reaches the minimum threshold, WRED randomly drops some packets with the specified IP precedence.
max-threshold	Maximum threshold in number of packets. Valid values are 1 to 4096. When the average queue length exceeds the maximum threshold, WRED drops all packets with the specified IP precedence.
mark-prob-denominator	Denominator for the fraction of packets dropped when the average queue depth is at the maximum threshold. For example, if the denominator is 512, 1 out of every 512 packets is dropped when the average queue is at the maximum threshold. Valid values are 1 to 65535. The default is 10; 1 out of every 10 packets is dropped at the maximum threshold.

Defaults

To return the values to the default for the discard class, use the **no** form of this command.

Command Modes

Policy-map configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

When you configure the **random-detect discard-class** command on an interface, packets are given preferential treatment based on the discard class of the packet. Use the **random-detect discard-class** command to adjust the discard class for different discard class values.

Examples

The following example shows that if the discard class is 2, there is a 10 percent chance that packets will be dropped if there are more packets than the minimum threshold of 100 packets or there are fewer packets than the maximum threshold of 200 packets:

```
policy-map set-MPLS-PHB
  class IP-AF11
    bandwidth percent 40
    random-detect discard-class-based
    random-detect-discard-class 2 100 200 10
```

Related Commands

Command	Description
bandwidth (policy-map class)	Specifies or modifies the bandwidth allocated for a class belonging to a policy map.
fair-queue (class-default)	Specifies the number of dynamic queues to be reserved for use by the class-default class as part of the default class policy.
random-detect discard-class-based	Bases WRED on the discard class value of a packet.
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.

random-detect discard-class-based

To base weighted random early detection (WRED) on the discard class value of a packet, use the **random-detect discard-class-based** command in policy-map configuration mode. To disable this feature, use the **no** form of this command.

random-detect discard-class-based

no random-detect discard-class-based

Syntax Description

This command has no arguments or keywords.

Defaults

The defaults are router-dependent.

Command Modes

Policy-map configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

Enter this command so that WRED is based on the discard class instead of on the IP precedence field.

Examples

The following example shows that random detect is based on the discard class value of a packet:

```
policy-map name
  class-name
    bandwidth percent 40
    random-detect discard-class-based
```

Related Commands

Command	Description
match discard-class	Matches packets of a certain discard class.

random-detect dscp

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

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

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

Syntax Description

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

Defaults

If WRED is using the DSCP value to calculate the drop probability of a packet, all entries of the DSCP table are initialized with the default settings shown in Table 13 in the “Usage Guidelines” section of this command.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(5)T	This command was introduced.

Usage Guidelines

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

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

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

Table 13 lists the default settings used by the **random-detect dscp** command for the DSCP value specified. Table 13 lists the DSCP value, and its corresponding minimum threshold, maximum threshold, and mark probability. The last row of the table (the row labeled "default") shows the default settings used for any DSCP value not specifically shown in the table.

Table 13 random-detect dscp Default Settings

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

Examples

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

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

Related Commands

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

random-detect (interface)

To enable Weighted Random Early Detection (WRED) or distributed WRED (DWRED), use the **random-detect** command in interface configuration mode. To configure WRED as class policy in a policy map, use the **random-detect** interface and policy-map class configuration command. To disable WRED or DWRED, use the **no** form of this command.

random-detect [*dscp-based* | *prec-based*]

no random-detect [*dscp-based* | *prec-based*]

Syntax Description

dscp-based	(Optional) Specifies that WRED is to use the differentiated services code point (DSCP) value when it calculates the drop probability for a packet.
prec-based	(Optional) Specifies that WRED is to use the IP Precedence value when it calculates the drop probability for a packet.

Defaults

WRED and DWRED are disabled by default.

If you choose not to use either the *dscp-based* or the *prec-based* argument, WRED uses the IP Precedence value (the default method) to calculate drop probability for the packet.

Command Modes

Interface configuration when used on an interface

Policy-map class configuration when used to specify class policy in a policy map

Command History

Release	Modification
11.1 CC	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T. Arguments were added to support Differentiated Services (DiffServ) and Assured Forwarding (AF) Per Hop Behavior (PHB).

Usage Guidelines

WRED is a congestion avoidance mechanism that slows traffic by randomly dropping packets when congestion exists. DWRED is similar to WRED but uses the Versatile Interface Processor (VIP) instead of the Route Switch Processor (RSP). WRED and DWRED are most useful with protocols like TCP that respond to dropped packets by decreasing the transmission rate.

The router automatically determines parameters to use in the WRED calculations. To change these parameters, use the **random-detect precedence** command.

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

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

WRED in a Policy Map

You can configure WRED as part of the policy for a standard class or the default class. The WRED **random-detect** command and the weighted fair queueing (WFQ) **queue-limit** command are mutually exclusive for class policy. If you configure WRED, its packet drop capability is used to manage the queue when packets exceeding the configured maximum count are enqueued. If you configure the WFQ **queue-limit** command for class policy, tail drop is used.

To configure a policy map and create class policies, use the **policy-map** and **class** (policy-map) commands. When specifying class policy within a policy map, you can use the **random-detect** command with either of the following commands:

- **bandwidth** (policy-map class)
- **fair-queue** (class-default)—for the default class only

Note that if you use WRED packet drop instead of tail drop for one or more classes composing a policy map, you must ensure that WRED is not configured for the interface to which you attach that service policy.

The DWRED feature is not supported for class policy.

Two Methods for Calculating the Drop Probability of a Packet

This command includes two optional arguments, *dscp-based* and *prec-based*, that determine the method WRED uses to calculate the drop probability of a packet.

Note the following points when deciding which method to instruct WRED to use:

- With the *dscp-based* argument, WRED uses the DSCP value (that is, the first six bits of the IP type of service (ToS) byte) to calculate the drop probability.
- With the *prec-based* argument, WRED will use the IP Precedence value to calculate the drop probability.
- The *dscp-based* and *prec-based* arguments are mutually exclusive.
- If neither argument is specified, WRED uses the IP Precedence value to calculate the drop probability (the default method).

Examples

The following example configures WRED on the High-Speed Serial Interface (HSSI) 0/0/0 interface:

```
interface Hssi0/0/0
 random-detect
```

The following example configures the policy map called policy1 to contain policy specification for the class called class1. During times of congestion, WRED packet drop is used instead of tail drop.

```
! The following commands create the class map called class1:
class-map class1
 match input-interface FE0/1

! The following commands define policy1 to contain policy specification for class1:
policy-map policy1
 class class1
  bandwidth 1000
  random-detect
```

The following example enables WRED to use the DSCP value 8. The minimum threshold for the DSCP value 8 is 24 and the maximum threshold is 40. This configuration was performed at the interface level.

```
Router(config-if)# interface seo/0
Router(config-if)# random-detect dscp-based
Router(config-if)# random-detect dscp 8 24 40
```

The following example enables WRED to use the DSCP value 8 for class c1. The minimum threshold for DSCP value 8 is 24 and the maximum threshold is 40. The last line attaches the service policy to the output interface or virtual circuit (VC) p1.

```
Router(config-if)# class-map c1
Router(config-cmap)# match access-group 101
Router(config-if)# policy-map p1
Router(config-pmap)# class c1
Router(config-pmap-c)# bandwidth 48
Router(config-pmap-c)# random-detect dscp-based
Router(config-pmap-c)# random-detect dscp 8 24 40
Router(config-if)# service-policy output p1
```

Related Commands

Command	Description
random-detect dscp	Changes the minimum and maximum packet thresholds for the DSCP value.
random-detect exponential-weighting-constant	Configures the WRED and DWRED exponential weight factor for the average queue size calculation.
random-detect flow	Enables flow-based WRED.
random-detect precedence	Configures WRED and DWRED parameters for a particular IP Precedence.
show interfaces	Displays statistics for all interfaces configured on the router or access server.
show queueing	Lists all or selected configured queueing strategies.
show tech-support rsvp	Generates a report of all RSVP-related information.

random-detect (per VC)

To enable per-virtual circuit (VC) Weighted Random Early Detection (WRED) or per-VC VIP-distributed WRED (DWRED), use the **random-detect** command in VC submode mode. To disable per-VC WRED and per-VC DWRED, use the **no** form of this command.

random-detect [**attach** *group-name*]

no random-detect [**attach** *group-name*]

Syntax Description

attach *group-name*	(Optional) The name of the WRED or DWRED group.

Defaults

WRED and DWRED are disabled by default.

Command Modes

VC submode

Command History

Release	Modification
12.0(3)T	This command was introduced.

Usage Guidelines

WRED is a congestion avoidance mechanism that slows traffic by randomly dropping packets when congestion exists. DWRED is similar to WRED but uses the Versatile Interface Processor (VIP) instead of the Route Switch Processor (RSP). WRED and DWRED are most useful with protocols like TCP that respond to dropped packets by decreasing the transmission rate.

WRED and DWRED are configurable at the interface and per-VC levels. The VC-level WRED or DWRED configuration will override the interface-level configuration if WRED or DWRED is also configured at the interface level.

Use this command to configure a single ATM VC or a VC that is a member of a bundle.

Note the following points when using the **random-detect** (per VC) command:

- If you use this command without the optional **attach** keyword, default WRED or DWRED parameters (such as minimum and maximum thresholds) are used.
- If you use this command with the optional **attach** keyword, the parameters defined by the specified WRED or DWRED parameter group are used. (WRED or DWRED parameter groups are defined through the **random-detect-group** command.) If the specified WRED or DWRED group does not exist, the VC is configured with default WRED or DWRED parameters.

When this command is used to configure an interface-level WRED or DWRED group to include per-VC WRED or DWRED as a drop policy, the configured WRED or DWRED group parameters are inherited under the following conditions:

- All existing VCs—including Resource Reservation Protocol (RSVP) switched virtual circuits (SVCs) that are not specifically configured with a VC-level WRED or DWRED group—will inherit the interface-level WRED or DWRED group parameters.
- Except for the VC used for signalling and the Interim Local Management Interface (ILMI) VC, any VCs created after the configuration of an interface-level DWRED group will inherit the parameters.

When an interface-level WRED or DWRED group configuration is removed, per-VC WRED or DWRED parameters are removed from any VC that inherited them from the configured interface-level WRED or DWRED group.

When an interface-level WRED or DWRED group configuration is modified, per-VC WRED or DWRED parameters are modified accordingly if the WRED or DWRED parameters were inherited from the configured interface-level WRED or DWRED group configuration.

This command is only supported on interfaces that are capable of VC-level queueing. The only currently supported interface is the Enhanced ATM port adapter (PA-A3).

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

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

Examples

The following example configures per-VC WRED for the permanent virtual circuit (PVC) called cisco. Because the **attach** keyword was not used, WRED uses default parameters.

```
pvc cisco 46
 random-detect
```

The following example creates a DWRED group called Rome and then applies the parameter group to an ATM PVC:

```
! The following commands create the DWRED parameter group Rome:
random-detect-group Rome
 precedence rsvp 46 50 10
 precedence 1 32 50 10
 precedence 2 34 50 10
 precedence 3 36 50 10
 precedence 4 38 50 10
 precedence 5 40 50 10
 precedence 6 42 50 10
 precedence 7 44 50 10
 exit
exit
```

```
! The following commands create a PVC on an ATM interface and then apply the
! DWRED group Rome to that PVC:
interface ATM2/0.23 point-to-point
 ip address 10.9.23.10 255.255.255.0
 no ip mroute-cache
 pvc vc1 201/201
  random-detect attach Rome
  vbr-nrt 2000 1000 200
  encapsulation aal5snap
```

The following **show queueing** command displays the current settings for each of the IP Precedences following configuration of per-VC DWRED:

```
Router# show queueing random-detect interface atm2/0.23 vc 201/201

random-detect group Rome:

exponential weight 9
class     min-threshold    max-threshold    mark-probability
----------------------------------------------------------

0         30               50               1/10
1         32               50               1/10
2         34               50               1/10
3         36               50               1/10
4         38               50               1/10
5         40               50               1/10
6         42               50               1/10
7         44               50               1/10
rsvp      46               50               1/10
```

Related Commands

Command	Description
class (policy-map)	Specifies the name of the class whose policy you want to create or change, and the default class (commonly known as the class-default class) before you configure its policy.
random-detect exponential-weighting-constant	Configures the WRED and DWRED exponential weight factor for the average queue size calculation.
random-detect-group	Defines the WRED or DWRED parameter group.
random-detect precedence	Configures WRED and DWRED parameters for a particular IP Precedence.
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	Lists all or selected configured queueing strategies.

random-detect ecn

To enable explicit congestion notification (ECN), use the **random-detect ecn** command in policy-map class configuration mode. To disable ECN, use the **no** form of this command.

random-detect ecn

no random-detect ecn

Syntax Description

This command has no arguments or keywords.

Defaults

By default, ECN is disabled.

Command Modes

Policy-map class configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.

Usage Guidelines

If ECN is enabled, ECN can be used whether Weighted Random Early Detection (WRED) is based on the IP precedence value or the differentiated services code point (DSCP) value.

Examples

The following example enables ECN in a policy map called "pol1":

```
Router(config)# policy-map pol1
Router(config-pmap)# class class-default
Router(config-pmap)# bandwidth per 70
Router(config-pmap-c)# random-detect
Router(config-pmap-c)# random-detect ecn
```

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 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.

random-detect exponential-weighting-constant

To configure the Weighted Random Early Detection (WRED) and distributed WRED (DWRED) exponential weight factor for the average queue size calculation for the queue, use the **random-detect exponential-weighting-constant** command in interface configuration mode. To configure the exponential weight factor for the average queue size calculation for the queue reserved for a class, use the **random-detect exponential-weighting-constant** command in policy-map class configuration mode. To return the value to the default, use the **no** form of this command.

random-detect exponential-weighting-constant *exponent*

no random-detect exponential-weighting-constant

Syntax Description

exponent	Exponent from 1 to 16 used in the average queue size calculation.

Defaults

The default exponential weight factor is 9.

Command Modes

Interface configuration when used on an interface

Policy-map class configuration when used to specify class policy in a policy map, or when used in the Modular Quality of Service Command-Line Interface (MQC)

Command History

Release	Modification
11.1 CC	This command was introduced.
12.0(5)T	This command was made available as a policy-map class configuration command.
12.0(5)XE	This command was integrated into Cisco IOS Release 12.0(5)XE. Support for VIP-enabled Cisco 7500 series routers was added.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T. Support for VIP-enabled Cisco 7500 series routers was added.

Usage Guidelines

WRED is a congestion avoidance mechanism that slows traffic by randomly dropping packets when congestion exists. DWRED is similar to WRED but uses the Versatile Interface Processor (VIP) instead of the Route Switch Processor (RSP). WRED and DWRED are most useful with protocols like TCP that respond to dropped packets by decreasing the transmission rate.

Use this command to change the exponent used in the average queue size calculation for the WRED and DWRED services. You can also use this command to configure the exponential weight factor for the average queue size calculation for the queue reserved for a class

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

The DWRED feature is not supported for class policy.

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

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

Examples

The following example configures WRED on an interface with a weight factor of 10:

```
interface Hssi0/0/0
 description 45Mbps to R1
 ip address 10.200.14.250 255.255.255.252
 random-detect
 random-detect exponential-weighting-constant 10
```

The following example configures the policy map called policy1 to contain policy specification for the class called class1. During times of congestion, WRED packet drop is used instead of tail drop. The weight factor used for the average queue size calculation for the queue for class1 is 12.

```
! The following commands create the class map called class1:
class-map class1
 match input-interface FE0/1

! The following commands define policy1 to contain policy specification for class1:
policy-map policy1
 class class1
 bandwidth 1000
 random-detect
 random-detect exponential-weighting-constant 12
```

The following example configures policy for a traffic class named int10 to configure the exponential weight factor as 12. This is the weight factor used for the average queue size calculation for the queue for traffic class int10. WRED packet drop is used for congestion avoidance for traffic class int10, not tail drop.

```
policy-map policy12
 class int10
 bandwidth 2000
 random-detect exponential-weighting-constant 12
```

Related Commands

Command	Description
bandwidth (policy-map class)	Specifies or modifies the bandwidth allocated for a class belonging to a policy map.
exponential-weighting-constant	Configures the exponential weight factor for the average queue size calculation for a WRED parameter group.
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.
precedence	Configures precedence levels for a VC or PVC class that can be assigned to a VC or PVC bundle and thus applied to all of the members of that bundle.
precedence (WRED group)	Configures a WRED group for a particular IP Precedence.
random-detect dscp	Changes the minimum and maximum packet thresholds for the DSCP value.
random-detect (per VC)	Enables per-VC WRED or per-VC DWRED.
random-detect precedence	Configures WRED and DWRED parameters for a particular IP Precedence.
show policy-map	Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps.
show policy-map interface	Displays the configuration of all classes configured for all service policies on the specified interface or displays the classes for the service policy for a specific PVC on the interface.
show queue	Displays the contents of packets inside a queue for a particular interface or VC.
show queueing	Lists all or selected configured queueing strategies.

random-detect flow

To enable flow-based Weighted Random Early Detection (WRED), use the **random-detect flow** command in interface configuration mode. To disable flow-based WRED, use the **no** form of this command.

random-detect flow

no random-detect flow

Syntax Description

This command has no arguments or keywords.

Defaults

Flow-based WRED is disabled by default.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(3)T	This command was introduced.

Usage Guidelines

You must use this command to enable flow-based WRED before you can use the **random-detect flow average-depth-factor** and **random-detect flow count** commands to further configure the parameters of flow-based WRED.

Before you can enable flow-based WRED, you must enable and configure WRED. For complete information, refer to the *Cisco IOS Quality of Service Solutions Configuration Guide*.

Examples

The following example enables flow-based WRED on serial interface 1:

```
interface Serial1
 random-detect
 random-detect flow
```

Related Commands

Command	Description
random-detect dscp	Changes the minimum and maximum packet thresholds for the DSCP value.
random-detect exponential-weighting-constant	Configures the WRED and DWRED exponential weight factor for the average queue size calculation.
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.
random-detect precedence	Configures WRED and DWRED parameters for a particular IP Precedence.
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	Lists all or selected configured queueing strategies.

random-detect flow average-depth-factor

To set the multiplier to be used in determining the average depth factor for a flow when flow-based Weighted Random Early Detection (WRED) is enabled, use the **random-detect flow average-depth-factor** command in interface configuration mode. To remove the current flow average depth factor value, use the **no** form of this command.

random-detect flow average-depth-factor *scaling-factor*

no random-detect flow average-depth-factor *scaling-factor*

Syntax Description

scaling-factor	The scaling factor can be a number from 1 to 16.

Defaults

The default average depth factor is 4.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(3)T	This command was introduced.

Usage Guidelines

Use this command to specify the scaling factor that flow-based WRED should use in scaling the number of buffers available per flow and in determining the number of packets allowed in the output queue for each active flow. This scaling factor is common to all flows. The outcome of the scaled number of buffers becomes the per-flow limit.

If this command is not used and flow-based WRED is enabled, the average depth scaling factor defaults to 4.

A flow is considered nonadaptive—that is, it takes up too much of the resources—when the average flow depth times the specified multiplier (scaling factor) is less than the depth for the flow, for example:

average-flow-depth * (scaling factor) < flow-depth

Before you use this command, you must use the **random-detect flow** command to enable flow-based WRED for the interface. To configure flow-based WRED, you may also use the **random-detect flow count** command.

Examples

The following example enables flow-based WRED on serial interface 1 and sets the scaling factor for the average flow depth to 8:

```
interface Serial1
 random-detect
 random-detect flow
 random-detect flow average-depth-factor 8
```

Related Commands

Command	Description
random-detect dscp	Changes the minimum and maximum packet thresholds for the DSCP value.
random-detect exponential-weighting-constant	Configures the WRED and DWRED exponential weight factor for the average queue size calculation.
random-detect flow	Enables flow-based WRED.
random-detect flow count	Sets the flow count for flow-based WRED.
random-detect precedence	Configures WRED and DWRED parameters for a particular IP Precedence.
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	Lists all or selected configured queueing strategies.

random-detect flow count

To set the flow count for flow-based Weighted Random Early Detection (WRED), use the **random-detect flow count** command in interface configuration mode. To remove the current flow count value, use the **no** form of this command.

random-detect flow count *number*

no random-detect flow count *number*

Syntax Description

number	Specifies a value from 16 to 2^{15} (32768).

Defaults

256

Command Modes

Interface configuration

Command History

Release	Modification
12.0(3)T	This command was introduced.

Usage Guidelines

Before you use this command, you must use the **random-detect flow** command to enable flow-based WRED for the interface.

Examples

The following example enables flow-based WRED on serial interface 1 and sets the flow threshold constant to 16:

```
interface Serial1
 random-detect
 random-detect flow
 random-detect flow count 16
```

Related Commands

Command	Description
random-detect dscp	Changes the minimum and maximum packet thresholds for the DSCP value.
random-detect exponential-weighting-constant	Configures the WRED and DWRED exponential weight factor for the average queue size calculation.
random-detect flow	Enables flow-based WRED.
random-detect precedence	Configures WRED and DWRED parameters for a particular IP Precedence.
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	Lists all or selected configured queueing strategies.

random-detect-group

To define the Weighted Random Early Detection (WRED) or distributed WRED (DWRED) parameter group, use the **random-detect group** command in global configuration mode. To delete the WRED or DWRED parameter group, use the **no** form of this command.

random-detect-group *group-name* [*dscp-based* | *prec-based*]

no random-detect-group *group-name* [*dscp-based* | *prec-based*]

Syntax Description

group-name	Name for the WRED or DWRED parameter group.
dscp-based	(Optional) Specifies that WRED is to use the differentiated services code point (DSCP) value when it calculates the drop probability for a packet.
prec-based	(Optional) Specifies that WRED is to use the IP Precedence value when it calculates the drop probability for a packet.

Defaults

No WRED or DWRED parameter group exists.

If you choose not to use either the *dscp-based* or the *prec-based* argument, WRED uses the IP Precedence value (the default method) to calculate drop probability for the packet.

Command Modes

Global configuration

Command History

Release	Modification
11.1(22)CC	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T. Arguments were added to support Differentiated Services (DiffServ) and Assured Forwarding (AF) Per Hop Behavior (PHB).

Usage Guidelines

WRED is a congestion avoidance mechanism that slows traffic by randomly dropping packets when there is congestion. DWRED is similar to WRED but uses the Versatile Interface Processor (VIP) instead of the Route Switch Processor (RSP). WRED and DWRED are most useful when the traffic uses protocols such as TCP that respond to dropped packets by decreasing the transmission rate.

The router automatically determines parameters to use in the WRED calculations. If you want to change these parameters for a group, use the **exponential-weighting-constant** or **precedence** command.

Two Methods for Calculating the Drop Probability of a Packet

This command includes two optional arguments, *dscp-based* and *prec-based*, that determine the method WRED uses to calculate the drop probability of a packet.

Note the following points when deciding which method to instruct WRED to use:

- With the *dscp-based* argument, WRED uses the DSCP value (that is, the first six bits of the IP type of service (ToS) byte) to calculate the drop probability.
- With the *prec-based* argument, WRED will use the IP Precedence value to calculate the drop probability.
- The *dscp-based* and *prec-based* arguments are mutually exclusive.
- If neither argument is specified, WRED uses the IP Precedence value to calculate the drop probability (the default method).

Examples

The following example defines the WRED parameter group called sanjose:

```
random-detect-group sanjose
  precedence 0 32 256 100
  precedence 1 64 256 100
  precedence 2 96 256 100
  precedence 3 128 256 100
  precedence 4 160 256 100
  precedence 5 192 256 100
  precedence 6 224 256 100
  precedence 7 256 256 100
```

The following example enables WRED to use the DSCP value 9. The minimum threshold for the DSCP value 9 is 20 and the maximum threshold is 50. This configuration can be attached to other virtual circuits (VCs) as required.

```
Router(config)# random-detect-group sanjose dscp-based
Router(cfg-red-grp)# dscp 9 20 50
Router(config-subif-vc)# random-detect attach sanjose
```

Related Commands

Command	Description
dscp	Changes the minimum and maximum packet thresholds for the DSCP value.
exponential-weighting-constant	Configures the exponential weight factor for the average queue size calculation for a WRED parameter group.
precedence (WRED group)	Configures a WRED group for a particular IP Precedence.
random-detect-group	Defines the WRED or DWRED parameter group.
show queueing	Lists all or selected configured queueing strategies.
show queueing interface	Displays the queueing statistics of an interface or VC.

random-detect precedence

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

random-detect precedence {*precedence* | **rsvp**} *min-threshold max-threshold mark-prob-denominator*

no random-detect precedence {*precedence* | **rsvp**} *min-threshold max-threshold mark-prob-denominator*

Syntax Description

precedence	IP Precedence number. The value range is from 0 to 7. For Cisco 7000 series routers with an RSP7000 interface processor and Cisco 7500 series routers with a VIP2-40 interface processor (VIP2-50 interface processor strongly recommended), the precedence value range is from 0 to 7 only; see Table 14 in the “Usage Guidelines” section of this command.
rsvp	Indicates Resource Reservation Protocol (RSVP) traffic.
min-threshold	Minimum threshold in number of packets. The value range of this argument is from 1 to 4096. When the average queue length reaches the minimum threshold, WRED randomly drops some packets with the specified IP Precedence.
max-threshold	Maximum threshold in number of packets. The value range of this argument is from the value of the *min-threshold* argument to 4096. When the average queue length exceeds the maximum threshold, WRED drops all packets with the specified IP Precedence.
mark-prob-denominator	Denominator for the fraction of packets dropped when the average queue depth is at the maximum threshold. For example, if the denominator is 512, 1 out of every 512 packets is dropped when the average queue is at the maximum threshold. The value range is from 1 to 65536. The default is 10; 1 out of every 10 packets is dropped at the maximum threshold.

Defaults

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

The default *min-threshold* depends on the precedence. The *min-threshold* for IP Precedence 0 corresponds to half of the *max-threshold*. The values for the remaining precedences fall between half the *max-threshold* and the *max-threshold* at evenly spaced intervals. See Table 14 in the “Usage Guidelines” section of this command for a list of the default minimum threshold values for each IP Precedence.

Command Modes

Interface configuration when used on an interface

Policy-map class configuration when used to specify class policy in a policy map

Command History

Release	Modification
11.1 CC	This command was introduced.

Usage Guidelines

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

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

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

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

Table 14 lists the default minimum threshold value for each IP Precedence.

Table 14 Default WRED and DWRED Minimum Threshold Values

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

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

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

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

Note The DWRED feature is not supported in a class policy.

Examples

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

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

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

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

Related Commands

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

rate-limit

To configure committed access rate (CAR) and distributed committed access rate (DCAR) policies, use the **rate-limit** command in interface configuration mode. To remove the rate limit from the configuration, use the **no** form of this command.

rate-limit {**input** | **output**} {*bps* | **access-group** *acl-index* | [**rate-limit**] *rate-limit-acl-index*] | **dscp** *dscp-value* | **qos-group** *qos-group-number*} *burst-normal burst-max* **conform-action** *conform-action* **exceed-action** *exceed-action*

no rate-limit {**input** | **output**} {*bps* | **access-group** *acl-index* | [**rate-limit**] *rate-limit-acl-index*] | **dscp** *dscp-value* | **qos-group** *qos-group-number*} *burst-normal burst-max* **conform-action** *conform-action* **exceed-action** *exceed-action*

Syntax Description

input	Applies this CAR traffic policy to packets received on this input interface.
output	Applies this CAR traffic policy to packets sent on this output interface.
bps	Average rate, in bits per second (bps). The value must be in increments of 8 kbps. The value is a number from 8,000 to 2,000,000,000.
access-group	(Optional) Applies this CAR traffic policy to the specified access list.
acl-index	(Optional) Access list number. Values are numbers from 1 to 2,699.
rate-limit	(Optional) The access list is a rate-limit access list.
rate-limit-acl-index	(Optional) Rate-limit access list number. Values are numbers from 0 to 99.
dscp	(Optional) Allows the rate limit to be applied to any packet matching a specified differentiated services code point (DSCP).
dscp-value	(Optional) The DSCP number. Values are numbers from 0 to 63.
qos-group	(Optional) Allows the rate limit to be applied to any packet matching a specified qos-group number. Values are numbers from 0 to 99.
qos-group-number	(Optional) The qos-group number. Values are numbers from 0 to 99.
burst-normal	Normal burst size, in bytes. The minimum value is bps divided by 2000. The value is a number from 1,000 to 512,000,000.
burst-max	Excess burst size, in bytes. The value is a number from 2,000 to 1,024,000,000.

conform-action *conform-action*	Action to take on packets that conform to the specified rate limit. Specify one of the following keywords: • **continue**—Evaluate the next **rate-limit** command. • **drop**—Drop the packet. • **set-dscp-continue**—Set the differentiated services codepoint (DSCP) (0 to 63) and evaluate the next **rate-limit** command. • **set-dscp-transmit**—Transmit the DSCP and transmit the packet. • **set-mpls-exp-imposition-continue**—Set the Multiprotocol Label Switching (MPLS) experimental bits (0 to 7) during imposition and evaluate the next **rate-limit** command. • **set-mpls-exp-imposition-transmit**—Set the MPLS experimental bits (0 to 7) during imposition and transmit the packet. • **set-prec-continue**—Set the IP precedence (0 to 7) and evaluate the next **rate-limit** command. • **set-prec-transmit**—Set the IP precedence (0 to 7) and transmit the packet. • **set-qos-continue**—Set the quality of service (QoS) group ID (1 to 99) and evaluate the next **rate-limit** command. • **set-qos-transmit**—Set the QoS group ID (1 to 99) and transmit the packet. • **transmit**—Transmit the packet.
exceed-action *exceed-action*	Action to take on packets that exceed the specified rate limit. Specify one of the following keywords: • **continue**—Evaluate the next **rate-limit** command. • **drop**—Drop the packet. • **set-dscp-continue**—Set the DSCP (0 to 63) and evaluate the next **rate-limit** command. • **set-dscp-transmit**—Transmit the DSCP and transmit the packet. • **set-mpls-exp-imposition-continue**—Set the MPLS experimental bits (0 to 7) during imposition and evaluate the next **rate-limit** command. • **set-mpls-exp-imposition-transmit**—Set the MPLS experimental bits (0 to 7) during imposition and transmit the packet. • **set-prec-continue**—Set the IP precedence (0 to 7) and evaluate the next **rate-limit** command. • **set-prec-transmit**—Set the IP precedence (0 to 7) and transmit the packet. • **set-qos-continue**—Set the QoS group ID (1 to 99) and evaluate the next **rate-limit** command. • **set-qos-transmit**—Set the QoS group ID (1 to 99) and transmit the packet. • **transmit**—Transmit the packet.

Defaults

CAR and DCAR are disabled.

Command Modes

Interface configuration

Command History

Release	Modification
11.1 CC	This command was introduced.
12.1(5)T	This command now includes **conform** and **exceed** actions for the MPLS experimental field.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(4)T	This command was implemented on the Cisco MGX 8850 switch and the MGX 8950 switch with a Cisco MGX RPM-PR card.
12.2(4)T2	This command was implemented on the Cisco 7500 series.

Usage Guidelines

Use this command to configure your CAR policy on an interface. To specify multiple policies, enter this command once for each policy.

CAR and DCAR can be configured on an interface or subinterface.

Policing Traffic with CAR

CAR embodies a rate-limiting feature for policing traffic. When policing traffic with CAR, Cisco recommends the following values for the normal and extended burst parameters:

```
normal burst = configured rate * (1 byte)/(8 bits) * 1.5 seconds
extended burst = 2 * normal burst
```

With the listed choices for parameters, extensive test results have shown CAR to achieve the configured rate. If the burst values are too low, then the achieved rate is often much lower than the configured rate.

For more information about using CAR to police traffic, see the "Policing with CAR" section of the "Policing and Shaping Overview" in the *Cisco IOS Quality of Service Configuration Guide*, Release 12.2.

Examples

In the following example, the rate is limited by the application in question:

- All World Wide Web traffic is transmitted. However, the MPLS experimental field for web traffic that conforms to the first rate policy is set to 5. For nonconforming traffic, the IP precedence is set to 0 (best effort). See the following commands in the example:

```
rate-limit input rate-limit access-group 101 20000000 24000 32000 conform-action
set-mpls-exp-transmit 5 exceed-action set-mpls-exp-transmit 0
access-list 101 permit tcp any any eq www
```

- FTP traffic is transmitted with an MPLS experimental field value of 5 if it conforms to the second rate policy. If the FTP traffic exceeds the rate policy, it is dropped. See the following commands in the example:

```
rate-limit input access-group 102 10000000 24000 32000
conform-action set-mpls-exp-transmit 5 exceed-action drop
access-list 102 permit tcp any any eq ftp
```

- Any remaining traffic is limited to 8 Mbps, with a normal burst size of 16000 bytes and an excess burst size of 24000 bytes. Traffic that conforms is transmitted with an MPLS experimental field value of 5. Traffic that does not conform is dropped. See the following command in the example:

  ```
  rate-limit input 8000000 16000 24000 conform-action set-mpls-exp-transmit 5
  exceed-action drop
  ```

Notice that two access lists are created to classify the web and FTP traffic so that they can be handled separately by the CAR feature.

```
Router(config)# interface Hssi0/0/0
Router(config-if)# description 45Mbps to R2
Router(config-if)# rate-limit input rate-limit access-group 101 20000000 24000 32000
  conform-action set-mpls-exp-transmit 5 exceed-action set-mpls-exp-transmit 0
Router(config-if)# rate-limit input access-group 102 10000000 24000 32000
  conform-action set-mpls-exp-transmit 5 exceed-action drop
Router(config-if)# rate-limit input 8000000 16000 24000 conform-action
  set-mpls-exp-transmit 5 exceed-action drop
Router(config-if)# ip address 200.200.14.250 255.255.255.252
!
Router(config-if)# access-list 101 permit tcp any any eq www
Router(config-if)# access-list 102 permit tcp any any eq ftp
```

In the following example, the MPLS experimental field is set, and the packet is transmitted:

```
Router(config)# interface FastEtheret1/1/0
Router(config-if)# rate-limit input 8000 1000 1000 access-group conform-action
  set mpls-exp-transmit 5 exceed-action set-mpls-exp-transmit 5
```

In the following example, any packet with a DSCP of 1 can apply the rate limit:

```
Router(config)# interface pos6/1/0
Router(config-if)# rate-limit output dscp 1 8000 1000 1000 conform-action transmit
  exceed-action drop
```

Related Commands

Command	Description
access-list rate-limit	Configures an access list for use with CAR policies.
show access-lists rate-limit	Displays information about rate-limit access lists.
show interfaces rate-limit	Displays information about CAR for a specified interface.

send qdm message

To send a text message to all Quality Device Manager (QDM) clients, use the **send qdm message** command in EXEC mode.

send qdm [**client** *client-id*] **message** *message-text*

Syntax Description

client	(Optional) Specifies a QDM client to receive the message.
client-id	(Optional) Specifies the QDM identification of the client that will receive the text message.
message	Specifies that a message will be sent.
message-text	The actual text of the message.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 12.1(1)E	This command was introduced.
Release 12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.

Usage Guidelines

Use the **send qdm** [**client** *client-id*] **message** *message-text* command to send a message to a specific QDM client. For example, entering the **send qdm client 9 message hello** command will send the message “hello” to client ID 9.

Use the **send qdm message** *message-text* command to send a message to all QDM clients. For example, entering the **send qdm message hello** command sends the message “hello” to all open QDM clients.

Examples

The following example sends the text message “how are you?” to client ID 12:

```
send qdm client 12 message how are you?
```

The following example sends the text message “how is everybody?” to all QDM clients connected to the router:

```
send qdm message how is everybody?
```

Related Commands

Command	Description
show qdm status	Displays the status of connected QDM clients.

service-policy

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

service-policy {**input** | **output**} *policy-map-name*

no service-policy {**input** | **output**} *policy-map-name*

Syntax Description

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.

Defaults

No service policy is specified.

Command Modes

Interface configuration

VC submode (for a standalone VC)

Bundle-vc configuration (for ATM VC bundle members)

Map-class configuration (for Frame Relay VCs)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(5)XE	This command was integrated into Cisco IOS Release 12.0(5)XE.
12.0(7)S	This command was integrated into Cisco IOS Release 12.0(7)S.
12.1(1)E	This command was integrated into Cisco IOS Release 12.1(1)E.
12.1(2)T	This command was integrated into Cisco IOS Release 12.l(2)T. This command was modified to enable low latency queueing (LLQ) on Frame Relay VCs.

Usage Guidelines

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

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

To successfully attach a policy map to an interface or a VC, the aggregate of the configured minimum bandwidths of the classes comprising the policy map must be less than or equal to 75 percent of the interface bandwidth or the bandwidth allocated to the VC.

To enable 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 will then attach an output service policy to the Frame Relay VC using the **service-policy** command in map-class configuration mode.

For a policy map to be successfully attached 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** map-class commands. If not configured, the minimum CIR defaults to half of the CIR.

Configuring CBWFQ on a physical interface is only possible if the interface is in the default queueing mode. Serial interfaces at E1 (2.048 Mbps) and below use WFQ by default. Other interfaces use 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.

Attaching a service policy and enabling CBWFQ on an interface renders ineffective any commands related to fancy queueing such as commands pertaining to fair queueing, custom queueing, priority queueing, and Weighted Random Early Detection (WRED). You can configure these features only after you remove the policy map from the interface.

You can modify a policy map attached to an interface or a VC, changing the bandwidth of any of the classes comprising the map. Bandwidth changes that you make to an attached policy map are effective only if the aggregate of the bandwidth amounts for all classes comprising the policy map, including the modified class bandwidth, 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.

Examples

The following example shows how to attache the service policy map called policy9 to data-link connection identifier (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 attaches the service policy map called policy9 to input serial interface 1:

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

The following example attaches the service policy map called policy9 to the input PVC called cisco:

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

The following example attaches the policy called 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 called policy9 to the output PVC called cisco:

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

Related Commands

Command	Description
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
show frame-relay pvc	Displays statistics about PVCs for Frame Relay interfaces.
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.

service-policy (class-map)

To attach a policy map to a class, use the **service-policy** command in class-map configuration mode. To remove a service policy from a class, use the **no** form of this command.

service-policy *policy-map*

no service-policy

Syntax Description

policy-map	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.

Defaults

No service policy is specified.

Command Modes

Class-map configuration

Command History

Release	Modification
12.1(2)T	This command was introduced.

Usage Guidelines

You can attach a single policy map to one or more classes to specify the service policy for those classes. This command is only available for the output interface, which is assumed.

Examples

In the following example, three policy maps are defined—cust1-classes, cust2-classes, and cust-policy. The policy maps cust1-classes and cust2-classes have three classes defined—gold, silver, and bronze.

For cust1-classes, gold is configured to use 50 percent of the bandwidth. Silver is configured to use 20 percent of the bandwidth, and bronze is configured to use 15 percent of the bandwidth.

For cust2-classes, gold is configured to use 30 percent of the bandwidth. Silver is configured to use 15 percent of the bandwidth, and bronze is configured to use 10 percent of the bandwidth.

The policy map cust-policy specifies average rate shaping of 384 kbps and assigns the service policy called cust1-classes to the policy map called cust1-classes. The policy map called cust-policy specifies peak rate shaping of 512 kbps and assigns the service policy called cust2-classes to the policy map called cust2-classes.

To configure classes for cust1-classes, use the following commands:

```
Router(config)# policy-map cust1-classes
Router(config-pmap)# class gold
Router(config-pmap-c)# bandwidth percent 50
Router(config-pmap)# class silver
Router(config-pmap-c)# bandwidth percent 20
Router(config-pmap)# class bronze
Router(config-pmap-c)# bandwidth percent 15
```

To configure classes for cust2, use the following commands:

```
Router(config)# policy-map cust2-classes
Router(config-pmap)# class gold
Router(config-pmap-c)# bandwidth percent 30
Router(config-pmap)# class silver
Router(config-pmap-c)# bandwidth percent 15
Router(config-pmap)# class bronze
Router(config-pmap-c)# bandwidth percent 10
```

To define the customer policy with cust1-classes and cust2-classes and QoS features, use the following commands:

```
Router(config)# policy-map cust-policy
Router(config-pmap)# class cust1
Router(config-pmap-c)# shape average 38400
Router(config-pmap-c)# service-policy cust1-classes
Router(config-pmap)# class cust2
Router(config-pmap-c)# shape peak 51200
Router(config-pmap-c)# service-policy cust2-classes
Router(config-pmap-c)# interface Serial 3/2
Router(config-if)# service out cust-policy
```

Related Commands

Command	Description
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
show policy-map	Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps.

service-policy (policy-map class)

To use a service policy as a QoS policy within a policy map (called a hierarchical service policy), use the **service-policy** command in policy-map class configuration mode. To disable a particular service policy as a QoS policy within a policy map, use the **no** form of this command.

service-policy *policy-map-name*

no service-policy *policy-map-name*

Syntax Description

policy-map-name	Specifies the name of the predefined policy map to be used as a QoS policy. The name can be a maximum of 40 alphanumeric characters.

Defaults

No default behavior or values

Command Modes

Policy-map class configuration

Command History

Release	Modification
12.1(2)E	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.

Usage Guidelines

This command is used to create hierarchical service policies in policy-map class configuration mode.

This command is different from the **service-policy** [**input | output**] *policy-map-name* command used in interface configuration mode. The purpose of the **service-policy** [**input | output**] *policy-map-name* is to attach service policies to interfaces.

The child policy is the previously defined service policy that is being associated with the new service policy through the use of the **service-policy** command. The new service policy using the preexisting service policy is the parent policy.

This command has the following restrictions:

- The **set** command is not supported on the child policy.
- The **priority** command can be used in either the parent or the child policy, but not *both* policies simultaneously.
- The **shape** command can be used in either the parent or the child policy, but not *both* polices simultaneously on a subinterface.
- The **fair-queue** command cannot be defined in the parent policy.
- If the **bandwidth** command is used in the child policy, the **bandwidth** command must also be used in the parent policy. The one exception is for policies using the default class.

Examples

The following example creates a hierarchical service policy in the service policy called parent:

```
Router(config)# policy-map child
Router(config-pmap)# class voice
Router(config-pmap-c)# priority 50

Router(config)# policy-map parent
Router(config-pmap)# class class-default
Router(config-pmap-c)# shape average 10000000
Router(config-pmap-c)# service-policy child
```

FRF.11 and FRF.12 configurations on a Versatile Interface Processor (VIP)-enabled Cisco 7500 series router often require a hierarchical service policy for configuration. A hierarchical service policy for FRF.11 and FRF.12 requires the following elements:

1. A traffic class that uses the Voice over Frame Relay (VoFR) protocol as the only match criterion.
2. A traffic policy that insures low latency queueing (LLQ), which is achieved using the **priority** command, for all VoFR protocol traffic
3. A traffic policy that defines the shaping parameters and includes the elements listed in element 2.

   Element 3 can only be fulfilled through the use of a hierarchical service policy, which is configured using the **service-policy** command.

In the following example, element 1 is configured in the traffic class called frf, element 2 is configured in the traffic policy called llq, and element 3 is configured in the traffic policy called llq-shape.

```
Router(config)# class-map frf
Router(config-cmap)# match protocol vofr
Router(config-cmap)# exit
Router(config)# policy-map llq
Router(config-pmap)# class frf
Router(config-pmap-c)# priority 2000
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# policy-map llq-shape
Router(config-pmap)# class class-default
Router(config-pmap-c)# shape average 1000 128000
Router(config-pmap-c)# service-policy llq
```

The final step in using a hierarchical service policy for FRF.11 and FRF.12 is using the service policy in map-class configuration mode. In the following example, the traffic policy called llq-shape is attached to the map class called frag:

```
Router(config)# map-class frame-relay frag
Router(config-map-class)# frame-relay fragment 40
Router(config-map-class)# service-policy llq-shape
```

Related Commands

Command	Description
bandwidth (policy-map class)	Specifies or modifies the bandwidth allocated for a class belonging to a policy map.
fair-queue	Specifies the number of queues to be reserved for use by a traffic class.
policy-map	Specifies the name of the service policy to configure.
priority	Gives priority to a class of traffic belonging to a policy map.
service-policy	Specifies the name of the service policy to be attached to the interface.
shape	Specifies average or peak rate traffic shaping.
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.

set atm-clp

To set the cell loss priority (CLP) bit when a policy map is configured, use the **set atm-clp** command in policy-map class configuration mode. To remove a specific CLP bit setting, use the **no** form of this command.

set atm-clp

Syntax Description

This command has no arguments or keywords.

Defaults

The CLP bit is automatically set to 0 when Cisco routers convert IP packets into ATM cells for transmission through Multiprotocol Label Switching (MPLS)-aware ATM networks.

Command Modes

Policy-map class configuration

Command History

Release	Modification
12.1(5)T	This command was introduced.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(4)T	This command was implemented on the Cisco MGX 8850 switch and the MGX 8950 switch with a Cisco MGX RPM-PR card.
12.2(4)T2	This command was implemented on the Cisco 7500 series.

Usage Guidelines

To disable this command, remove the service policy from the interface.

To use the **set atm-clp** command, you must have one of the following adapters: the Enhanced ATM Port Adapter (PA-A3), the ATM Inverse Multiplexer over ATM Port Adapter with 8 T1 Ports (PA-A3-8T1IMA), or the ATM Inverse Multiplexer over ATM Port Adapter with 8 E1 Ports (PA-A3-8E1IMA). Therefore, the **set atm-clp** command is not supported on any platform that does not support these adapters. For more information, refer to the documentation for your specific router.

A policy map containing the **set atm-clp** command can be attached as an output policy only. The **set atm-clp** command does not support packets that originate from the router.

Examples

The following example illustrates setting the CLP bit using the **set atm-clp** command in the policy map:

```
Router(config)# class-map ip-precedence
Router(config-cmap)# match ip precedence 0 1
Router(config-cmap)# exit
Router(config)# policy-map atm-clp-set
Router(config-pmap)# class ip-precedence
Router(config-pmap-c)# set atm-clp
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface atm 1/0/0.1
Router(config-if)# service-policy output bear
```

Related Commands

Command	Description
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
show atm pvc	Displays all ATM PVCs and traffic information.
show policy-map	Displays information about the policy map for an interface.

set cos

To set the Layer 2 class of service (CoS) value of an outgoing packet, use the **set cos** 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*]}

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) Used in conjunction with the *from-field* argument. Indicates that the values set in a specified table map will be used to set the CoS value.
table-map-name	(Optional) Used in conjunction with the **table** keyword. Name of the table map used to specify the CoS value. The table map name can be a maximum of 64 alphanumeric characters.

Defaults

Disabled

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 the Enhanced Packet Marking feature. A mapping table (table map) can now be used to convert and propagate packet-marking values.

Usage Guidelines

CoS packet marking is supported only in the Cisco Express Forwarding (CEF)-switching path.

The **set cos** 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 **set cos** 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 **match cos** and **set cos** 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

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 CoS value. The "from-field" packet-marking categories are as follows:

- Precedence
- Differentiated services code point (DSCP)

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

Note If you configure the **set cos dscp** 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 CoSs 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)# exit
Router(config-pmap)# exit
```

Enhanced Packet Marking Example

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)# exit
```

Note The **set cos** command is applied when you create a service policy in 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*, Release 12.2.

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 discard-class

To mark a packet with a discard-class value, use the **set discard-class** command in policy-map configuration mode. To prevent the discard-class value of a packet from being altered, use the **no** form of this command.

set discard-class *value*

no set discard-class *value*

Syntax Description

value	Per-hop behavior (PHB) for dropping traffic. The priority of a type of traffic. Valid values are numbers from 0 to 7.

Defaults

If you do not enter this command, the packet has a discard-class value of zero.

Command Modes

Policy-map configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

Discard-class indicates the discard portion of the PHB. Use the **set discard-class** command only in Pipe mode. Discard-class is required when the input PHB marking will be used to classify packets on the output interface.

You can also use this command to specify the type of traffic that will be dropped when there is congestion.

Examples

The following example shows that traffic will be set to the discard-class value of 2:

```
set discard-class 2
```

Related Commands

Command	Description
match discard-class	Matches packets of a certain discard class.
random-detect discard-class-based	Bases WRED on the discard class value of a packet.

set dscp

To mark a packet by setting the differentiated services code point (DSCP) value in the type of service (ToS) byte, use the **set dscp** command in policy-map class configuration mode. To remove a previously set DSCP value, use the **no** form of this command.

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

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

Syntax Description

ip	(Optional) Specifies that the match is for IPv4 packets only. If not used, the match is on both IPv4 and IPv6 packets.
dscp-value	A number from 0 to 63 that sets the DSCP value. The following reserved keywords can be specified instead of numeric values: • **EF** (expedited forwarding) • **AF11** (assured forwarding class AF11) • **AF12** (assured forwarding class AF12)
from-field	Specific packet-marking category to be used to set the DSCP 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** • **qos-group**
table	(Optional) Used in conjunction with the *from-field* argument. Indicates that the values set in a specified table map will be used to set the DSCP value.
table-map-name	(Optional) Used in conjunction with the **table** keyword. Name of the table map used to specify the DSCP value. The name can be a maximum of 64 alphanumeric characters.

Defaults

No default behavior or values

Command Modes

Policy-map class configuration

Command History

Release	Modification
12.2(13)T	This command was introduced. This command replaces the **set ip dscp** command.

Usage Guidelines

After the DSCP bit is set, other quality of service (QoS) features can then operate on the bit settings.

The **set dscp** command cannot be used with the **set precedence** command to mark the *same* packet. The two values, DSCP and precedence, are mutually exclusive. A packet can have one value or the other, but not both.

The network gives priority (or some type of expedited handling) to marked traffic. Typically, you set the precedence value at the edge of the network (or administrative domain); data then is queued according to the precedence. Weighted fair queueing (WFQ) can speed up handling for high-precedence traffic at congestion points. Weighted Random Early Detection (WRED) ensures that high-precedence traffic has lower loss rates than other traffic during times of congestion.

The value of the *dscp-valu*e argument can be specified by the reserved keywords **EF**, **AF11**, and **AF12** instead of numeric values.

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 DSCP value. The "from-field" packet-marking categories are as follows:

- Class of service (CoS)
- QoS group

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 DSCP value. For instance, if you configure the **set dscp cos** command, the CoS value will be copied and used as the DSCP value.

Note The CoS field is a three-bit field, and the DSCP field is a six-bit field. If you configure the **set dscp cos** command, only the three bits of the CoS field will be used.

If you configure the **set dscp qos-group** command, the QoS group value will be copied and used as the DSCP value.

The valid value range for the DSCP is a number from 0 to 63. The valid value range for the QoS group is a number from 0 to 99. Therefore, when configuring the **set dscp qos-group** command, note the following points:

- If a QoS group value falls within both value ranges (for example, 44), the packet-marking value will be copied and the packets will be marked.
- If QoS group value exceeds the DSCP range (for example, 77), the packet-marking value will not be copied and the packet will not be marked. No action is taken.

Setting DSCP Values for IPv6 Packets Only

To set the DSCP values for IPv6 values only, the **match protocol ipv6** command must also be used. Without the **match protocol ipv6** command, the match defaults to match both IPv4 and IPv6 packets.

Setting DSCP Values for IPv4 Packets Only

To set the DSCP values for IPv4 packets only, use the **ip** keyword. Without the **ip** keyword the match occurs on both IPv4 and IPv6 packets.

Examples

In the following example, the policy map called "policy1" is created to use the packet-marking values defined in a table map called "table-map1". The table map 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 DSCP value will be set according to the CoS value defined in the table map called "table-map1".

```
Router(config)# policy-map policy1
Router(config-pmap)# class class-default
Router(config-pmap-c)# set dscp cos table table-map1
Router(config-pmap-c)# exit
```

Note The **set dscp** command is applied when you create a service policy in QoS policy-map configuration mode. This service policy is not yet attached to an interface. For information on attaching a service policy to an interface, refer to the "Modular Quality of Service Command-Line Interface Overview" chapter of the *Cisco IOS Quality of Service Solutions Configuration Guide,* Release 12.2.

Related Commands

Command	Description
match protocol	Configures the match criteria for a class map on the basis of the specified protocol.
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
service-policy	Attaches a policy map to an input interface or VC, or an output interface or VC, to be used as the service policy for that interface or VC.
set cos	Sets the Layer 2 CoS value of an outgoing packet.
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.
show table-map	Displays the configuration of a specified table map or all table maps.
table-map (value mapping)	Creates and configures a mapping table for mapping and converting one packet-marking value to another.

set fr-de

To change the discard eligible (DE) bit setting in the address field of a Frame Relay frame to 1 for all traffic leaving an interface, use the **set fr-de** command in policy-map class command. To remove the DE bit setting, use the **no** form of this command.

set fr-de

no set fr-de

Syntax Description

This command has no arguments or keywords.

Defaults

The DE bit is usually set to 0. This command changes the DE bit setting to 1.

Command Modes

Policy-map class

Command History

Release	Modification
12.2(2)T	This command was introduced.

Usage Guidelines

To disable this command in a traffic policy, use the **no set fr-de** command in policy-map class configuration mode of the traffic policy.

If the DE bit is already set to 1, no changes will be made to the frame.

Examples

The following example illustrates a DE bit that was set using the **set fr-de** command in the traffic policy:

```
Router(config)# class-map ip-precedenc
Router(config-cmap)# match ip precedence 0 1
Router(config-cmap)# exit
Router(config)# policy-map atm-clp-set
Router(config-pmap)# class ip-precedence
Router(config-pmap-c)# set fr-de
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface atm 1/0/0
Router(config)# service-policy output bear
```

Related Commands

Command	Description
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
show policy-map	Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps.

set ip dscp

> **Note** Effective with Release 12.2(13)T, the **set ip dscp** command is replaced by the **set dscp** command. See the **set dscp** command for more information.

To mark a packet by setting the IP differentiated services code point (DSCP) in the type of service (ToS) byte, use the **set ip dscp** QoS policy-map configuration command. To remove a previously set IP DSCP, use the **no** form of this command.

set ip dscp *ip-dscp-value*

no set ip dscp *ip-dscp-value*

Syntax Description

ip-dscp-value	A number from 0 to 63 that sets the IP DSCP value. Reserved keywords **EF** (expedited forwarding), **AF11** (assured forwarding class AF11), and **AF12** (assured forwarding class AF12) can be specified instead of numeric values.

Defaults

This command has no default behavior or values.

Command Modes

QoS policy-map configuration

Command History

Release	Modification
12.0(5)XE	This command was introduced.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T. This command was enhanced to include reserved keywords **EF**, **AF11**, and **AF12** instead of numeric values.
12.2(13)T	This command was replaced by the **set dscp** command.

Usage Guidelines

Once the IP DSCP bit is set, other QoS services can then operate on the bit settings.

You cannot mark a packet by the IP precedence with the **set ip precedence** command and mark the same packet with an IP DSCP value by entering the **set ip dscp** command.

The network gives priority (or some type of expedited handling) to marked traffic. Typically, you set IP precedence at the edge of the network (or administrative domain); data then is queued based on the precedence. Weighted fair queueing (WFQ) can speed up handling for high-precedence traffic at congestion points. Weighted Random Early Detection (WRED) ensures that high-precedence traffic has lower loss rates than other traffic during times of congestion.

Reserved keywords **EF**, **AF11**, and **AF12** can be specified instead of numeric values.

Examples

In the following example, the IP DSCP ToS byte is set to 8 in the policy map called policy1:

```
Router(config)# policy-map policy1
Router(config-pmap)# class class1
Router(config-pmap-c)# set ip dscp 8
```

All packets that satisfy the match criteria of class1 are marked with the IP DSCP value of 8. How packets marked with the IP DSCP value of 8 are treated is determined by the network configuration.

After you configure the settings shown for voice packets at the edge, all intermediate routers are then configured to provide low latency treatment to the voice packets, as follows:

```
Router(config)# class-map voice
Router(config-cmap)# match ip dscp ef
Router(config)# policy qos-policy
Router(config-pmap)# class voice
Router(config-pmap-c)# priority 24
```

The **set ip dscp** command is applied when you create a service policy in QoS policy-map configuration mode. This service policy is not yet attached to an interface. For information on attaching a service policy to an interface, refer to the "Modular Quality of Service Command-Line Interface" chapter of the *Cisco IOS Quality of Service Solutions Configuration Guide*.

Related Commands

Command	Description
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
service-policy	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 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 ip precedence (policy-map)

Note Effective with Release 12.2(13)T, the **set ip precedence** (policy-map) command is replaced by the **set precedence** command. See the **set precedence** command for more information.

To set the precedence value in the IP header, use the **set ip precedence** QoS policy-map configuration command. To leave the precedence value at the current setting, use the **no** form of this command.

set ip precedence *ip-precedence-value*

no set ip precedence

Syntax Description

ip-precedence-value	A number from 0 to 7 that sets the precedence bit in the IP header.

Defaults

This command is disabled by default.

Command Modes

QoS policy-map configuration

Command History

Release	Modification
11.0	This command was introduced.
12.0(5)XE	This command was integrated into Cisco IOS Release 12.0(5)XE. This command was introduced in the Modular Quality of Service Command-Line Interface (MQC) feature.
12.2(13)T	This command was replaced by the **set precedence** command.

Usage Guidelines

Once the IP precedence bits are set, other QoS services such as weighted fair queueing (WFQ) and Weighted Random Early Detection (WRED) then operate on the bit settings.

The network gives priority (or some type of expedited handling) to marked traffic through the application of WFQ or WRED at points downstream in the network. Typically, you set IP Precedence at the edge of the network (or administrative domain); data then is queued based on the precedence. WFQ can speed up handling for certain precedence traffic at congestion points. WRED can ensure that certain precedence traffic has lower loss rates than other traffic during times of congestion.

Examples

The following example sets the IP Precedence to 5 for packets that satisfy the match criteria of the class map called class1:

```
Router(config)# policy-map policy1
Router(config-pmap)# class class1
Router(config-pmap-c)# set ip precedence 5
```

All packets that satisfy the match criteria of class1 are marked with the IP Precedence value of 5. How packets marked with the IP Precedence value of 5 are treated is determined by the network configuration.

The **set ip precedence** command is applied when you create a service policy in QoS policy-map configuration mode. This service policy is not yet attached to an interface or to an ATM virtual circuit. For information on attaching a service policy to an interface, refer to the "Modular Quality of Service Command-Line Interface" chapter of the *Cisco IOS Quality of Service Solutions Configuration Guide*.

Related Commands

Command	Description
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
service-policy	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 for 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 ip precedence (route-map)

To set the precedence value (and an optional IP number or IP name) in the IP header, use the **set ip precedence** command in route-map configuration mode. To leave the precedence value unchanged, use the **no** form of this command.

set ip precedence [*number* | *name*]

no set ip precedence

Syntax Description

number | *name*	(Optional) A number or name that sets the precedence bits in the IP header. The values for the *number* argument and the corresponding *name* argument are listed in Table 15 from least to most important.

Defaults

Disabled

Command Modes

Route-map configuration

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

Table 15 lists the values for the *number* argument and the corresponding *name* argument for precedence values in the IP header. They are listed from least to most important.

Table 15 Number and Name Values for IP Precedence

Number	Name
0	**routine**
1	**priority**
2	**immediate**
3	**flash**
4	**flash-override**
5	**critical**
6	**internet**
7	**network**

You can set the precedence using either a number or the corresponding name. Once the IP Precedence bits are set, other QoS services such as weighted fair queueing (WFQ) and Weighted Random Early Detection (WRED) then operate on the bit settings.

The network gives priority (or some type of expedited handling) to marked traffic through the application of WFQ or WRED at points downstream in the network. Typically, you set IP Precedence at the edge of the network (or administrative domain); data then is queued based on the precedence. WFQ can speed up handling for certain precedence traffic at congestion points. WRED can ensure that certain precedence traffic has lower loss rates than other traffic during times of congestion.

The mapping from arguments such as **routine** and **priority** to a precedence value is useful only in some instances. That is, the use of the precedence bit is evolving. You can define the meaning of a precedence value by enabling other features that use the value. In the case of the high-end Internet QoS available from Cisco, IP Precedences can be used to establish classes of service that do not necessarily correspond numerically to better or worse handling in the network.

Use the **route-map** (IP) global configuration command with the **match** and **set** route-map configuration commands to define the conditions for redistributing routes from one routing protocol into another, or for policy routing. Each **route-map** command has an associated list of **match** and **set** commands. The **match** commands specify the match criteria—the conditions under which redistribution or policy routing is allowed for the current **route-map** command. The **set** commands specify the set actions—the particular redistribution or policy routing actions to perform if the criteria enforced by the **match** commands are met. The **no route-map** command deletes the route map.

The **set** route-map configuration commands specify the redistribution set actions to be performed when all of the match criteria of a route map are met.

Examples

The following example sets the IP Precedence to 5 (critical) for packets that pass the route map match:

```
interface serial 0
 ip policy route-map texas

route-map texas
match length 68 128
set ip precedence 5
```

Related Commands

Command	Description
fair-queue (WFQ)	Enables WFQ for an interface.
ip policy route-map	Identifies a route map to use for policy routing on an interface.
random-detect dscp	Changes the minimum and maximum packet thresholds for the DSCP value.
rate-limit	Configures CAR and DCAR policies.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
traffic-shape adaptive	Configures a Frame Relay subinterface to estimate the available bandwidth when BECN signals are received.
traffic-shape fecn-adapt	Replies to messages with the FECN bit (which are set with TEST RESPONSE messages with the BECN bit set).
traffic-shape group	Enables traffic shaping based on a specific access list for outbound traffic on an interface.
traffic-shape rate	Enables traffic shaping for outbound traffic on an interface.

set precedence

To set the precedence value in the packet header, use the **set precedence** command in policy-map class configuration mode. To remove the precedence value, use the **no** form of this command.

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

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

Syntax Description

precedence-value	A number from 0 to 7 that sets the precedence bit in the packet header.
from-field	Specific packet-marking category to be used to set the precedence 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** • **qos-group**
table	(Optional) Used in conjunction with the *from-field* argument. Indicates that the values set in a specified table map will be used to set the precedence value.
table-map-name	(Optional) Used in conjunction with the **table** keyword. Name of the table map used to specify a precedence value based on the class of service (CoS) value. The name can be a maximum of 64 alphanumeric characters.

Defaults

Disabled

Command Modes

Policy-map class configuration

Command History

Release	Modification
12.2(13)T	This command was introduced. This command replaces the **set ip precedence** command.

Usage Guidelines

Command Compatibility

If a router is loaded with an image from this version (that is, Cisco IOS Release 12.2(13)T) that contained an old configuration, the **set ip precedence** command is still recognized. However, the **set precedence** command will be used in place of the **set ip precedence** command.

The **set precedence** command cannot be used with the **set dscp** command to mark the *same* packet. The two values, DSCP and precedence, are mutually exclusive. A packet can one value or the other, but not both.

Bit Settings

After the precedence bits are set, other quality of service (QoS) features such as weighted fair queueing (WFQ) and Weighted Random Early Detection (WRED) then operate on the bit settings.

Precedence Value

The network gives priority (or some type of expedited handling) to marked traffic through the application of WFQ or WRED at points downstream in the network. Typically, you set the precedence value at the edge of the network (or administrative domain); data then is queued according to the specified precedence. WFQ can speed up handling for certain precedence traffic at congestion points. WRED can ensure that certain precedence traffic has lower loss rates than other traffic during times of congestion.

The **set precedence** command cannot be used with the **set dscp** command to mark the *same* packet. The two values, differentiated services code point (DSCP) and precedence, are mutually exclusive. A packet can have one value or the other, but not both.

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. The "from-field" packet-marking categories are as follows:

- CoS
- QoS group

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 precedence value. For instance, if you configure the **set precedence cos** command, the CoS value will be copied and used as the precedence value.

You can do the same for the QoS group-marking category. That is, you can configure the **set precedence qos-group** command, and the QoS group value will be copied and used as the precedence value.

The valid value range for the precedence value is a number from 0 to 7. The valid value range for the QoS group is a number from 0 to 99. Therefore, when configuring the **set precedence qos-group** command, note the following points:

- If a QoS group value falls within both value ranges (for example, 6), the packet-marking value will be copied and the packets will be marked.
- If QoS group value exceeds the precedence range (for example, 10), the packet-marking value will not be copied, and the packet will not be marked. No action is taken.

Setting Precedence Values for IPv6 Packets Only

To set the precedence values for IPv6 packets only, the **match protocol ipv6** command must also be used in the class-map that classified packets for this action. Without the **match protocol ipv6** command, the class-map may classify both IPv6 and IPv4 packets, (depending on other match criteria) and the **set precedence** command will act upon both types of packets.

Setting Precedence Values for IPv4 Packets Only

To set the precedence values for IPv4 packets only, use a command involving the **ip** keyword like the **match ip precedence** command or include the **match protocol ip** command along with the others in the class map. Without the additional **ip** keyword, the class-map may match both IPv6 and IPv4 packets (depending on the other match criteria) and the **set precedence** command may act upon both types of packets.

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-map-1" 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 precedence value will be set according to the CoS value defined in "table-map1".

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

Note The **set precedence** command is applied when you create a service policy in QoS policy-map configuration mode. This service policy is not yet attached to an interface or to an ATM virtual circuit. For information on attaching a service policy to an interface, refer to the "Modular Quality of Service Command-Line Interface Overview" chapter of the *Cisco IOS Quality of Service Solutions Configuration Guide,* Release 12.2.

Related Commands

Command	Description
match precedence	Identifies IP precedence values as match criteria.
match protocol	Configures the match criteria for a class map on the basis of the specified protocol.
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
service-policy	Attaches a policy map to an input interface or VC, or an output interface or VC, to be used as the service policy for that interface or VC.
set cos	Sets the Layer 2 CoS value of an outgoing packet.
set dscp	Marks a packet by setting the Layer 3 DSCP value in the ToS byte.
set qos-group	Sets a group ID that can be used later to classify packets.
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 for 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 table-map	Displays the configuration of a specified table map or all table maps.
table-map (value mapping)	Creates and configures a mapping table for mapping and converting one packet-marking value to another.

set qos-group

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

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

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

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: • **precedence** • **dscp** • **mpls exp topmost**
table	(Optional) Used in conjunction with the *from-field* argument. Indicates that the values set in a specified table map will be used to set the QoS group value.
table-map-name	(Optional) Used in conjunction with the **table** keyword. Name of the table map used to specify the QoS group value.

Defaults

Disabled

No group ID is specified.

Command Modes

Policy-map class configuration

Command History

Release	Modification
11.1 CC	This command was introduced.
12.0(5)XE	This command was integrated into Cisco IOS Release 12.0(5)XE. This command was included in the Modular Quality of Service Command-Line Interface (MQC) feature.
12.2(13)T	This command can be used with the **random-detect discard-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.

Usage Guidelines

The **set qos-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. The "from-field" packet-marking categories are as follows:

- Precedence
- Differentiated services code point (DSCP)
- Multiprotocol Label Switching (MPLS) Experimental (EXP) topmost

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 configure the **set qos-group precedence** command, the precedence value will be copied and used as the QoS group value.

Examples

The following example sets the QoS group to 1 for all packets that match the class map called "class1". 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
```

Enhanced Packet Marking Example

The following example sets 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)# exit
```

Note The **set qos-group** command is applied when 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*, Release 12.2.

Related Commands

Command	Description
match qos-group	Identifies a specified QoS group value as a match criterion.
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.

shape

To specify average or peak rate traffic shaping, use the **shape** command in class-map configuration mode. To remove traffic shaping, use the **no** form of this command.

shape {**average** | **peak**} *cir* [*bc*] [*be*]

no shape {**average** | **peak**} *cir* [*bc*] [*be*]

Syntax Description

average	Specifies average rate shaping.
peak	Specifies peak rate shaping.
cir	Specifies the committed information rate (CIR), in bits per second (bps).
bc	(Optional) Specifies the Committed Burst size, in bits.
be	(Optional) Specifies the Excess Burst size, in bits.

Defaults

No default behavior or values

Command Modes

Class-map configuration

Command History

Release	Modification
12.1(2)T	This command was introduced.

Usage Guidelines

Traffic shaping limits the rate of transmission of data. In addition to using a specifically configured transmission rate, you can use Generic Traffic Shaping (GTS) to specify a derived transmission rate based on the level of congestion.

You can specify two types of traffic shaping; average rate shaping and peak rate shaping. Average rate shaping limits the transmission rate to the CIR. Using the CIR ensures that the average amount of traffic being sent conforms to the rate expected by the network.

Peak rate shaping configures the router to send more traffic than the CIR. To determine the peak rate, the router uses the following formula:

peak rate = CIR(1 + Be / Bc)

where:

- Be is the Excess Burst size.
- Bc is the Committed Burst size.

Peak rate shaping allows the router to burst higher than average rate shaping. However, using peak rate shaping, the traffic sent above the CIR (the delta) could be dropped if the network becomes congested.

If your network has additional bandwidth available (over the provisioned CIR) and the application or class can tolerate occasional packet loss, that extra bandwidth can be exploited through the use of peak rate shaping. However, there may be occasional packet drops when network congestion occurs. If the traffic being sent to the network must strictly conform to the configured network provisioned CIR, then you should use average traffic shaping.

Examples

The following example sets the uses average rate shaping to ensure a bandwidth of 256 kbps:

```
shape average 256000
```

The following example uses peak rate shaping to ensure a bandwidth of 300 kbps but allow throughput up to 512 kbps if enough bandwidth is available on the interface:

```
bandwidth 300
shape peak 512000
```

Related Commands

Command	Description
bandwidth	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 the default class (commonly known as the class-default class) before you configure its policy.
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.
shape max-buffers	Specifies the maximum number of buffers allowed on shaping queues.

shape (percent)

To specify average or peak-rate traffic shaping on the basis of a percentage of bandwidth available on an interface, use the **shape** command in policy-map class configuration mode. To remove traffic shaping, use the **no** form of this command.

shape {**average** | **peak**} **percent** *percent* [*bc*] [*be*]

no shape {**average** | **peak**} **percent** *percent* [*bc*] [*be*]

Syntax Description

average	Specifies average rate traffic shaping.
peak	Specifies peak rate traffic shaping.
percent	Specifies that percent of bandwidth will be used for either the average rate or peak rate traffic shaping.
percent	Specifies the bandwidth percentage. Valid range is a number from 1 to 100.
bc	(Optional) Specifies the committed burst (bc) size in milliseconds (ms). Valid range is a number from 10 to 2000.
be	(Optional) Specifies the excess burst (be) size in ms. Valid range is a number from 10 to 2000.

Defaults

Disabled

Command Modes

Policy-map class configuration

Command History

Release	Modification
12.1(2)T	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T. This command was modified for the Percentage-Based Policing and Shaping feature.

Usage Guidelines

This command calculates the committed information rate (CIR) based on a percentage of the available bandwidth on the interface. Once a policy map is attached to the interface, the equivalent CIR value in bits per second (bps) is calculated based on the interface bandwidth and the percent value entered with this command. The **show policy-map interface** command can then be used to verify the CIR bps value calculated.

The calculated CIR bps rate must be in the range of 8000 and 154400000 bps. If the rate is less than 8000 bps, the associated policy map cannot be attached to the interface. If the interface bandwidth changes (for example, more is added), the CIR bps values are recalculated based on the revised amount of bandwidth. If the CIR percentage is changed after the policy map is attached to the interface, the bps value of the CIR is recalculated.

This command also allows you to specify the values for the conform burst size and the peak burst size in milliseconds. If you want bandwidth to be calculated as a percentage, the conform burst size and the peak burst size must be specified in milliseconds.

The **shape** (percent) command, when used in "child" (nested) policy maps, is not supported on the Cisco 7500, the Cisco 7200, or lower series routers. Therefore, the **shape** (percent) command cannot be configured for use in nested policy maps on these routers.

How Bandwidth Is Calculated

The **shape** (percent) command is often used in conjunction with the **bandwidth** and **priority** commands. The **bandwidth** and **priority** commands can be used to calculate the total amount of bandwidth available on an entity (for example, a physical interface). When the **bandwidth** and **priority** commands calculate the total amount of bandwidth available on an entity, the following guidelines are invoked:

- If the entity is a physical interface, the total bandwidth is the bandwidth on the physical interface.
- If the entity is a shaped ATM permanent virtual circuit (PVC), the total bandwidth is calculated as follows:
  - For a variable bit rate (VBR) virtual circuit (VC), the sustained cell rate (SCR) is used in the calculation.
  - For an available bit rate (ABR) VC, the minimum cell rate (MCR) is used in the calculation.

For more information on bandwidth allocation, refer to the "Congestion Management Overview" chapter of the *Cisco IOS Quality of Service Solutions Configuration Guide*, Release 12.2.

Examples

The following example configures traffic shaping using an average shaping rate based on a percentage of bandwidth. In this example, 25 percent of the bandwidth has been specified. Additionally, an optional bc value and be value (300 ms and 400 ms, respectively) have been specified.

```
Router(config)# policy-map policy1
Router(config-pmap)# class-map class1
Router(config-pmap-c)# shape average percent 25 300 ms 400 ms
Router(config-pmap-c)# service-policy child-policy1
Router(config-pmap-c)# exit
Router(config-pmap-c)# interface serial 3/1
Router(config-if)# service-policy output policy1
```

Related Commands

Command	Description
bandwidth	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 the default class (commonly known as the class-default class) before you configure its policy.
police (percent)	Configures traffic policing based on a percentage of bandwidth available on an interface.
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.
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.
shape max-buffers	Specifies the maximum number of buffers allowed on shaping queues.

shape (policy-map class)

To shape traffic to the indicated bit rate according to the algorithm specified, use the **shape** command in policy-map class configuration mode. To remove shaping and leaving the traffic unshapped, use the **no** form of this command.

shape [**average** | **peak**] *mean-rate* [[*burst-size*] [*excess-burst-size*]]

no shape [**average** | **peak**]

Syntax Description

average	(Optional) Committed Burst (Bc) is the maximum number of bits sent out in each interval.
peak	(Optional) Bc + Excess Burst (Be) is the maximum number of bits sent out in each interval.
mean-rate	(Optional) Also called committed information rate (CIR). Indicates the bit rate used to shape the traffic, in bits per second. When this command is used with backward explicit congestion notification (BECN) approximation, the bit rate is the upper bound of the range of bit rates that will be permitted.
burst-size	(Optional) The number of bits in a measurement interval (Bc).
excess-burst-size	(Optional) The acceptable number of bits permitted to go over the Be.

Defaults

When Be is not configured, the default value is equal to Bc. For more information about burst size defaults, see the "Usage Guidelines" section of this command.

Command Modes

Policy-map class configuration

Command History

Release	Modification
12.0(5)XE	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.

Usage Guidelines

The measurement interval is Bc divided by CIR. Bc cannot be set to 0. If the measurement interval is too large (greater than 128 milliseconds), the system subdivides it into smaller intervals.

If you do not specify Bc and Be, the algorithm decides the default values for the shape entity. The algorithm uses a 4 milliseconds measurement interval, so Bc will be CIR * (4 / 1000).

Burst sizes larger than the default Bc need to be explicitly specified. The larger the Bc, the longer the measurement interval. A long measurement interval may affect voice traffic latency, if applicable.

When Be is not configured, the default value is equal to Bc.

Examples

The following example configures a shape entity with a CIR of 1 Mbps and attaches the policy map called dts-interface-all-action to interface pos1/0/0:

```
policy-map dts-interface-all-action
 class class-interface-all
   shape average 1000000

    interface pos1/0/0
       service-policy output dts-interface-all-action
```

Related Commands

Command	Description
shape adaptive	Configures a Frame Relay interface or a point-to-point subinterface to estimate the available bandwidth by BECN integration while traffic shaping is enabled.
shape fecn-adapt	Configures a Frame Relay PVC to reflect received FECN bits as BECN bits in Q.922 TEST RESPONSE messages.

shape adaptive

To configure a Frame Relay interface or a point-to-point subinterface to estimate the available bandwidth by backward explicit congestion notification (BECN) integration while traffic shaping is enabled, use the **shape adaptive** command in policy-map class configuration mode. To leave the available bandwidth unestimated, use the **no** form of this command.

shape adaptive *mean-rate-lower-bound*

no shape adaptive

Syntax Description

mean-rate-lower-bound	Specifies the lower bound of the range of permitted bit rates.

Defaults

No default behavior or values.

Command Modes

Policy-map class configuration

Command History

Release	Modification
12.0(5)XE	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(13)T	Support for this command was implemented on the Cisco 1700 series, Cisco 2500 series, Cisco 2600 series, Cisco 3620 router, Cisco 3631 router, Cisco 3640 router, Cisco 3660 router, Cisco 3725 router, Cisco 3745 router, Cisco 7200 series, Cisco 7400 series routers.

Usage Guidelines

If traffic shaping is not enabled, this command has no effect.

When continuous BECN messages are received, the shape entity immediately decreases its maximum shape rate by one-fourth for each BECN message received until it reaches the lower bound committed information rate (CIR). If, after several intervals, the interface has not received another BECN and traffic is waiting in the shape queue, the shape entity increases the shape rate back to the maximum rate by 1/16 for each interval. A shape entity configured with the **shape adaptive** *mean-rate-lower-bound* command will always be shaped between the mean rate upper bound and the mean rate lower bound.

Examples

The following example configures a shape entity with CIR of 128 kbps and sets the lower bound CIR to 64 kbps when BECNs are received:

```
policy-map dts-p2p-all-action
  class class-p2p-all
    shape average 128000
    shape adaptive 64000
```

shape fecn-adapt

To configure a Frame Relay interface to reflect received forward explicit congestion notification (FECN) bits as backward explicit congestion notification (BECN) bits in Q.922 TEST RESPONSE messages, use the **shape fecn-adapt** command in policy-map class configuration mode. To configure the Frame Relay interface to not reflect FECN as BECN, use the **no** form of this command.

shape fecn-adapt

no shape fecn-adapt

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Policy-map class configuration

Command History

Release	Modification
12.0(5)XE	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(13)T	Support for this command was implemented on the Cisco 1700 series, Cisco 2500 series, Cisco 2600 series, Cisco 3620 router, Cisco 3631 router, Cisco 3640 router, Cisco 3660 router, Cisco 3725 router, Cisco 3745 router, Cisco 7200 series, Cisco 7400 series routers.

Usage Guidelines

When the downstream Frame Relay switch is congested, a Frame Relay interface or point-to-point interface receives a Frame Relay message with the FECN bit on. This message may be an indication that no traffic is waiting to carry a BECN to the far end (voice/multimedia traffic is one-way). When the **shape fecn-adapt** command is configured, a small buffer is allocated and a Frame Relay TEST RESPONSE is built on behalf of the Frame Relay switch. The Frame Relay TEST RESPONSE is equipped with the triggering data-link connection identifier (DLCI) of the triggering mechanism. It also sets the BECN bit and sends it out to the wire.

Examples

The following example configures a shape entity with a committed information rate (CIR) of 1 Mbps and adapts the Frame Relay message with FECN to BECN:

```
policy-map dts-p2p-all-action
  class class-p2p-all
    shape average 1000000
    shape fecn-adapt
```

Related Commands

Command	Description
shape adaptive	Configures a Frame Relay interface or a point-to-point subinterface to estimate the available bandwidth by BECN integration while traffic shaping is enabled.
shape (percent)	Configures an interface to shape traffic to an indicated bit rate.

shape max-buffers

To specify the maximum number of buffers allowed on shaping queues, use the **shape max-buffers** command in class-map configuration mode. To remove the maximum number of buffers, use the **no** form of this command.

shape max-buffers *number-of-buffers*

no shape max-buffers *number-of-buffers*

Syntax Description

number-of-buffers	Specifies the maximum number of buffers. The minimum number of buffers is 1; the maximum number of buffers is 4096.

Defaults

1000 buffers

Command Modes

Class-map configuration

Command History

Release	Modification
12.1(2)T	This command was introduced.

Usage Guidelines

You can specify the maximum number of buffers allowed on shaping queues for each class configured to use Generic Traffic Shaping (GTS).

Examples

The following example configures shaping and sets the maximum buffer limit to 100:

```
shape average 350000
shape max-buffers 100
```

Related Commands

Command	Description
bandwidth	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 the default class (commonly known as the class-default class) before you configure its policy.
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.
shape	Specifies average or peak rate traffic shaping.

show access-lists rate-limit

To display information about rate-limit access lists, use the **show access-lists rate-limit** command in EXEC mode.

show access-lists rate-limit [*acl-index*]

Syntax Description

acl-index	(Optional) Rate-limit access list number from 1 to 299.

Command Modes

EXEC

Command History

Release	Modification
11.1 CC	This command was introduced.

Examples

The following is sample output from the **show access-lists rate-limit** command:

```
Router# show access-lists rate-limit

Rate-limit access list 1
    0
Rate-limit access list 2
    1
Rate-limit access list 3
    2
Rate-limit access list 4
    3
Rate-limit access list 5
    4
Rate-limit access list 6
    5
Rate-limit access list 9
    mask FF
Rate-limit access list 10
    mask 0F
Rate-limit access list 11
    mask F0
Rate-limit access list 100
    1001.0110.1111
Rate-limit access list 101
    00E0.34B8.D840
Rate-limit access list 199
    1111.1111.1111
```

The following is sample output from the **show access-lists rate-limit** command when specific rate-limit access lists are specified:

```
Router# show access-lists rate-limit 1

Rate-limit access list 1
    0
```

```
Router# show access-lists rate-limit 9

Rate-limit access list 9
    mask FF

Router# show access-lists rate-limit 101

Rate-limit access list 101
    00E0.34B8.D840
```

Table 16 describes the significant fields shown in the displays.

Table 16 show access-lists rate-limit Field Descriptions

Field	Description
Rate-limit access list	Rate-limit access list number. A number from 1 to 99 represents a precedence-based access list. A number from 100 to 199 indicates a MAC address-based access list.
0	IP Precedence for packets in this rate-limit access list.
mask FF	IP Precedence mask for packets in this rate-limit access list.
1001.0110.1111	MAC address for packets in this rate-limit access list.

Related Commands

Command	Description
access-list rate-limit	Configures an access list for use with CAR policies.
show access-lists	Displays the contents of current IP and rate-limit access lists.

show atm bundle

To display the bundle attributes assigned to each bundle virtual circuit (VC) member and the current working status of the VC members, use the **show atm bundle** command in privileged EXEC mode.

show atm bundle *bundle-name*

Syntax Description

bundle-name	The name of the bundle whose member information is displayed. This is the bundle name specified by the **bundle** command when the bundle was created.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(3)T	This command was introduced.

Examples

The following is sample output from the **show atm bundle** command (* indicates that this VC is the VC for all precedence levels not explicitly configured):

```
Router# show atm bundle

new-york on atm1/0.1 Status: UP

                      Config. Active  Bumping    PG/ Peak  Avg/Min  Burst
Name       VPI/VCI    Preced. Preced. Predec./   PV  kbps  kbps     Cells  Status
                                          Accept

ny-control   0/207      7        7      4  /Yes   pv  10000  5000     32      UP
ny-premium   0/206      6-5      6-5    7  /No    pg  20000  10000    32      UP
ny-priority  0/204      4-2      4-2    1  /Yes   pg  10000  3000             UP
ny-basic*    0/201      1-0      1-0    -  /Yes   pg  10000                   UP


los-angeles on atm1/0.1 - Status: UP

                      Config. Active  Bumping    pg/ Peak  Avg/Min  Burst
Name       VPI/VCI    Preced. Preced. Predec./   pv  kbps  kbps     Cells  Status
                                      Accept

la-high     0/407     7-5     7-5     4 /Yes      pv  20000  5000     32     UP
la-med      0/404     4-2     4-2     1 /Yes      pg  10000  3000            UP
la-low*     0/401     1-0     1-0     - /Yes      pg  10000                  UP
```

```
san-francisco on atm1/0.1 Status: UP

                       Config. Active  Bumping    PG/  Peak   Avg/Min   Burst
Name        VPI/VCI    Preced. Preced. Predec./   PV   kbps   kbps      Cells   Status
                                       Accept

sf-control    0/307      7        7      4 /Yes   pv   10000   5000      32       UP
sf-premium    0/306     6-5      6-5     7 /No    pg   20000   10000     32       UP
sf-priority   0/304     4-2      4-2     1 /Yes   pg   10000   3000               UP
sf-basic*     0/301     1-0      1-0     - /Yes   pg   10000                      UP
```

Related Commands

Command	Description
show atm bundle statistics	Displays statistics on the specified bundle.
show atm map	Displays the list of all configured ATM static maps to remote hosts on an ATM network.

show atm bundle statistics

To display statistics or detailed statistics on the specified bundle, use the **show atm bundle statistics** command in privileged EXEC mode.

show atm bundle *bundle-name* **statistics** [**detail**]

Syntax Description

bundle-name	Specifies the name of the bundle whose member information is displayed. This is the bundle name specified by the **bundle** command when the bundle was created.
detail	(Optional) Displays detailed statistics.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(3)T	This command was introduced.

Examples

The following is sample output from the **show atm bundle statistics** command:

```
Router# show atm bundle san-jose statistics

Bundle Name: Bundle State: UP
AAL5-NLPID
OAM frequency : 0 second(s), OAM retry frequency: 1 second(s)
OAM up retry count: 3, OAM down retry count: 5
BUNDLE is not managed.
InARP frequency: 15 minute(s)
InPkts: 3, OutPkts: 3, Inbytes: 1836, Outbytes: 1836
InPRoc: 3, OutPRoc: 0, Broadcasts: 3
InFast: 0, OutFast: 0, InAS: 0, OutAS: 0

Router# show atm bundle san-jose statistics detail

Bundle Name: Bundle State: UP
AAL5-NLPID
OAM frequency: 0 second(s), OAM retry frequency: 1 second(s)
OAM up retry count: 3, OAM down retry count: 5
BUNDLE is not managed.
InARP frequency: 15 minute(s)
InPkts: 3, OutPkts: 3, InBytes; 1836, OutBytes: 1836
InPRoc: 3, OutPRoc: 0, Broadcasts: 3
InFast: 0, OutFast: 0, InAS: 0, OutAS: 0

ATM1/0.52: VCD: 6, VPI: 0 VCI: 218, Connection Name: sj-basic
UBR, PeakRate: 155000
AAL5-LLC/SNAP, etype:0x0, Flags: 0xC20, VCmode: 0xE00
OAM frequency: 0 second(s), OAM retry frequency: 1 second(s)
OAM up retry count: 3, OAM down retry count: 5
OAM Loopbavk status: OAM Disabled
OMA VC state: Not Managed
ILMI VC state: Not Managed
InARP frequency: 15 minute(s)
```

```
InPkts: 3, OutPkts: 3, InBytes; 1836, OutBytes: 1836
InPRoc: 3, OutPRoc: 0,Broadcasts: 3
InFast: 0, OutFast: 0, InAS: 0, OututAS: 0
OAM cells received: 0
F5 InEndloop: 0, F5 InSegloop: 0, F5 InAIS: 0, F5 InRDI: 0
F4 InEndloop: 0, F4 OutSegloop:0, F4 InAIS: 0, F4 InRDI: 0
OAM cells sent: 0
F5 OutEndloop: 0. F5 OutSegloop: 0, f5 Out RDI:0
F4 OutEndloop: 0, F4 OutSegloop: 0, F4 OUtRDI: 0
OAM cell drops: 0
Status; UP

ATM1/0.52: VCD: 4, VPI: 0 VCI: 216, Connection Name: sj-premium
UBR, PeakRate: 155000
AAL5-LLC/SNAP, etype: 0x0, Flags: 0xC20, VCmode: 0xE000
OAM frequency: 0 second(s), OAM retry frequency: 1 second(s)
OAM up retry count: 3, OAM down retry count: 5
OAM Loopback status: OAM Disabled
OAM VC state:  Not Managed
ILMI VC state: Not Managed
InARP frequency: 15 minute(s)
InPkts: 0, OutPkts: 0, InBytes; 0, OutBytes: 0
InPRoc: 0, OutPRoc: 0, Broadcasts: 0
InFast: 0, OutFast: 0, InAS: 0
OAM cells received: 0
F5 InEndloop: 0, F4 InSegloop: 0, F4InAIS; 0, F4 InRDI: 0
F4 OutEndloop: 0, F4 OutSegloop: F4 OutRDI: 0
OAM cell drops: 0
Status: UP
```

Related Commands

Command	Description
show atm bundle	Displays the bundle attributes assigned to each bundle VC member and the current working status of the VC members.
show atm map	Displays the list of all configured ATM static maps to remote hosts on an ATM network.

show atm bundle svc

To display the bundle attributes assigned to each bundle virtual circuit (VC) member and the current working status of the VC members, use the **show atm bundle svc** command in privileged EXEC mode.

show atm bundle svc [*bundle-name*]

Syntax Description

bundle-name	(Optional) Name of the switched virtual circuit (SVC) bundle to be displayed, as identified by the **bundle svc** command.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(4)T	This command was introduced.

Usage Guidelines

If no bundle name is specified, all SVC bundles configured on the system are displayed.

Examples

The following example provides output for the **show atm bundle svc** command. The bundle named “finance” is configured on ATM interface 1/0.1 with eight members. All of the members are up except bundle member zero. Bundle member zero is the default member, which if initiated once will always be on and used as the default for all traffic.

```
Router# show atm bundle svc finance

finance on ATM1/0.1:UP

                        Config    Current   Peak    Avg/Min   Burst
VC Name       VPI/VCI   Preced.   Preced.   Kbps    kbps      Cells    Sts


seven         0/37        7         7       10000    5000       32     UP
six           0/36        6         6        6000                      UP
five          0/40        5         5        5000                      UP
four          0/41        4         4        4000                      UP
three         0/42        3         3        3000                      UP
two           0/43        2         2        2000                      UP
one           0/44        1         1        1000                      UP
zero*                     0
```

Table 17 describes the significant fields in the display.

Table 17 show atm bundle svc Field Descriptions

Field	Description
finance on ATM1/0.1: UP	Name of SVC bundle, interface type and number, status of bundle.
VC Name	Name of SVC bundle.
VPI/VCI	Virtual path identifier / virtual channel identifier.
Config. Preced.	Configured precedence.
Current Preced.	Current precedence.
Peak Kbps	Peak kbps for the SVC.
Avg/Min kbps	Average or minimum kbps for the SVC.
Sts	Status of the bundle member.
*	Indicates the default bundle member.

Related Commands

Command	Description
bundle svc	Creates or modifies an SVC bundle.

show atm bundle svc statistics

To display the statistics of a switched virtual circuit (SVC) bundle, use the **show atm bundle svc statistics** command in privileged EXEC mode.

show atm bundle svc *bundle-name* **statistics**

Syntax Description

bundle-name	Name of the SVC bundle as identified by the **bundle svc** command.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(4)T	This command was introduced.

Examples

The following example provides output for the **show atm bundle svc statistics** command using a bundle named "sanjose":

```
Router# show atm bundle svc sanjose statistics

Bundle Name:Bundle State:INITIALIZING
AAL5-NLPID
OAM frequency:0 second(s), OAM retry frequency:10 second(s)
OAM up retry count:4, OAM down retry count:3
BUNDLE is managed by.
InARP frequency:15 minutes(s)
InPkts:0, OutPkts:0, InBytes:0, OutBytes:0
InPRoc:0, OutPRoc:0, Broadcasts:0
InFast:0, OutFast:0, InAS:0, OutAS:0
InPktDrops:0, OutPktDrops:0
CrcErrors:0, SarTimeOuts:0, OverSizedSDUs:0,
                 LengthViolation:0, CPIErrors:0
```

Table 18 describes the significant fields in the display.

Table 18 show atm bundle svc statistics Field Descriptions

Field	Description
Bundle Name:	Name of the bundle.
Bundle State:	State of the bundle.
BUNDLE is managed by.	Bundle management.
InARP frequency:	Number of minutes between Inverse ARP messages, or "DISABLED" if Inverse ARP is not in use on this VC.
InPkts:	Total number of packets received on this virtual circuit (VC), including all fast-switched and process-switched packets.

Table 18 show atm bundle svc statistics Field Descriptions (continued)

Field	Description
OutPkts:	Total number of packets sent on this VC, including all fast-switched and process-switched packets.
InBytes:	Total number of bytes received on this VC, including all fast-switched and process-switched packets.
OutBytes:	Total number of bytes sent on this VC, including all fast-switched and process-switched packets.
InPRoc:	Number of incoming packets being process switched.
OutPRoc:	Number of outgoing packets being process switched.
Broadcasts:	Number of process-switched broadcast packets.
InFast:	Number of incoming packets being fast switched.
OutFast:	Number of outgoing packets being fast switched.
InAS	Number of autonomous-switched or silicon-switched input packets received.
OutAS	Number of autonomous-switched or silicon-switched input packets sent.
InPktDrops:	Number of incoming packets dropped.
OutPktDrops:	Number of outgoing packets dropped.
CrcErrors:	Number of cyclic redundancy check (CRC) errors.
SarTimeOuts:	Number of packets that timed out before segmentation and reassembly occurred.
LengthViolation:	Number of packets too long or too short.

Related Commands

Command	Description
bundle svc	Creates or modifies an SVC bundle.

show auto qos

To display the configurations created by the AutoQoS — VoIP feature on a specific interface or all interfaces, use the **show auto qos** command in EXEC mode.

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

Syntax Description

interface	(Optional) Indicates that the configurations for a specific interface type will be displayed.
interface type	(Optional) Specifies the interface type.

Defaults

Displays the configurations created for all interface types

Command Modes

EXEC

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

When the **auto qos voip** command is used to configure the AutoQoS — VoIP feature, configurations are generated for each interface or permanent virtual circuit (PVC). These configurations are then used to create the interface configurations, policy maps, class maps, and access control lists (ACLs). The **show auto qos** command can be used to verify the contents of the interface configurations, policy maps, class maps, and ACLs.

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

Examples

The following section contains sample output of the **show auto qos** command when the various optional keywords are specified.

Note The **show auto qos** command displays only those configurations created by the AutoQoS — VoIP feature.

show auto qos interface Command Example

When the **interface** keyword is configured along with the corresponding *interface type* argument, the **show auto qos interface** [*interface type*] command displays the configurations created by the AutoQoS — VoIP feature on the specified interface.

In the following example, the serial subinterface S6/1.1 has been specified:

```
Router# show auto qos interface s6/1.1

S6/1.1: DLCI 100 -
!
interface Serial6/1
 frame-relay traffic-shaping
!
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 **show auto qos interface** command displays the configurations created by the AutoQoS — VoIP feature on all the interfaces or PVCs on which the AutoQoS — VoIP feature is enabled.

```
Router# show auto qos interface

Serial6/1.1: DLCI 100 -
!
interface Serial6/1
 frame-relay traffic-shaping
!
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
```

show auto qos Command Example

The **show auto qos** command displays all of the configurations created by the AutoQoS — VoIP feature.

```
Router# show auto qos

Serial6/1.1: DLCI 100 -
!
interface Serial6/1
 frame-relay traffic-shaping
!
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
```

Table 19 describes the significant fields shown in the display.

Table 19 show auto qos Field Descriptions

Field	Description
class AutoQoS-VoIP-FR-Serial6/1-100	Name of 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 interface in the outbound direction of the interface.

Related Commands

Command	Description
auto qos voip	Configures the AutoQoS — VoIP feature on an interface.

show class-map

To display all class maps and their matching criteria, use the **show class-map** command in EXEC mode.

show class-map [*class-map-name*]

Syntax Description

class-map-name	(Optional) Name of the class map. The class map name can be a maximum of 40 alphanumeric characters.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(13)T	This command was modified to display the Frame Relay data-link connection identified (DLCI) number as a criterion for matching traffic inside a class map. In addition, this command was modified to display Layer 3 packet length as a criterion for matching traffic inside a class map.

Usage Guidelines

You can use the **show class-map** command to display all class maps and their matching criteria. If you enter the optional *class-map-name* argument, the specified class map and its matching criteria will be displayed.

Examples

In the following example, three class maps are defined. Packets that match access list 103 belong to class c3, IP packets belong to class c2, and packets that come through input Ethernet interface 1/0 belong to class c1. The output from the **show class-map** command shows the three defined class maps.

```
Router# show class-map

 Class Map c3
 Match access-group 103

 Class Map c2
 Match protocol ip

 Class Map c1
 Match input-interface Ethernet1/0
```

In the following example, a class map called "c1" has been defined, and the Frame Relay DLCI number of 500 has been specified as a match criterion:

```
Router# show class-map

class map match-all c1
   match fr-dlci 500
```

Table 20 describes the significant fields shown in the display.

Table 20 show class-map Field Descriptions[1]

Field	Description
Class-map	Class of traffic being displayed. Output is displayed for each configured class map 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 map. Choices include criteria such as the Frame Relay DLCI number, 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.

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

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class.
match fr-dlci	Specifies the Frame Relay DLCI number as a match criterion in a class map.
match packet length (class-map)	Specifies and uses the length of the Layer 3 packet in the IP header as a match criterion in a class map.
show policy-map	Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps.
show policy-map interface	Displays the packet statistics of all classes that are configured for all service policies either on the specified interface or subinterface or on a specific PVC on the interface.

show cops servers

To display the IP address and connection status of the policy servers for which the router is configured, use the **show cops servers** command in EXEC mode. The display also tells you about the Common Open Policy Service (COPS) client on the router.

show cops servers

Syntax Description

This command has no keywords or arguments.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
12.1(1)T	This command was introduced.

Examples

In the following example, information is displayed about the current policy server and client. When Client Type appears followed by an integer, 1 stands for Resource Reservation Protocol (RSVP) and 2 stands for Differentiated Services Provisioning. (0 indicates keepalive.)

```
Router# show cops servers

COPS SERVER: Address: 161.44.135.172. Port: 3288. State: 0. Keepalive: 120 sec
    Number of clients: 1. Number of sessions: 1.
COPS CLIENT: Client type: 1.  State: 0.
```

Related Commands

Command	Description
show ip rsvp policy cops	Displays policy server address(es), ACL IDs, and current state of the router-server connection.

show interfaces fair-queue

To display information and statistics about weighted fair queueing (WFQ) for a Versatile Interface Processor (VIP)-based interface, use the **show interfaces fair-queue** command in EXEC mode.

show interfaces [*interface-type interface-number*] **fair-queue**

Syntax Description

interface-type	(Optional) The type of the interface.
interface-number	(Optional) The number of the interface.

Command Modes

EXEC

Command History

Release	Modification
11.1 CC	This command was introduced.

Examples

The following is sample output from the **show interfaces fair-queue** command for VIP-distributed WFQ (DWFQ):

```
Router# show interfaces fair-queue

Hssi0/0/0 queue size 0
        packets output 1417079, drops 2
 WFQ: aggregate queue limit 54, individual queue limit 27
    max available buffers 54

     Class 0: weight 10 limit 27 qsize 0 packets output 1150 drops 0
     Class 1: weight 20 limit 27 qsize 0 packets output 0 drops 0
     Class 2: weight 30 limit 27 qsize 0 packets output 775482 drops 1
     Class 3: weight 40 limit 27 qsize 0 packets output 0 drops 0
```

Table 21 describes the significant fields shown in the display.

Table 21 show interfaces fair-queue Field Descriptions

Field	Description
queue size	Current output queue size for this interface.
packets output	Number of packets sent out this interface or number of packets in this class sent out the interface.
drops	Number of packets dropped or number of packets in this class dropped.
aggregate queue limit	Aggregate limit, in number of packets.
individual queue limit	Individual limit, in number of packets.
max available buffers	Available buffer space allocated to aggregate queue limit, in number of packets.
Class	QoS group or type of service (ToS) class.

Table 21 show interfaces fair-queue Field Descriptions (continued)

Field	Description
weight	Percent of bandwidth allocated to this class during periods of congestion.
limit	Queue limit for this class in number of packets.
qsize	Current size of the queue for this class.

Related Commands

Command	Description
show interfaces	Displays statistics for all interfaces configured on the router or access server.

show interfaces random-detect

To display information about Weighted Random Early Detection (WRED) for a Versatile Interface Processor (VIP)-based interface, use the **show interfaces random-detect** command in EXEC mode.

show interfaces [*interface-type interface-number*] **random-detect**

Syntax Description

interface-type	(Optional) The type of the interface.
interface-number	(Optional) The number of the interface.

Command Modes

EXEC

Command History

Release	Modification
11.1 CC	This command was introduced.

Examples

The following is sample output from the **show interfaces random-detect** command for VIP-distributed WRED (DWRED):

```
Router# show interfaces random-detect

 FastEthernet1/0/0 queue size 0
        packets output 29692, drops 0
 WRED: queue average 0
       weight 1/512
     Precedence 0: 109 min threshold, 218 max threshold, 1/10 mark weight
       1 packets output, drops: 0 random, 0 threshold
     Precedence 1: 122 min threshold, 218 max threshold, 1/10 mark weight
        (no traffic)
     Precedence 2: 135 min threshold, 218 max threshold, 1/10 mark weight
       14845 packets output, drops: 0 random, 0 threshold
     Precedence 3: 148 min threshold, 218 max threshold, 1/10 mark weight
        (no traffic)
     Precedence 4: 161 min threshold, 218 max threshold, 1/10 mark weight
        (no traffic)
     Precedence 5: 174 min threshold, 218 max threshold, 1/10 mark weight
        (no traffic)
     Precedence 6: 187 min threshold, 218 max threshold, 1/10 mark weight
       14846 packets output, drops: 0 random, 0 threshold
     Precedence 7: 200 min threshold, 218 max threshold, 1/10 mark weight
        (no traffic)
```

Table 22 describes the significant fields shown in the display.

Table 22 show interfaces random-detect Field Descriptions

Field	Description
queue size	Current output queue size for this interface.
packets output	Number of packets sent out this interface.
drops	Number of packets dropped.

Table 22 show interfaces random-detect Field Descriptions (continued)

Field	Description
queue average	Average queue length.
weight	Weighting factor used to determine the average queue size.
Precedence	WRED parameters for this precedence.
min threshold	Minimum threshold for this precedence.
max threshold	Maximum length of the queue. When the average queue is this long, any additional packets will be dropped.
mark weight	Probability of a packet being dropped if the average queue is at the maximum threshold.
packets output	Number of packets with this precedence that have been sent.
random	Number of packets dropped randomly through the WRED process.
threshold	Number of packets dropped automatically because the average queue was at the maximum threshold length.
(no traffic)	No packets with this precedence.

Related Commands

Command	Description
random-detect (interface)	Enables WRED or DWRED.
random-detect flow	Enables flow-based WRED.
show interfaces	Displays statistics for all interfaces configured on the router or access server.
show queueing	Lists all or selected configured queueing strategies.

show interfaces rate-limit

To display information about committed access rate (CAR) for an interface, use the **show interfaces rate-limit** command in EXEC mode.

show interfaces [*interface-type interface-number*] **rate-limit**

Syntax Description

interface-type	(Optional) The type of the interface.
interface-number	(Optional) The number of the interface.

Command Modes

EXEC

Command History

Release	Modification
11.1 CC	This command was introduced.

Examples

The following is sample output from the **show interfaces rate-limit** command:

```
Router# show interfaces fddi2/1/0 rate-limit

Fddi2/1/0
 Input
  matches: access-group rate-limit 100
   params: 800000000 bps, 64000 limit, 80000 extended limit
   conformed 0 packets, 0 bytes; action: set-prec-continue 1
   exceeded 0 packets, 0 bytes; action: set-prec-continue 0
   last packet: 4737508ms ago, current burst: 0 bytes
   last cleared 01:05:47 ago, conformed 0 bps, exceeded 0 bps
  matches: access-group 101
   params: 80000000 bps, 56000 limit, 72000 extended limit
   conformed 0 packets, 0 bytes; action: set-prec-transmit 5
   exceeded 0 packets, 0 bytes; action: set-prec-transmit 0
   last packet: 4738036ms ago, current burst: 0 bytes
   last cleared 01:02:05 ago, conformed 0 bps, exceeded 0 bps
  matches: all traffic
   params: 50000000 bps, 48000 limit, 64000 extended limit
   conformed 0 packets, 0 bytes; action: set-prec-transmit 5
   exceeded 0 packets, 0 bytes; action: set-prec-transmit 0
   last packet: 4738036ms ago, current burst: 0 bytes
   last cleared 01:00:22 ago, conformed 0 bps, exceeded 0 bps
 Output
  matches: all traffic
   params: 80000000 bps, 64000 limit, 80000 extended limit
   conformed 0 packets, 0 bytes; action: transmit
   exceeded 0 packets, 0 bytes; action: drop
   last packet: 4809528ms ago, current burst: 0 bytes
   last cleared 00:59:42 ago, conformed 0 bps, exceeded 0 bps
```

Table 23 describes the significant fields shown in the display.

Table 23 show interfaces rate-limit Field Descriptions

Field	Description
Input	These rate limits apply to packets received by the interface.
matches	Packets that match this rate limit.
params	Parameters for this rate limit, as configured by the **rate-limit** command.
bps	Average rate, in bits per second.
limit	Normal burst size, in bytes.
extended limit	Excess burst size, in bytes.
conformed	Number of packets that have conformed to the rate limit.
action	Conform action.
exceeded	Number of packets that have exceeded the rate limit.
action	Exceed action.
last packet	Time since the last packet, in milliseconds.
current burst	Instantaneous burst size at the current time.
last cleared	Time since the burst counter was set back to zero by the **clear counters** command.
conformed	Rate of conforming traffic.
exceeded	Rate of exceeding traffic.
Output	These rate limits apply to packets sent by the interface.

Related Commands

Command	Description
access-list rate-limit	Configures an access list for use with CAR policies.
clear counters	Clears the interface counters.
shape	Specifies average or peak rate traffic shaping.
show access-lists	Displays the contents of current IP and rate-limit access lists.
show interfaces	Displays statistics for all interfaces configured on the router or access server.

show ip nbar pdlm

To display the Packet Description Language Module (PDLM) in use by network-based application recognition (NBAR), use the **show ip nbar pdlm** command in privileged EXEC mode.

show ip nbar pdlm

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)XE2	This command was introduced.
12.1(1)E	This command was integrated into Cisco IOS Release 12.1(1)E.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.1(13)E	This command was integrated into Cisco IOS Release 12.1(13)E. This command became available on Catalyst 6000 family switches without FlexWAN modules.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.

Usage Guidelines

This command is used to display a list of all the PDLMs that have been loaded into NBAR using the **ip nbar pdlm** command.

Examples

In this example of the **show ip nbar pdlm** command, the citrix.pdlm PDLM has been loaded from Flash memory:

```
Router# show ip nbar pdlm

The following PDLMs have been loaded:
flash://citrix.pdlm
```

Related Commands

Command	Description
ip nbar pdlm	Extends or enhances the list of protocols recognized by NBAR through a Cisco-provided PDLM.

show ip nbar port-map

To display the current protocol-to-port mappings in use by network-based application recognition (NBAR), use the **show ip nbar port-map** command in privileged EXEC mode.

show ip nbar port-map [*protocol-name*]

Syntax Description

protocol-name	(Optional) Limits the command display to the specified protocol.

Defaults

This command displays port assignments for NBAR protocols.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)XE2	This command was introduced.
12.1(1)E	This command was integrated into Cisco IOS Release 12.1(1)E.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.1(13)E	This command was integrated into Cisco IOS Release 12.1(13)E. This command became available on Catalyst 6000 family switches without FlexWAN modules.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.

Usage Guidelines

This command is used to display the current protocol-to-port mappings in use by NBAR. When the **ip nbar port-map** command has been used, the **show ip nbar port-map** command displays the ports assigned by the user to the protocol. If no **ip nbar port-map** command has been used, the **show ip nbar port-map** command displays the default ports. The *protocol-name* argument can also be used to limit the display to a specific protocol.

Examples

The following example displays output from the **show ip nbar port-map** command:

```
Router# show ip nbar port-map

port-map bgp      udp 179
port-map bgp      tcp 179
port-map cuseeme  udp 7648 7649
port-map cuseeme  tcp 7648 7649
port-map dhcp     udp 67 68
port-map dhcp     tcp 67 68
```

Related Commands

Command	Description
ip nbar-port-map	Configures NBAR to search for a protocol or protocol name using a port number other than the well-known port.

show ip nbar protocol-discovery

To display the statistics gathered by the network-based application recognition (NBAR) Protocol Discovery feature, use the **show ip nbar protocol-discovery** command in privileged EXEC mode.

show ip nbar protocol-discovery [**interface** *interface-spec*] [**stats** {**byte-count** | **bit-rate** | **packet-count**}][{**protocol** *protocol-name* | **top-n** *number*}]

Syntax Description

interface	(Optional) Specifies that Protocol Discovery statistics for the interface are to be displayed.
interface-spec	(Optional) Specifies an interface to display.
stats	(Optional) Specifies that the byte count, byte rate, or packet count is to be displayed.
byte-count	(Optional) Specifies that the byte count is to be displayed.
bit-rate	(Optional) Specifies that the bit rate is to be displayed.
packet-count	(Optional) Specifies that the packet count is to be displayed.
protocol	(Optional) Specifies that statistics for a specific protocol are to be displayed.
protocol-name	(Optional) User-specified protocol name for which the statistics are to be displayed.
top-n	(Optional) Specifies that a top-n is to be displayed. A top-n is the number of most active NBAR-supported protocols, where n is the number of protocols to be displayed. For instance, if top-n 3 is entered, the three most active NBAR-supported protocols will be displayed.
number	(Optional) Specifies the number of most active NBAR-supported protocols to be displayed.

Defaults

Statistics for all interfaces on which the Protocol Discovery feature is enabled are displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)XE2	This command was introduced.
12.1(1)E	This command was integrated into Cisco IOS Release 12.1(1)E.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.1(13)E	This command was integrated into Cisco IOS Release 12.1(13)E. This command became available on Catalyst 6000 family switches without FlexWAN modules.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.

Usage Guidelines

Use the **show ip nbar protocol-discovery** command to display statistics gathered by the NBAR Protocol Discovery feature. This command, by default, displays statistics for all interfaces on which protocol discovery is currently enabled. The default output of this command includes, in the following order, input bit rate (in bits per second), input byte count, input packet count, and protocol name.

Protocol discovery can be used to monitor both input and output traffic and may be applied with or without a service policy enabled. NBAR protocol discovery gathers statistics for packets switched to output interfaces. These statistics are not necessarily for packets that exited the router on the output interfaces, because packets may have been dropped after switching for various reasons, including policing at the output interface, access lists, or queue drops.

Examples

The following example displays partial output of the **show ip nbar protocol-discovery** command for an Ethernet interface:

```
Router# show ip nbar protocol-discovery interface FastEthernet 6/0

 FastEthernet6/0
                            Input                    Output
   Protocol                 Packet Count             Packet Count
                            Byte Count               Byte Count
                            5 minute bit rate (bps)  5 minute bit rate (bps)
   ------------------------ ------------------------ ------------------------
   igrp                     316773                   0
                            26340105                 0
                            3000                     0
   streamwork               4437                     7367
                            2301891                  339213
                            3000                     0
   rsvp                     279538                   14644
                            319106191                673624
                            0                        0
   ntp                      8979                     7714
                            906550                   694260
                            0                        0
.
.
.
Total                    17203819                 151684936
                            19161397327              50967034611
                            4179000                  6620000
```

Related Commands

Command	Description
ip nbar protocol-discovery	Configures NBAR to discover traffic for all protocols known to NBAR on a particular interface.

show ip rsvp

To display specific information for Resource Reservation Protocol (RSVP) categories, use the **show ip rsvp** command in EXEC mode.

show ip rsvp [**atm-peak-rate-limit** | **counters** | **host** | **installed** | **interface** | **listeners** | **neighbor** | **policy** | **precedence** | **request** | **reservation** | **sbm** | **sender** | **signalling** | **tos**]

Syntax Description

atm-peak-rate-limit	(Optional) RSVP peak rate limit.
counters	(Optional) RSVP statistics.
host	(Optional) RSVP endpoint senders and receivers.
installed	(Optional) RSVP installed reservations.
interface	(Optional) RSVP interface information.
listeners	(Optional) RSVP listeners.
neighbor	(Optional) RSVP neighbor information.
policy	(Optional) RSVP policy information.
precedence	(Optional) RSVP precedence settings.
request	(Optional) RSVP reservations upstream.
reservation	(Optional) RSVP reservation requests from downstream.
sender	(Optional) RSVP path state information.
sbm	(Optional) RSVP subnet bandwidth manager (SBM) information.
signalling	(Optional) RSVP signalling information.
tos	(Optional) RSVP type of service (TOS) settings.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.2(13)T	The **listeners** and **policy** keywords were added, and this command was modified to display RSVP global settings when no keywords or arguments are entered.

Examples

The following command shows RSVP rate-limiting, refresh-reduction, and neighbor information:

```
Router# show ip rsvp

Rate Limiting:enabled
  Max msgs per interval:4
  Interval length (msec):20
  Max queue size:500
```

```
  Max msgs per second:200

Refresh Reduction:enabled
  ACK delay (msec):250
  Initial retransmit delay (msec):1000
  Local epoch:0x16528C
  Message IDs:in use 580, total allocated 3018, total freed 2438

Neighbors:1
  RSVP encap:1 UDP encap:0 RSVP and UDP encap:0

Local policy:
COPS:

Generic policy settings:
    Default policy:Accept all
    Preemption:    Disabled
```

Table 24 describes the fields shown in the display.

Table 24 show ip rsvp Command Field Descriptions

Field	Description
Rate Limiting: enabled (active) or disabled (not active)	The RSVP rate-limiting parameters in effect including the following: • Max msgs per interval = number of messages allowed to be sent per interval (timeframe). • Interval length (msecs) = interval (timeframe) length in milliseconds. • Max queue size = maximum size of the message queue in bytes. • Max msgs per second = maximum number of messages allowed to be sent per second.
Refresh Reduction: enabled (active) or disabled (not active)	The RSVP refresh-reduction parameters in effect including the following: • ACK delay (msec) = how long in milliseconds before the receiving router sends an acknowledgment (ACK). • Initial retransmit delay (msec) = how long in milliseconds before the router retransmits a message. • Local epoch = the RSVP message identifier (ID) number space identifier; randomly generated each time a node reboots or the RSVP process restarts. • Message IDs = the number of message IDs in use, the total number allocated, and the total number available (freed).
Neighbors	The total number of neighbors and the types of encapsulation in use including RSVP and User Datagram Protocol (UDP).
Local policy	The local policy currently configured.

Table 24 show ip rsvp Command Field Descriptions (continued)

Field	Description
COPS	The Common Open Policy Service (COPS) currently in effect.
Generic policy settings	Policy settings that are not specific to COPS or the local policy. Default policy: Accept all means all RSVP messages are accepted and forwarded. Reject all means all RSVP messages are rejected. Preemption: Disabled means RSVP is not prioritizing reservations and allocating bandwidth accordingly. Enabled means RSVP is prioritizing reservations and allocating more bandwidth to those with the highest priority.

Related Commands

Command	Description
debug ip rsvp	Displays debug messages for RSVP categories.

show ip rsvp atm-peak-rate-limit

To display the current peak rate limit set for an interface, if any, use the **show ip rsvp atm-peak-rate-limit** command in EXEC mode.

show ip rsvp atm-peak-rate-limit [*interface-name*]

Syntax Description

interface-name	(Optional) The name of the interface.

Command Modes

EXEC

Command History

Release	Modification
12.0(3)T	This command was introduced.

Usage Guidelines

The **show ip rsvp atm-peak-rate-limit** command displays the configured peak rate using the following notations for brevity:

- Kilobytes is shown as K bytes, for example, 1200 kilobytes is displayed as 1200K bytes.
- 1000 kilobytes is displayed as 1M bytes.

If no interface name is specified, configured peak rates for all Resource Reservation Protocol (RSVP)-enabled interfaces are displayed.

Examples

The following example depicts results of the **show ip rsvp atm-peak-rate-limit** command, presuming that the ATM subinterface 2/0/0.1 was configured with a reservation peak rate limit of 100 KB using the **ip rsvp atm-peak-rate-limit** command.

The following is sample output from the **show ip rsvp atm-peak-rate-limit** command using the *interface* argument:

```
Router# show ip rsvp atm-peak-rate-limit atm2/0/0.1

RSVP: Peak rate limit for ATM2/0/0.1 is 100K bytes
```

The following samples show output from the **show ip rsvp atm-peak-rate-limit** command when no interface name is given:

```
Router# show ip rsvp atm-peak-rate-limit

Interface name        Peak rate limit
Ethernet0/1/1         not set
ATM2/0/0              not set
ATM2/0/0.1            100K
```

```
Router# show ip rsvp atm-peak-rate-limit

Interface name       Peak rate limit
Ethernet0/1          not set
ATM2/1/0             1M
ATM2/1/0.10          not set
ATM2/1/0.11          not set
ATM2/1/0.12          not set
```

Related Commands

Command	Description
ip rsvp atm-peak-rate-limit	Sets a limit on the peak cell rate of reservations for all newly created RSVP SVCs established on the current interface or any of its subinterfaces.

show ip rsvp counters

To display the number of Resource Reservation Protocol (RSVP) messages that were sent and received on each interface, use the **show ip rsvp counters** command in EXEC mode.

show ip rsvp counters [**interface** *interface_unit* | **summary** | **neighbor**]

Syntax Description

interface *interface_unit*	(Optional) Number of RSVP messages sent and received for the specified interface name.
summary	(Optional) Cumulative number of RSVP messages sent and received by the router over all interfaces.
neighbor	(Optional) Number of RSVP messages sent and received by the specified neighbor.

Defaults

If you enter the **show ip rsvp counters** command without a keyword, the command displays the number of RSVP messages that were sent and received for each interface on which RSVP is configured.

Command Modes

EXEC

Command History

Release	Modification
12.0(14)ST	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T, and the **neighbor** keyword was added.
12.2(15)T	The following modifications were made to this command: • The **neighbor** keyword was added. • The output was modified to show the errors counter incrementing. This occurs whenever an RSVP message, on which the authentication checks have failed, is received on an interface that has RSVP authentication enabled.

Usage Guidelines

Use the **show ip rsvp counters** command to display the number of RSVP messages that were sent and received for each interface on which RSVP is configured.

Examples

The following command shows the values for the number of RSVP messages of each type that were sent and received by the router over all interfaces:

```
Router# show ip rsvp counters summary

All Interfaces          Recv      Xmit                          Recv      Xmit
    Path                23284        0     Resv                     0     23258
    PathError               0        0     ResvError                0         0
    PathTear                6        0     ResvTear                 0         6
    ResvConf                0        0     RTearConf                0         0
```

```
Ack                   186        86    Srefresh              85        93
DSBM_WILLING            0         0    I_AM_DSBM              0         0
Unknown                 0         0    Errors                 0         0
```

Table 25 describes the fields shown in the display.

Table 25 show ip rsvp counters summary Command Field Descriptions

Field	Description
All Interfaces	Types of messages displayed for all interfaces.
Recv	Number of messages received on the specified interface or on all interfaces.
Xmit	Number of messages transmitted from the specified interface or from all interfaces.

Related Commands

Command	Description
clear ip rsvp counters	Clears (sets to zero) all IP RSVP counters that are being maintained by the router.

show ip rsvp installed

To display Resource Reservation Protocol (RSVP)-related installed filters and corresponding bandwidth information, use the **show ip rsvp installed** command in EXEC mode.

show ip rsvp installed [*interface-type interface-number*] [**detail**]

Syntax Description

detail	(Optional) Specifies additional information about interfaces and their reservations.
interface-type	(Optional) Specifies the type of the interface.
interface-number	(Optional) Specifies the number of the interface.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
11.2	This command was introduced.
12.2(15)T	The command output was modified to display the resources required for a traffic control state block (TCSB) after compression has been taken into account.

Usage Guidelines

The **show ip rsvp installed** command displays information about interfaces and their reservations. Enter the optional **detail** keyword for additional information, including the reservation's traffic parameters, downstream hop, compression, and resources used by RSVP to ensure quality of service (QoS) for this reservation.

Examples

The following is sample output from the **show ip rsvp installed** command:

```
Router# show ip rsvp installed

RSVP:
RSVP: Ethernet1: has no installed reservations
RSVP: Serial0:
     kbps   To              From        Protocol DPort Sport Weight Conversation
     0      224.250.250.1   132.240.2.28     UDP 20    30    128    270
     150    224.250.250.1   132.240.2.1      UDP 20    30    128    268
     100    224.250.250.1   132.240.1.1      UDP 20    30    128    267
     200    224.250.250.1   132.240.1.25     UDP 20    30    256    265
     200    224.250.250.2   132.240.1.25     UDP 20    30    128    271
     0      224.250.250.2   132.240.2.28     UDP 20    30    128    269
     150    224.250.250.2   132.240.2.1      UDP 20    30    128    266
     350    224.250.250.3   0.0.0.0          UDP 20    0     128    26
```

Table 26 describes the significant fields shown in the display.

Table 26 show ip rsvp installed Field Descriptions

Field	Description
kbps	Reserved rate.
To	IP address of the source device.
From	IP address of the destination device.
Protocol	Protocol User Datagram Protocol (UDP)/TCP type.
DPort	Destination UDP/TCP port
Sport	Source UDP/TCP port.
Weight	Weight used in weighted fair queueing (WFQ).
Conversation	WFQ conversation number. If the WFQ is not configured on the interface, weight and conversation will be zero.

RSVP Compression Method Prediction Example

The following example of the **show ip rsvp installed detail** command shows the compression parameters, including the compression method, the compression context ID, and the bytes saved per packet, on the serial3/0 interface in effect:

```
Router# show ip rsvp installed detail

RSVP:Ethernet2/1 has no installed reservations

RSVP:Serial3/0 has the following installed reservations
RSVP Reservation. Destination is 10.1.1.2. Source is 10.1.1.1,
  Protocol is UDP, Destination port is 18054, Source port is 19156
  Compression:(method rtp, context ID = 1, 37.98 bytes-saved/pkt avg)
  Admitted flowspec:
    Reserved bandwidth:65600 bits/sec, Maximum burst:328 bytes, Peak rate:80K bits/sec
    Min Policed Unit:164 bytes, Max Pkt Size:164 bytes
  Admitted flowspec (as required if compression were not applied):
    Reserved bandwidth:80K bits/sec, Maximum burst:400 bytes, Peak rate:80K bits/sec
    Min Policed Unit:200 bytes, Max Pkt Size:200 bytes
  Resource provider for this flow:
    WFQ on FR PVC dlci 101 on Se3/0: PRIORITY queue 24.  Weight:0, BW 66 kbps
  Conversation supports 1 reservations [0x1000405]
  Data given reserved service:3963 packets (642085 bytes)
  Data given best-effort service:0 packets (0 bytes)
  Reserved traffic classified for 80 seconds
  Long-term average bitrate (bits/sec):64901 reserved, 0 best-effort
  Policy:INSTALL. Policy source(s):Default
```

The following example of the **show ip rsvp installed detail** command shows that compression is not predicted on the serial3/0 interface because no compression context IDs are available:

```
Router# show ip rsvp installed detail

RSVP:Ethernet2/1 has no installed reservations

RSVP:Serial3/0 has the following installed reservations
RSVP Reservation. Destination is 10.1.1.2. Source is 10.1.1.1,
  Protocol is UDP, Destination port is 18116, Source port is 16594
  Compression:(rtp compression not predicted:no contexts available)
```

```
Admitted flowspec:
  Reserved bandwidth:80K bits/sec, Maximum burst:400 bytes, Peak rate:80K bits/sec
  Min Policed Unit:200 bytes, Max Pkt Size:200 bytes
Resource provider for this flow:
  WFQ on FR PVC dlci 101 on Se3/0: PRIORITY queue 24.  Weight:0, BW 80 kbps
Conversation supports 1 reservations [0x2000420]
Data given reserved service:11306 packets (2261200 bytes)
Data given best-effort service:0 packets (0 bytes)
Reserved traffic classified for 226 seconds
Long-term average bitrate (bits/sec):79951 reserved, 0 best-effort
Policy:INSTALL. Policy source(s):Default
```

Note When no compression context IDs are available, use the **ip rtp compression-connections** *number* command to increase the pool of compression context IDs.

Related Commands

Command	Description
ip rtp compression-connections	Specifies the total number of RTP header compression connections that can exist on an interface.
show ip rsvp interface	Displays RSVP-related information.

show ip rsvp interface

To display Resource Reservation Protocol (RSVP)-related information, use the **show ip rsvp interface** command in EXEC mode.

show ip rsvp interface [*interface-type interface-number*] [**detail**]

Syntax Description

interface-type	(Optional) Type of the interface.
interface-number	(Optional) Number of the interface.
detail	(Optional) Additional information about interfaces.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
11.2	This command was introduced.
12.2(2)T	This command was modified to include the keyword **detail**.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T and was implemented on the Cisco 7500 series and the ATM-permanent virtual circuit (PVC) interface.
12.2(13)T	The following modifications were made to this command: • Rate-limiting and refresh-reduction information were added to the output display. • This command was modified to display RSVP global settings when no keywords or arguments are entered.
12.2(15)T	The following modifications were made to this command: • The command output was modified to display the effects of compression on admission control and the RSVP bandwidth limit counter. • Cryptographic authentication parameters were added to the display.

Usage Guidelines

Use the **show ip rsvp interface** command to display information about interfaces on which RSVP is enabled, including the current allocation budget and maximum available bandwidth. Enter the optional detail keyword for additional information, including bandwidth and signaling parameters and blockade state.

Use the **show ip rsvp interface detail** command to display information about the RSVP parameters associated with an interface. These parameters include the following:

- Total RSVP bandwidth
- RSVP bandwidth allocated to existing flows

- Maximum RSVP bandwidth that can be allocated to a single flow
- The type of admission control supported (header compression methods)
- The compression methods supported by RSVP compression prediction

Examples

The following command shows information for each interface on which RSVP is enabled:

```
Router# show ip rsvp interface

interface    allocated  i/f max  flow max sub max
PO0/0        0          200M     200M     0
PO1/0        0          50M      50M      0
PO1/1        0          50M      50M      0
PO1/2        0          50M      50M      0
PO1/3        0          50M      50M      0
Lo0          0          200M     200M     0
```

Table 27 describes the fields shown in the display.

Table 27 show ip rsvp interface Field Descriptions

Field	Description
interface	Interface name.
allocated	Current allocation budget.
i/f max	Maximum allocatable bandwidth.
flow max	Largest single flow allocatable on this interface.
sub max	Largest sub-pool value allowed on this interface.

Detailed RSVP Information Example

The following command shows detailed RSVP information for each interface on which RSVP is enabled:

```
Router# show ip rsvp interface detail

PO0/0:
   Bandwidth:
     Curr allocated:0 bits/sec
     Max. allowed (total):200M bits/sec
     Max. allowed (per flow):200M bits/sec
     Max. allowed for LSP tunnels using sub-pools:0 bits/sec
     Set aside by policy (total):0 bits/sec
   Signalling:
     DSCP value used in RSVP msgs:0x3F
     Number of refresh intervals to enforce blockade state:4
     Number of missed refresh messages:4
     Refresh interval:30

 PO1/0:
   Bandwidth:
     Curr allocated:0 bits/sec
     Max. allowed (total):50M bits/sec
     Max. allowed (per flow):50M bits/sec
     Max. allowed for LSP tunnels using sub-pools:0 bits/sec
     Set aside by policy (total):0 bits/sec
```

```
   Signalling:
     DSCP value used in RSVP msgs:0x3F
     Number of refresh intervals to enforce blockade state:4
     Number of missed refresh messages:4
     Refresh interval:30

PO1/1:
   Bandwidth:
     Curr allocated:0 bits/sec
     Max. allowed (total):50M bits/sec
     Max. allowed (per flow):50M bits/sec
     Max. allowed for LSP tunnels using sub-pools:0 bits/sec
     Set aside by policy (total):0 bits/sec
   Signalling:
     DSCP value used in RSVP msgs:0x3F
     Number of refresh intervals to enforce blockade state:4
     Number of missed refresh messages:4
     Refresh interval:30

 PO1/2:
   Bandwidth:
     Curr allocated:0 bits/sec
     Max. allowed (total):50M bits/sec
     Max. allowed (per flow):50M bits/secMax. allowed for LSP tunnels using sub-pools:0 
bits/sec
     Set aside by policy (total):0 bits/sec
   Signalling:
     DSCP value used in RSVP msgs:0x3F
     Number of refresh intervals to enforce blockade state:4
     Number of missed refresh messages:4
     Refresh interval:30

 PO1/3:
   Bandwidth:
     Curr allocated:0 bits/sec
     Max. allowed (total):50M bits/sec
     Max. allowed (per flow):50M bits/sec
     Max. allowed for LSP tunnels using sub-pools:0 bits/sec
     Set aside by policy (total):0 bits/sec
   Signalling:
     DSCP value used in RSVP msgs:0x3F
     Number of refresh intervals to enforce blockade state:4
     Number of missed refresh messages:4
     Refresh interval:30

 Lo0:
   Bandwidth:
     Curr allocated:0 bits/sec
     Max. allowed (total):200M bits/sec
     Max. allowed (per flow):200M bits/sec
     Max. allowed for LSP tunnels using sub-pools:0 bits/sec
     Set aside by policy (total):0 bits/sec
   Signalling:
     DSCP value used in RSVP msgs:0x3F
     Number of refresh intervals to enforce blockade state:4
     Number of missed refresh messages:4
     Refresh interval:30
```

Table 28 describes the significant fields shown in the detailed display for interface PO0/0. The fields for the other interfaces are similar.

Table 28 show ip rsvp interface detail Field Descriptions — Detailed RSVP Information Example

Field	Description
PO0/0	Interface name.
Bandwidth	The RSVP bandwidth parameters in effect including the following: • Curr allocated = amount of bandwidth currently allocated in bits per second. • Max. allowed (total) = maximum amount of bandwidth allowed in bits per second. • Max. allowed (per flow) = maximum amount of bandwidth allowed per flow in bits per second. • Max. allowed for LSP tunnels using sub-pools = maximum amount of bandwidth allowed for label switched path (LSP) tunnels in bits per second. • Set aside by policy (total) = the amount of bandwidth set aside by the local policy in bits per second.
Signalling	The RSVP signalling parameters in effect including the following: • DSCP value used in RSVP msgs = differentiated services code point (DSCP) used in RSVP messages. • Number of refresh intervals to enforce blockade state = how long in milliseconds before the blockade takes effect. • Number of missed refresh messages = how many refresh messages until the router state expires. • Refresh interval = how long in milliseconds until a refresh message is sent.

RSVP Compression Method Prediction Example

The following example from the **show ip rsvp interface detail** command shows the RSVP compression method prediction configuration for each interface on which RSVP is configured:

```
Router# show ip rsvp interface detail

 Et2/1:
   Bandwidth:
     Curr allocated:0 bits/sec
     Max. allowed (total):1158K bits/sec
     Max. allowed (per flow):128K bits/sec
     Max. allowed for LSP tunnels using sub-pools:0 bits/sec
     Set aside by policy (total):0 bits/sec
   Admission Control:
     Header Compression methods supported:
       rtp (36 bytes-saved), udp (20 bytes-saved)
   Neighbors:
     Using IP encap:0.  Using UDP encap:0
   Signalling:
     Refresh reduction:disabled
   Authentication:disabled
```

```
Se3/0:
  Bandwidth:
    Curr allocated:0 bits/sec
    Max. allowed (total):1158K bits/sec
    Max. allowed (per flow):128K bits/sec
    Max. allowed for LSP tunnels using sub-pools:0 bits/sec
    Set aside by policy (total):0 bits/sec
  Admission Control:
    Header Compression methods supported:
      rtp (36 bytes-saved), udp (20 bytes-saved)
  Neighbors:
    Using IP encap:1.  Using UDP encap:0
  Signalling:
    Refresh reduction:disabled
  Authentication:disabled
```

Table 29 describes the significant fields shown in the display for interface Et2/1. The fields for interface Se3/0 are similar.

Table 29 show ip rsvp interface detail Field Descriptions — RSVP Compression Method Prediction Example

Field	Description
Et2/1: Se3/0	Interface name.
Bandwidth	The RSVP bandwidth parameters in effect including the following: • Curr allocated = amount of bandwidth currently allocated in bits per second. • Max. allowed (total) = maximum amount of bandwidth allowed in bits per second. • Max. allowed (per flow) = maximum amount of bandwidth allowed per flow in bits per second. • Max. allowed for LSP tunnels using sub-pools = maximum amount of bandwidth allowed for LSP tunnels in bits per second. • Set aside by policy (total) = the amount of bandwidth set aside by the local policy in bits per second.
Admission Control	The type of admission control in effect including the following: • Header Compression methods supported: – Real-Time Transport Protocol (RTP) or User Data Protocol (UDP) compression schemes and the number of bytes saved per packet.
Neighbors	The number of neighbors using IP and UDP encapsulation.
Signalling	The type of signaling in effect; Refresh reduction is either enabled (active) or disabled (inactive).
Authentication	Authentication is either enabled (active) or disabled (inactive).

Cryptographic Authentication Example

The following example of the **show ip rsvp interface detail** command displays detailed information, including the cryptographic authentication parameters, for all RSVP-configured interfaces on the router:

```
Router# show ip rsvp interface detail

 Et0/0:
   Bandwidth:
    Curr allocated: 0 bits/sec
    Max. allowed (total): 7500K bits/sec
    Max. allowed (per flow): 7500K bits/sec
    Max. allowed for LSP tunnels using sub-pools: 0 bits/sec
    Set aside by policy (total):0 bits/sec
   Neighbors:
    Using IP encap: 0.  Using UDP encap: 0
   Signalling:
    Refresh reduction: disabled
   Authentication: enabled
    Key:            11223344
    Type:           sha-1
    Window size:    2
    Challenge:      enabled
```

Table 30 describes the significant fields shown in the display.

Table 30 show ip rsvp interface detail Field Descriptions — Cryptograhic Authentication Example

Field	Description
Et0/0	Interface name.
Bandwidth	The RSVP bandwidth parameters in effect including the following: • Curr allocated = amount of bandwidth currently allocated in bits per second. • Max. allowed (total) = maximum amount of bandwidth allowed in bits per second. • Max. allowed (per flow) = maximum amount of bandwidth allowed per flow in bits per second. • Max. allowed for LSP tunnels using sub-pools = maximum amount of bandwidth allowed for LSP tunnels in bits per second. • Set aside by policy (total) = the amount of bandwidth set aside by the local policy in bits per second.
Neighbors	The number of neighbors using IP and UDP encapsulation.
Signalling	The type of signaling in effect; Refresh reduction is either enabled (active) or disabled (inactive).

Table 30 show ip rsvp interface detail Field Descriptions — Cryptograhic Authentication Example

Field	Description
Authentication	Authentication is either enabled (active) or disabled (inactive). The parameters include the following: • Key = The key (string) for the RSVP authentication algorithm displayed in clear text (for example, 11223344) or encrypted <encrypted>. • Type = The algorithm to generate cryptographic signatures in RSVP messages; possible values are md5 and sha-1. • Window size = Maximum number of RSVP authenticated messages that can be received out of order. • Challenge = The challenge-response handshake performed with any new RSVP neighbors that are discovered on a network; possible values are **enabled** (active) or **disabled** (inactive).

Related Commands

Command	Description
show ip rsvp installed	Displays RSVP-related installed filters and corresponding bandwidth information.
show ip rsvp neighbor	Displays current RSVP neighbors.

show ip rsvp listeners

To display the Resource Reservation Protocol (RSVP) listeners for a specified port or protocol, use the **show ip rsvp listeners** command in EXEC mode.

show ip rsvp listeners [*dst* | **any**] [**UDP** | **TCP** | **any** | *protocol*] [*dst-port* | **any**]

Syntax Description

dst | **any**	(Optional) A particular destination or any destination for an RSVP message.
UDP | **TCP** | **any** | *protocol*	(Optional) User Datagram Protocol (UDP), TCP, or any protocol to be used on the receiving interface and the UDP or TCP source port number. **Note** If you select *protocol*, the range is 0 to 255 and the protocol is IP.
dst-port | **any**	(Optional) A particular destination port from 0 to 65535 or any destination for an RSVP message.

Defaults

If you enter **show ip rsvp listeners** command without a keyword or an argument, the command displays all the listeners that were sent and received for each interface on which RSVP is configured.

Command Modes

EXEC

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

Use the **show ip rsvp listeners** command to display the number of listeners that were sent and received for each interface on which RSVP is configured.

Examples

The following command shows the current listeners:

```
Router# show ip rsvp listeners

To                Protocol    DPort   Description                    Action
145.10.2.1        any         any     RSVP Proxy                     reply
```

Table 31 describes the fields shown in the display.

Table 31 show ip rsvp listeners Command Field Descriptions

Field	Description
To	IP address of the receiving interface.
Protocol	Protocol used.

Table 31 show ip rsvp listeners Command Field Descriptions (continued)

Field	Description
DPort	Destination port on the receiving router.
Description	Cisco IOS component that requested RSVP to do the listening; for example, RSVP proxy and label-switched path (LSP) tunnel signaling.
Action	Action taken when a flow arrives at its destination. The choices include: • Announce—The arrival of the flow is announced. • Reply—After the flow arrives at its destination, the sender receives a reply.

Related Commands

Command	Description
ip rsvp listener	Configures an RSVP router to listen for Path messages.

show ip rsvp neighbor

To display current Resource Reservation Protocol (RSVP) neighbors, use the **show ip rsvp neighbor** command in EXEC mode.

show ip rsvp neighbor [**detail**]

Syntax Description

detail	(Optional) Additional information about RSVP neighbors.

Command Modes

EXEC

Command History

Release	Modification
11.2	This command was introduced.
12.2(13)T	The *interface-type interface-number* arguments were deleted. The **detail** keyword was added to the command, and rate-limiting and refresh-reduction information was added to the output.

Usage Guidelines

Use the **show ip rsvp neighbor** command to show the IP addresses for the current RSVP neighbors. Enter the **detail** keyword to display rate-limiting and refresh-reduction parameters for the RSVP neighbors.

Examples

The following command shows the current RSVP neighbors:

```
Router# show ip rsvp neighbor

 21.0.0.1        RSVP
 22.0.0.2        RSVP
```

Table 32 describes the fields shown in the display.

Table 32 show ip rsvp neighbor Command Field Descriptions

Field	Description
21.0.0.1	IP address of neighboring router.
RSVP	Type of encapsulation being used.

The following command shows the rate-limiting and refresh-reduction parameters for the current RSVP neighbors:

```
Router# show ip rsvp neighbor detail

Neighbor:21.0.0.1
    Encapsulation:RSVP
    Rate-Limiting:
      Dropped messages:0
```

```
Refresh Reduction:
      Remote epoch:0x1BFEA5
      Out of order messages:0
      Retransmitted messages:0
      Highest rcvd message id:1059
      Last rcvd message:00:00:04

Neighbor:22.0.0.2
    Encapsulation:RSVP
    Rate-Limiting:
      Dropped messages:0
    Refresh Reduction:
      Remote epoch:0xB26B1
      Out of order messages:0
      Retransmitted messages:0
      Highest rcvd message id:945
      Last rcvd message:00:00:05
```

Table 33 describes the fields shown in the display.

Table 33 show ip rsvp neighbor detail Command Field Descriptions

Field	Description
Neighbor	IP address of the neighboring router.
Encapsulation	Type of encapsulation being used.
Rate-Limiting	The rate-limiting parameters in effect including: • Dropped messages = number of messages dropped by the neighbor.
Refresh Reduction	The refresh-reduction parameters in effect including: • Remote epoch = the RSVP message number space identifier (ID); randomly generated whenever the node reboots or the RSVP process restarts. • Out of order messages = messages that were dropped because they are out of sequential order. • Retransmitted messages = number of messages retransmitted to the neighbor. • Highest rcvd message id = highest message ID number sent by the neighbor. • Last rcvd message= time delta in hours, minutes, and seconds when last message was received by the neighbor.

Related Commands

Command	Description
show ip rsvp interface	Displays RSVP-related interface information.

show ip rsvp policy

To display the policies currently configured, use the **show ip rsvp policy** command in EXEC mode.

show ip rsvp policy [**cops** | **local** [*acl*]]

Syntax Description

cops | **local**	(Optional) Displays either the configured Common Open Policy Service (COPS) servers or the local policies.
acl	(Optional) Displays the access control lists (ACLs) whose sessions are governed by COPS servers or the local policies.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
12.1(1)T	This command was introduced as **show ip rsvp policy cops**.
12.2(13)T	This command was modified to include the **local** keyword. This command replaces the **show ip rsvp policy cops** command.

Usage Guidelines

Use the **show ip rsvp policy** command to display current local policies, configured COPS servers, default policies, and the preemption parameter (disabled or enabled).

Examples

The following is sample output from the **show ip rsvp policy** command:

```
Router# show ip rsvp policy

Local policy:

    A=Accept    F=Forward

    Path:-- Resv:-- PathErr:-- ResvErr:-- ACL:104
    Path:-- Resv:-- PathErr:-- ResvErr:-- ACL:None [Default policy]

COPS:

Generic policy settings:
    Default policy: Accept all
    Preemption:     Disabled
```

Table 34 describes the fields shown in the display.

Table 34 show ip rsvp policy Command Field Descriptions

Field	Description
Local policy	The local policy currently configured. A = Accept the message. F = Forward the message. Blank (--) means messages of the specified type are neither accepted or forwarded.
COPS	The COPS servers currently in effect.
Generic policy settings	Policy settings that are not specific to COPS or the local policy. Default policy: Accept all means all RSVP messages are accepted and forwarded. Reject all means all RSVP messages are rejected. Preemption: Disabled means that RSVP should not implement any preemption decisions required by a particular local or remote policy. Enabled means that RSVP should implement any preemption decisions required by a particular local or remote policy.

Related Commands

Command	Description
ip rsvp signalling initial-retransmit-delay	Creates a local procedure that determines the use of RSVP resources in a network.

show ip rsvp policy cops

Note Effective with Release 12.2(13)T, the **show ip rsvp policy cops** command is replaced by the **show ip rsvp policy** command. See the **show ip rsvp policy** command for more information.

To display the policy server addresses, access control list (ACL) IDs, and current state of the router-server connection, use the **show ip rsvp policy cops** command.

show ip rsvp policy cops [*acl*]

Syntax Description

[*acl*]	(Optional) The ACLs whose sessions are governed by Common Open Policy Service (COPS). ACLs can be numbers between 1 and 199.

Defaults

This command has no default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
12.1(1)T	This command was introduced.
12.2(13)T	This command was replaced by the **show ip rsvp policy** command.

Usage Guidelines

If you omit the final keyword of this command **(cops)**, the display reports only on the ACLs and their connection status. This kind of display is shown in the second example in the "Examples" section.

If the server connection has recently broken, this command also displays the reconnection attempt interval.

Examples

The following example shows the full display, using the full command:

```
Router# show ip rsvp policy cops

COPS/RSVP entry. ACLs: 40 60
    PDPs: 161.44.135.172
    Current state: Connected
    Currently connected to PDP 161.44.135.172, port 0
```

The following example shows the ID for the configured ACLs and their connection status, using the shortened command:

```
Router# show ip rsvp policy

Local policy: Currently unsupported
COPS:
    ACLs: 40 60 . State: CONNECTED.
    ACLs: 40 160 . State: CONNECTING.
```

Related Commands

Command	Description
show cops servers	Displays the IP address and connection status of the policy servers for which the router is configured.

show ip rsvp policy local

To display the local policies currently configured, use the **show ip rsvp policy local** command in EXEC mode.

show ip rsvp policy local [**detail**] [**default** | **acl** *acl*]

Syntax Description

detail	(Optional) Additional information about the configured local policies including preempt-priority and local-override.
default	(Optional) Information about the default policy.
acl *acl*	(Optional) Used when an access control list (ACL) is specified. Values are numbers from 1 to 199.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

Use the **show ip rsvp policy local** command to display information about the (selected) local policies currently configured.

If you use the ACL option, you can specify only one ACL. However, that parameter can be any ACL of any local policy that you have created. If you have multiple local policies with a common ACL, then using the ACL option displays all local policies with that ACL. On the other hand, if you have created local policies each with multiple ACLs, you cannot use the ACL option to show only a specific policy. You must omit the ACL option and show all the local policies.

Examples

The following is sample output from the **show ip rsvp policy local detail** command after you enter the **ip rsvp policy local acl 104** command:

```
Router# show ip rsvp policy local detail

Local policy for ACL(s): 104
    Preemption Priority: Start at 0, Hold at 0.
    Local Override: Disabled.

                Accept   Forward
    Path:       No       No
    Resv:       No       No
    PathError:  No       No
    ResvError:  No       No

Default local policy:
    Preemption Priority: Start at 0, Hold at 0.
```

```
    Local Override: Disabled.
Accept   Forward
    Path:       No       No
    Resv:       No       No
    PathError:  No       No
    ResvError:  No       No

Generic policy settings:
    Default policy: Accept all
    Preemption:     Disabled
```

Table 35 describes the fields shown in the display.

Table 35 show ip rsvp policy local detail Command Field Descriptions

Field	Description
Local policy for ACL(s)	The local policy currently configured for a specified ACL.
Preemption Priority	Start at 0, Hold at 0 indicates the priorities for resource requests contained in Resv messages that match the ACL(s) of this policy. Values are 0 to 65,535. • Start at 0 indicates the priority of the reservation when it was installed. • Hold at 0 indicates the priority of the reservation after it was installed.
Local Override	Overrides any remote Common Open Policy Service (COPS) policy by enforcing the local policy in effect. • Disabled = not active. • Enabled = active.
Path, Resv, PathError, ResvError	Types of RSVP messages being accepted and forwarded. • No = message not being accepted or forwarded. • Yes = message being accepted and forwarded.
Default local policy	The default local policy currently configured.
Preemption Priority	Start at 0, Hold at 0 indicates the priorities for resource requests contained in Resv messages that match the ACL(s) of this policy. Values are 0 to 65,535. • Start at 0 indicates the priority of the reservation when it was installed. • Hold at 0 indicates the priority of the reservation after it was installed.
Local Override	Overrides any remote (COPS) policy by enforcing the local policy in effect. • Disabled = not active. • Enabled = active.

Related CommandsL

Command	Description
ip rsvp signalling initial-retransmit-delay	Creates a local procedure that determines the use of RSVP resources in a network.

show ip rsvp request

To display Resource Reservation Protocol (RSVP)-related request information being requested upstream, use the **show ip rsvp request** command in EXEC mode.

show ip rsvp request [*ip-address*][**detail**]

Syntax Description

ip-address	(Optional) IP or group address of the requestor.
detail	(Optional) Specifies additional request information.

Command Modes

EXEC

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

Use this command to show the RSVP reservations currently being requested upstream for a specified interface or all interfaces. The received reservations may differ from requests because of aggregated or refused reservations.

Examples

The following is sample output from the **show ip rsvp request** command:

```
Router# show ip rsvp request

To              From            Pro DPort Sport Next Hop       I/F    Fi Serv
132.240.1.49    132.240.4.53    1   0     0     132.240.3.53   Et1    FF LOAD
```

Table 36 describes the significant fields shown in the display.

Table 36 show ip rsvp request Field Descriptions

Field	Description
To	IP address of the receiver.
From	IP address of the sender.
Pro	Protocol code. Code 1 indicates Internet Control Message Protocol (ICMP).
DPort	Destination port number.
Sport	Source port number.
Next Hop	IP address of the next hop.
I/F	Interface of the next hop.
Fi	Filter (Wild Card Filter, Shared Explicit, or Fixed Filter).
Serv	Service (value can be **rate** or **load**).

show ip rsvp reservation

To display Resource Reservation Protocol (RSVP)-related receiver information currently in the database, use the **show ip rsvp reservation** command in EXEC mode.

show ip rsvp reservation [*ip-address*][**detail**]

Syntax Description

ip-address	(Optional) IP or group address of the receiver.
detail	(Optional) Specifies additional reservation information.

Command Modes

EXEC

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

Use this command to show the current receiver (RESV) information in the database for a specified interface or all interfaces. This information includes reservations aggregated and forwarded from other RSVP routers.

Examples

The following is sample output from the **show ip rsvp reservation** command:

```
Router# show ip rsvp reservation

To            From          Pro DPort Sport Next Hop      I/F    Fi Serv
132.240.1.49  132.240.4.53  1    0      0     132.240.1.49  Se1    FF LOAD
```

Table 37 describes the significant fields shown in the display.

Table 37 show ip rsvp reservation Field Descriptions

Field	Descriptions
To	IP address of the receiver.
From	IP address of the sender.
Pro	Protocol code. Code 1 indicates Internet Control Message Protocol (ICMP).
DPort	Destination port number.
Sport	Source port number.
Next Hop	IP address of the next hop.
I/F	Interface of the next hop.
Fi	Filter (Wild Card Filter, Shared Explicit, or Fixed Filter).
Serv	Service (value can be **rate** or **load**).

show ip rsvp sbm

To display information about a Subnetwork Bandwidth Manager (SBM) configured for a specific Resource Reservation Protocol (RSVP)-enabled interface or for all RSVP-enabled interfaces on the router, use the **show ip rsvp sbm** command in EXEC mode.

show ip rsvp sbm [**detail**] [*interface-name*]

Syntax Description

detail	(Optional) Detailed SBM configuration information, including values for the NonResvSendLimit object.
interface-name	(Optional) Name of the interface for which you want to display SBM configuration information.

Command Modes

EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T. The **detail** keyword was added.

Usage Guidelines

To obtain SBM configuration information about a specific interface configured to use RSVP, specify the interface name with the **show ip rsvp sbm** command. To obtain information about all interfaces enabled for RSVP on the router, use the **show ip rsvp sbm** command without specifying an interface name.

To view the values for the NonResvSendLimit object, use the **detail** keyword.

Examples

The following example displays information for the RSVP-enabled Ethernet interfaces 1 and 2 on router1:

```
Router# show ip rsvp sbm

Interface DSBM Addr      DSBM Priority    DSBM Candidate   My Priority
Et1       1.1.1.1        70               yes              70
Et2       10.2.2.150     100              yes              100
```

The following example displays information about the RSVP-enabled Ethernet interface e2 on router1:

```
Router# show ip rsvp sbm e2

Interface DSBM Addr       DSBM Priority    DSBM candidate   My Priority
e2        10.2.2.150      100              yes              100
```

Table 38 describes the significant fields shown in the display.

Table 38 show ip rsvp sbm Field Descriptions

Field	Description
Interface	Name of the Designated Subnetwork Bandwidth Manager (DSBM) candidate interface on the router.
DSBM Addr	IP address of the DSBM.
DSBM Priority	Priority of the DSBM.
DSBM Candidate	Yes if the **ip rsvp dsbm candidate** command was issued for this SBM to configure it as a DSBM candidate. No if it was not so configured.
My Priority	Priority configured for this interface.

The following example displays information about the RSVP-enabled Ethernet interface 2 on router1. In the left column, the local SBM configuration is shown; in the right column, the corresponding information for the current DSBM is shown. In this example, the information is the same because the DSBM won election.

```
Router# show ip rsvp sbm detail

Interface:Ethernet2
Local Configuration              Current DSBM
  IP Address:10.2.2.150          IP Address:10.2.2.150
  DSBM candidate:yes              I Am DSBM:yes
  Priority:100                    Priority:100
  Non Resv Send Limit              Non Resv Send Limit
    Rate:500 Kbytes/sec             Rate:500 Kbytes/sec
    Burst:1000 Kbytes               Burst:1000 Kbytes
    Peak:500 Kbytes/sec             Peak:500 Kbytes/sec
    Min Unit:unlimited              Min Unit:unlimited
    Max Unit:unlimited              Max Unit:unlimited
```

Table 39 describes the significant fields shown in the display.

Table 39 show ip rsvp sbm detail Field Descriptions

Field	Description
Local Configuration	The local DSBM candidate configuration.
Current DSBM	The current DSBM configuration.
Interface	Name of the DSBM candidate interface on the router.
IP Address	IP address of the local DSBM candidate or the current DSBM.
DSBM candidate	Yes if the **ip rsvp dsbm candidate** command was issued for this SBM to configure it as a DSBM candidate. No if it was not so configured.
I am DSBM	Yes if the local candidate is the DSBM. No if the local candidate is not the DSBM.
Priority	Priority configured for the local DSBM candidate or the current SBM.
Rate	The average rate, in kbps, for the DSBM candidate.
Burst	The maximum burst size, in KB, for the DSBM candidate.

Table 39 show ip rsvp sbm detail Field Descriptions (continued)

Field	Description
Peak	The peak rate, in kbps, for the DSBM candidate.
Min Unit	The minimum policed unit, in bytes, for the DSBM candidate.
Max Unit	The maximum packet size, in bytes, for the DSBM candidate.

Related Commands

Command	Description
debug ip rsvp	Displays information about SBM message processing, the DSBM election process, and standard RSVP enabled message processing information
debug ip rsvp detail	Displays detailed information about RSVP and SBM.
debug ip rsvp detail sbm	Display detailed information about SBM messages only, and SBM and DSBM state transitions
ip rsvp dsbm candidate	Configures an interface as a DSBM candidate.
ip rsvp dsbm non-resv-send-limit	Configures the NonResvSendLimit object parameters.

show ip rsvp sender

To display Resource Reservation Protocol (RSVP) PATH-related sender information currently in the database, use the **show ip rsvp sender** command in EXEC mode.

show ip rsvp sender [*ip-address*] [**detail**]

Syntax Description

ip-address	(Optional) IP or group address of the sender.
detail	(Optional) Specifies additional sender information.

Command Modes

EXEC

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

Use this command to show the RSVP sender (PATH) information currently in the database for a specified interface or all interfaces.

Examples

The following is sample output from the **show ip rsvp sender** command:

```
Router# show ip rsvp sender

To              From            Pro DPort Sport Prev Hop        I/F
132.240.1.49    132.240.4.53    1   0     0     132.240.3.53    Et1
132.240.2.51    132.240.5.54    1   0     0     132.240.3.54    Et1
```

Table 40 describes the significant fields shown in this display.

Table 40 show ip rsvp sender Field Descriptions

Field	Description
To	IP address of the receiver.
From	IP address of the sender.
Pro	Protocol code. Code 1 indicates Internet Control Message Protocol (ICMP).
DPort	Destination port number.
Sport	Source port number.
Prev Hop	IP address of the previous hop.
I/F	Interface of the previous hop.

show ip rsvp signalling

To display Resource Reservation Protocol (RSVP) signaling information that optionally includes rate-limiting and refresh-reduction parameters for RSVP messages, use the **show ip rsvp signalling** command in EXEC mode.

show ip rsvp signalling [**rate-limit** | **refresh reduction**]

Syntax Description

rate-limit	(Optional) Rate-limiting parameters for signalling messages.
refresh reduction	(Optional) Refresh-reduction parameters and settings.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

Use the **show ip rsvp signalling** command with either the **rate-limit** or the **refresh reduction** keyword to display rate-limiting parameters or refresh-reduction parameters, respectively.

Examples

The following command shows rate-limiting parameters:

```
Router# show ip rsvp signalling rate-limit

Rate Limiting:enabled
  Max msgs per interval:4
  Interval length (msec):20
  Max queue size:500
  Max msgs per second:200
  Max msgs allowed to be sent:37
```

Table 41 describes the fields shown in the display.

Table 41 show ip rsvp signalling rate-limit Command Field Descriptions

Field	Description
Rate Limiting: enabled (active) or disabled (not active)	The RSVP rate-limiting parameters in effect including the following: • Max msgs per interval = number of messages allowed to be sent per interval (timeframe). • Interval length (msecs) = interval (timeframe) length in milliseconds. • Max queue size = maximum size of the message queue in bytes. • Max msgs per second = maximum number of messages allowed to be sent per second.

The following command shows refresh-reduction parameters:

```
Router# show ip rsvp signalling refresh reduction

Refresh Reduction:enabled
  ACK delay (msec):250
  Initial retransmit delay (msec):1000
  Local epoch:0x74D040
  Message IDs:in use 600, total allocated 3732, total freed 3132
```

Table 42 describes the fields shown in the display.

Table 42 show ip rsvp signalling refresh reduction Command Field Descriptions

Field	Description
Refresh Reduction: enabled (active) or disabled (not active)	The RSVP refresh-reduction parameters in effect including the following: • ACK delay (msec) = how long in milliseconds before the receiving router sends an acknowledgment (ACK). • Initial retransmit delay (msec) = how long in milliseconds before the sending router retransmits a message. • Local epoch = the RSVP process identifier that defines a local router for refresh reduction and reliable messaging; randomly generated each time a node reboots or the RSVP process restarts. • Message IDs = the number of message identifiers (IDs) in use, the total number allocated, and the total number available (freed).

Related Commands

Command	Description
clear ip rsvp signalling rate-limit	Clears the counters recording dropped messages.
clear ip rsvp signalling refresh reduction	Clears the counters recording retransmissions and out-of-order messages.
debug ip rsvp rate-limit	Displays debug messages for RSVP rate-limiting events.
ip rsvp signalling rate-limit	Controls the transmission rate for RSVP messages sent to a neighboring router during a specified amount of time.
ip rsvp signalling refresh reduction	Enables refresh reduction.

show ip rsvp signalling blockade

To display the Resource Reservation Protocol (RSVP) sessions that are currently blockaded, use the **show ip rsvp signalling blockade** command in EXEC mode.

show ip rsvp signalling blockade [**detail**] [*name* | *address*]

Syntax Description

detail	(Optional) Additional blockade information.
name	(Optional) Name of the router being blockaded.
address	(Optional) IP address of the destination of a reservation.

Defaults

If you enter the **show ip rsvp signalling blockade** command without a keyword or an argument, the command displays all the blockaded sessions on the router.

Command Modes

EXEC

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

Use the **show ip rsvp signalling blockade** command to display the RSVP sessions that are currently blockaded.

An RSVP sender becomes blockaded when the corresponding receiver sends a Resv message that fails admission control on a router that has RSVP configured. A ResvError message with an admission control error is sent in reply to the Resv message, causing all routers downstream of the failure to mark the associated sender as blockaded. As a result, those routers do not include that contribution to subsequent Resv refreshes for that session until the blockade state times out.

Blockading solves a denial-of-service problem on shared reservations where one receiver can request so much bandwidth as to cause an admission control failure for all the receivers sharing that reservation, even though the other receivers are making requests that are within the limit.

Examples

The following example shows all the sessions currently blockaded:

```
Router# show ip rsvp signalling blockade

To               From            Pro DPort Sport Time Left Rate
192.168.101.2    192.168.101.1   UDP 1000  1000  27        5K
192.168.101.2    192.168.101.1   UDP 1001  1001  79        5K
192.168.101.2    192.168.101.1   UDP 1002  1002  17        5K
225.1.1.1        192.168.104.1   UDP 2222  2222  48        5K
```

Table 43 describes the fields shown in the display.

Table 43 show ip rsvp signalling blockade Command Field Descriptions

Field	Description
To	IP address of the receiver.
From	IP address of the sender.
Pro	Protocol used.
DPort	Destination port number.
Sport	Source port number.
Time Left	Amount of time, in seconds, before the blockade expires.
Rate	The average rate, in bits per second, for the data.

The following example shows more detail about the sessions currently blockaded:

```
Router# show ip rsvp signalling blockade detail

Session address: 192.168.101.2, port: 1000. Protocol: UDP
Sender address:  192.168.101.1, port: 1000
  Admission control error location: 192.168.101.1
  Flowspec that caused blockade:
    Average bitrate:      5K bits/second
    Maximum burst:        5K bytes
    Peak bitrate:         5K bits/second
    Minimum policed unit: 0 bytes
    Maximum packet size:  0 bytes
    Requested bitrate:    5K bits/second
    Slack:                0 milliseconds
  Blockade ends in:       99 seconds

Session address: 192.168.101.2, port: 1001. Protocol: UDP
Sender address:  192.168.101.1, port: 1001
  Admission control error location: 192.168.101.1
  Flowspec that caused blockade:
    Average bitrate:      5K bits/second
    Maximum burst:        5K bytes
    Peak bitrate:         5K bits/second
    Minimum policed unit: 0 bytes
    Maximum packet size:  0 bytes
    Requested bitrate:    5K bits/second
    Slack:                0 milliseconds
  Blockade ends in:       16 seconds

Session address: 192.168.101.2, port: 1002. Protocol: UDP
Sender address:  192.168.101.1, port: 1002
  Admission control error location: 192.168.101.1
  Flowspec that caused blockade:
    Average bitrate:      5K bits/second
    Maximum burst:        5K bytes
    Peak bitrate:         5K bits/second
    Minimum policed unit: 0 bytes
    Maximum packet size:  0 bytes
    Requested bitrate:    5K bits/second
    Slack:                0 milliseconds
  Blockade ends in:       47 seconds
```

```
Session address: 225.1.1.1, port: 2222. Protocol: UDP
Sender address:  192.168.104.1, port: 2222
  Admission control error location: 192.168.101.1
  Flowspec that caused blockade:
    Average bitrate:       5K bits/second
    Maximum burst:         5K bytes
    Peak bitrate:          5K bits/second
    Minimum policed unit: 0 bytes
    Maximum packet size:  0 bytes
    Requested bitrate:     5K bits/second
    Slack:                 0 milliseconds
  Blockade ends in:        124 seconds
```

Table 44 describes the fields shown in the display.

Table 44 show ip rsvp signalling blockade detail Command Field Descriptions

Field	Description
Session address	Destination IP address of the reservation affected by the blockade.
port	Destination port number of the reservation affected by the blockade.
Protocol	Protocol used by the reservation affected by the blockade; choices include User Datagram Protocol (UDP) and TCP.
Sender address	Source IP address of the reservation affected by the blockade.
port	Source port number of the reservation affected by the blockade.
Admission control error location	IP address of the router where the admission control error occurred.
Flowspec that caused blockade	Parameters for the flowspec that caused the blockade.
Average bitrate	The average rate, in bits per second, for the flowspec.
Maximum burst	The maximum burst size, in bytes, for the flowspec.
Peak bitrate	The peak rate, in bps, for the flowspec.
Minimum policed unit	The minimum policed unit, in bytes, for the flowspec.
Maximum packet size	The maximum packet size, in bytes, for the flowspec.
Requested bitrate	The requested rate, in bits per second, for the flowspec.
Slack	Time, in milliseconds, allocated to a router for scheduling delivery of packets.
Blockade ends in	Time, in seconds, until the blockade expires.

show ip rsvp signalling rate-limit

To display the Resource Reservation Protocol (RSVP) rate-limiting parameters, use the **show ip rsvp signalling rate-limit** command in EXEC mode.

show ip rsvp signalling rate-limit

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
12.2(13)T	This command was introduced.

Examples

The following command shows the rate-limiting parameters:

```
Router# show ip rsvp signalling rate-limit

Rate Limiting:
  Max msgs per interval: 4
  Interval length (msec): 20
  Max queue size: 500
  Max msgs per second: 200
```

Table 45 describes the fields shown in the display.

Table 45 show ip rsvp signalling rate-limit Command Field Descriptions

Field	Description
Rate Limiting	The RSVP rate-limiting parameters in effect including the following: • Max msgs per interval = number of messages allowed to be sent per interval (timeframe). • Interval length (msecs) = interval (timeframe) length in milliseconds. • Max queue size = maximum size of the message queue in bytes. • Max msgs per second = maximum number of messages allowed to be sent per second.

Related Commands

Command	Description
clear ip rsvp signalling rate-limit	Clears (sets to zero) the number of messages that were dropped because of a full queue.
debug ip rsvp rate-limit	Displays debug messages for RSVP rate-limiting events.
ip rsvp signalling rate-limit	Controls the transmission rate for RSVP messages sent to a neighboring router during a specified amount of time.

show ip rsvp signalling refresh reduction

To display the Resource Reservation Protocol (RSVP) refresh-reduction parameters, use the **show ip rsvp signalling refresh reduction** command in EXEC mode.

show ip rsvp signalling refresh reduction

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
12.2(13)T	This command was introduced.

Examples

The following command shows the refresh-reduction parameters:

```
Router# show ip rsvp signalling refresh reduction

Refresh Reduction:
  ACK delay (msec): 250
  Initial retransmit delay (msec): 1000
  Local epoch: 0xF2F6BC
  Message IDs: in use 1, total allocated 4, total freed 3
```

Table 46 describes the fields shown in the display.

Table 46 show ip rsvp signalling refresh reduction Command Field Descriptions

Field	Description
Refresh Reduction	The RSVP refresh-reduction parameters in effect including the following: • ACK delay (msec) = how long in milliseconds before the receiving router sends an acknowledgment (ACK). • Initial retransmit delay (msec) = how long in milliseconds before the sending router retransmits a message. • Local epoch = the RSVP message number space ID (identifier); randomly generated each time a node reboots or the RSVP process restarts. • Message IDs = the number of message IDs in use, the total number allocated, and the total number available (freed).

Related Commands

Command	Description
clear ip rsvp signalling refresh reduction	Clears (sets to zero) the counters recording retransmissions and out-of-order messages.
ip rsvp signalling refresh reduction	Enables refresh reduction.

show policy-map

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

show policy-map [*policy-map*]

Syntax Description

policy-map	(Optional) The name of the service policy map whose complete configuration is to be displayed.

Defaults

All existing policy map configurations are displayed.

Command Modes

EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(5)XE	This command was incorporated into Cisco IOS Release 12.0(5)XE.
12.0(7)S	This command was incorporated into Cisco IOS Release 12.0(7)S.
12.1(1)E	This command was incorporated into Cisco IOS Release 12.1(1)E.
12.2(4)T	This command was modified for two-rate traffic policing. It now can display burst parameters and associated actions.
12.2(8)T	The command was modified for the Policer Enhancement — Multiple Actions feature and the WRED — Explicit Congestion Notification (ECN) feature.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T, and 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.
12.2(15)T	This command was modified to support display of Frame Relay voice-adaptive traffic-shaping information.

Usage Guidelines

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

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

Examples

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)
    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:

```
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)
```

Table 47 describes the significant fields shown in the display.

Table 47 show policy-map Field Descriptions

Field	Description
Policy Map	Policy map name.
Class	Class name.
Bandwidth	Amount of bandwidth in kbps allocated to class.
Max thresh	Maximum threshold. Maximum Weighted Random Early Detection (WRED) threshold in number of packets.

Frame Relay Voice-Adaptive Traffic-Shaping Example

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

```
Router# show policy-map

  Policy Map VSD1
    Class VOICE1
      Strict Priority
      Bandwidth 10 (kbps) Burst 250 (Bytes)
    Class SIGNALS1
      Bandwidth 8 (kbps) Max Threshold 64 (packets)
    Class DATA1
      Bandwidth 15 (kbps) Max Threshold 64 (packets)

  Policy Map MQC-SHAPE-LLQ1
    Class class-default
      Traffic Shaping
         Average Rate Traffic Shaping
                 CIR 63000 (bps) Max. Buffers Limit 1000 (Packets)
                 Adapt to 8000 (bps)
                 Voice Adapt Deactivation Timer 30 Sec
      service-policy VSD1
```

Table 48 describes the significant fields shown in the display.

Table 48 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.

Table 48 show policy-map Field Descriptions — Configured for Frame Relay Voice-Adaptive Traffic- Shaping (continued)

Field	Description
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".

Two-Rate Traffic Policing show policy-map Command Example

The following is sample output from the **show policy-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 s3/0
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.

Table 49 describes the significant fields shown in the display.

Table 49 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 show policy-map Command Example

The following is sample output from the **show policy-map** command when the Policer Enhancement — Multiple Actions feature has been configured. The following sample output of the **show policy-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.

Table 50 describes the significant fields shown in the display.

Table 50 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 show policy-map Command Example

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

```
Router# show policy-map

   Policy Map 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
```

Table 51 describes the significant fields shown in the display.

Table 51 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 show policy-map Command 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
```

Table 52 describes the significant fields shown in the display.

Table 52 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 show policy-map Command 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)
```

Table 53 describes the significant fields shown in the display.

Table 53 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 show policy-map Command Example

The following sample output of the **show policy-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 of the **show policy-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
```

Table 54 describes the fields shown in the display.

Table 54 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.

Related Commands

Command	Description
drop	Configures a traffic class to discard packets belonging to a specific class.
police	Configures traffic policing.
police (two rates)	Configures traffic policing using two rates, the CIR and the PIR.
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
random-detect ecn	Enables ECN.
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 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 **show policy-map class** command in EXEC 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.

Defaults

No default behavior or values

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.

Usage Guidelines

You can use the **show policy-map class** 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 packet statistics of all classes that are configured for all service policies either on the specified interface or subinterface or on a specific permanent virtual circuit (PVC) on the interface, use the **show policy-map interface** command in EXEC mode.

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

Syntax Description

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

Defaults

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

Command Modes

EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(5)XE	This command was incorporated into Cisco IOS Release 12.0(5)XE.
12.0(7)S	This command was incorporated into Cisco IOS Release 12.0(7)S.
12.1(1)E	This command was incorporated into Cisco IOS Release 12.1(1)E.
12.1(2)T	This command was integrated into Cisco IOS Release 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 integrated into Cisco IOS Release 12.1(3)T. This command was modified to display per-class accounting statistics.
12.2(4)T	This command was modified for two-rate traffic policing. It now can display burst parameters and associated actions.
12.2(8)T	The command was modified for the Policer Enhancement — Multiple Actions feature and the WRED — Explicit Congestion Notification (ECN) feature.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T and the following modifications were made: • The output was modified for the Percentage-Based Policing and Shaping feature. • This command was modified for the Class-Based RTP and TCP Header Compression feature. • This command was modified as part of the Modular QoS CLI (MQC) Unconditional Packet Discard feature. Traffic classes in policy maps can now be configured to discard packets belonging to a specified class. • This command was modified to display the Frame Relay DLCI number as a criterion for matching traffic inside a class map. • This command was modified to display Layer 3 packet length as a criterion for matching traffic inside a class map. • This command was modified for the Enhanced Packet Marking feature. A mapping table (table map) can now be used to convert and propagate packet-marking values.
12.2(15)T	This command was modified to support display of Frame Relay voice-adaptive traffic-shaping information.

Usage Guidelines

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

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

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

The **show policy-map interface** command will display 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.

Examples

This section provides sample output of a typical **show policy-map interface** command. Depending upon the interface in use and the options enabled, the output you see may vary slightly from the ones shown below. See Table 55 for an explanation of the significant fields that commonly appear in the command output.

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.

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

Router# show policy-map output interface s3/1

 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
```

The following sample output of 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.

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

Router# show policy-map output interface s3/2

 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: ip precedence 0
      Traffic Shaping
        Target    Byte   Sustain   Excess    Interval  Increment Adapt
        Rate      Limit  bits/int  bits/int  (ms)      (bytes)   Active
        320000    2000   8000      8000      25        1000      -

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

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

Table 55 describes the significant fields shown in the displays. The fields in the table are grouped according to the relevant QoS feature.

Table 55 show policy-map interface Field Descriptions [1]

Field	Description
Fields Associated with Classes or Service Policies	
Service-policy output	Name of the output service policy applied to the specified interface or VC.
Class-map	Class of traffic being displayed. Output is displayed for each configured class in the policy. The choice for implementing class matches (for example, match-all or match-any) can also appear next to the traffic class.
packets and bytes	Number of packets (also shown in bytes) identified as belonging to the class of traffic being displayed.
offered rate	Rate, in kbps, of packets coming in to the class. **Note** If the packets are compressed over an outgoing interface, the improved packet rate achieved by packet compression is not reflected in the offered rate. Also, if the packets are classified *before* they enter a combination of tunnels (for example, a generic routing encapsulation (GRE) tunnel and an IP Security (IPSec) tunnel), the offered rate does not include all the extra overhead associated with tunnel encapsulation in general. Depending on the configuration, the offered rate may include no overhead, may include the overhead for only *one* tunnel encapsulation, or may include the overhead for *all* tunnel encapsulations. In most of the GRE and IPSec tunnel configurations, the offered rate includes the overhead for GRE tunnel encapsulation only.
drop rate	Rate, in kbps, at which packets are dropped from the class. The drop rate is calculated by subtracting the number of successfully transmitted packets from the offered rate.
Match	Match criteria specified for the class of traffic. Choices include criteria such as IP precedence, IP differentiated services code point (DSCP) value, Multiprotocol Label Switching (MPLS) experimental (EXP) value, access groups, and QoS groups. For more information about the variety of match criteria options available, refer to the chapter "Configuring the Modular Quality of Service Command-Line Interface" in the *Cisco IOS Quality of Service Solutions Configuration Guide*, Release 12.2.
Fields Associated with Queueing (if Enabled)	
Output Queue	The weighted fair queueing (WFQ) conversation to which this class of traffic is allocated.
Bandwidth	Bandwidth, in either kbps or percentage, configured for this class and the burst size.
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.

Table 55 show policy-map interface Field Descriptions [1] (continued)

Field	Description
Fields Associated with Weighted Random Early Detection (WRED) (if Enabled)	
exponential weight	Exponent used in the average queue size calculation for a WRED parameter group.
mean queue depth	Average queue depth based on the actual queue depth on the interface and the exponential weighting constant. It is a fluctuating average. The minimum and maximum thresholds are compared against this value to determine drop decisions.
class	IP precedence level.
Transmitted pkts/bytes	Number of packets (also shown in bytes) passed through WRED and not dropped by WRED. **Note** If there is insufficient memory in the buffer to accommodate the packet, the packet can be dropped *after* the packet passes through WRED. Packets dropped because of insufficient memory in the buffer (sometimes referred to as "no-buffer drops") are not taken into account by the WRED packet counter.
Random drop pkts/bytes	Number of packets (also shown in bytes) randomly dropped when the mean queue depth is between the minimum threshold value and the maximum threshold value for the specified IP precedence level.
Tail drop pkts/bytes	Number of packets dropped when the mean queue depth is greater than the maximum threshold value for the specified IP precedence level.
Minimum thresh	Minimum threshold. Minimum WRED threshold in number of packets.
Maximum thresh	Maximum threshold. Maximum WRED threshold in number of packets.
Mark prob	Mark probability. Fraction of packets dropped when the average queue depth is at the maximum threshold.
Fields Associated with Traffic Shaping (if Enabled)	
Target Rate	Rate used for shaping traffic.
Byte Limit	Maximum number of bytes that can be transmitted per interval. Calculated as follows: ((Bc+Be) /8) x 1
Sustain bits/int	Committed burst (Bc) rate.
Excess bits/int	Excess burst (Be) rate.
Interval (ms)	Time interval value in milliseconds (ms).
Increment (bytes)	Number of credits (in bytes) received in the token bucket of the traffic shaper during each time interval.

Table 55 show policy-map interface Field Descriptions [1] (continued)

Field	Description
Queue Depth	Current queue depth of the traffic shaper.
Packets	Total number of packets that have entered the traffic shaper system.
Bytes	Total number of bytes that have entered the traffic shaper system.
Packets Delayed	Total number of packets delayed in the queue of the traffic shaper before being transmitted.
Bytes Delayed	Total number of bytes delayed in the queue of the traffic shaper before being transmitted.
Shaping Active	Indicates whether the traffic shaper is active. For example, if a traffic shaper is active, and the traffic being sent exceeds the traffic shaping rate, a "yes" appears in this field.

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

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

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

```
Router# show policy interface Serial3/1.1

 Serial3/1.1:DLCI 201 -

  Service-policy output:MQC-SHAPE-LLQ1

    Class-map:class-default (match-any)
      1434 packets, 148751 bytes
      30 second offered rate 14000 bps, drop rate 0 bps
      Match:any
      Traffic Shaping
           Target/Average   Byte   Sustain   Excess    Interval  Increment
             Rate           Limit  bits/int  bits/int  (ms)      (bytes)
            63000/63000     1890   7560      7560      120       945

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

Table 56 describes the significant fields shown in the display. Significant fields that are not described in Table 56 are described in Table 55, "show policy-map interface Field Descriptions."

Table 56 show policy-map interface Field Descriptions — Configured for Frame Relay Voice-Adaptive Traffic Shaping

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

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

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

```
Router# show policy-map interface s3/0

 Serial3/0

  Service-policy output: policy1

   Class-map: police (match all)
    148803 packets, 36605538 bytes
    30 second offered rate 1249000 bps, drop rate 249000 bps
    Match: access-group 101
    police:
     cir 500000 bps, conform-burst 10000, pir 1000000, peak-burst 100000
     conformed 59538 packets, 14646348 bytes; action: transmit
     exceeded 59538 packets, 14646348 bytes; action: set-prec-transmit 2
     violated 29731 packets, 7313826 bytes; action: drop
     conformed 499000 bps, exceed 500000 bps violate 249000 bps
   Class-map: class-default (match-any)
    19 packets, 1990 bytes
    30 seconds offered rate 0 bps, drop rate 0 bps
    Match: any
```

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

Table 57 describes the significant fields shown in the display.

Table 57 show policy-map interface Field Descriptions — Configured for Two-Rate Traffic Policing

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

Multiple Traffic Policing Actions show policy-map interface Command Example

The following is sample output from the **show policy-map** command when the Policer Enhancement — Multiple Actions feature has been configured. The sample output of 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 s3/2

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 of **show policy-map interface** command shows the following:

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

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

Table 58 describes the significant fields shown in the display.

Table 58 show policy-map interface Field Descriptions — Configured for Multiple Traffic Policing Actions

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

Explicit Congestion Notification show policy-map interface Command Example

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

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

 Serial4/1

  Service-policy output:policy_ecn
        Class-map:prec1 (match-all)
          1000 packets, 125000 bytes
          30 second offered rate 14000 bps, drop rate 5000 bps
          Match:ip precedence 1
          Weighted Fair Queueing
            Output Queue:Conversation 42
            Bandwidth 20 (%)
            Bandwidth 100 (kbps)
            (pkts matched/bytes matched) 989/123625
        (depth/total drops/no-buffer drops) 0/455/0
             exponential weight:9
             explicit congestion notification
             mean queue depth:0

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

```
class    ECN Mark
        pkts/bytes
  0       0/0
  1      43/5375
  2       0/0
  3       0/0
  4       0/0
  5       0/0
  6       0/0
  7       0/0
rsvp      0/0
```

Table 59 describes the significant fields shown in the display.

Table 59 show policy-map interface Field Descriptions — Configured for ECN

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

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

The following sample output of 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 Serial 4/1

Serial4/1

Service-policy output:p1

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

Table 60 describes the significant fields shown in the display.

Table 60 show policy-map interface Field Descriptions — Configured for Class-Based RTP and TCP Header Compression[1]

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

Table 60 show policy-map interface Field Descriptions — Configured for Class-Based RTP and TCP Header Compression[1] (continued)

Field	Description
UDP/RTP Compression	Indicates that RTP header compression has been configured for the class.
Sent total	Count of every packet sent, both compressed packets and full-header packets.
Sent compressed	Count of number of compressed packets sent.
bytes saved	Total number of bytes saved (that is, bytes not needing to be sent).
bytes sent	Total number of bytes sent for both compressed and full-header packets.
efficiency improvement factor	The percentage of increased bandwidth efficiency as a result of header compression. For example, with RTP streams, the efficiency improvement factor can be as much as 2.9 (or 290 percent).
hit ratio	Used mainly for troubleshooting purposes, this is the percentage of packets found in the context database. In most instances, this percentage should be high.
five minute miss rate	The number of new traffic flows found in the last five minutes.
misses/sec max	The average number of new traffic flows found per second, and the highest rate of new traffic flows to date.
rate	The actual traffic rate (in bits per second) after the packets are compressed.

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

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

The following sample output of the **show policy-map interface** command displays the statistics for the Serial2/0 interface, to which a policy map called “policy1” is attached. The discarding action has been specified for all the packets belonging to a class called “c1.” In this example, 32000 bps of traffic is sent (“offered”) to the class and all of them are dropped. Therefore, the drop rate shows 32000 bps.

```
Router# show policy-map interface Serial2/0

 Serial2/0

  Service-policy output: policy1

    Class-map: c1 (match-all)
       10184 packets, 1056436 bytes
       5 minute offered rate 32000 bps, drop rate 32000 bps
       Match: ip precedence 0
       drop
```

Table 61 describes the significant fields shown in the display.

Table 61 show policy-map interface Field Descriptions — Configured for MQC Unconditional Packet Discard[1]

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

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

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

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

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

 Serial3/1

  Service-policy output: mypolicy
```

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

Table 62 describes the significant fields shown in the display.

Table 62 show policy-map interface Field Descriptions — Configured for Percentage-Based Policing and Shaping[1]

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

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

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

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

Serial3/2

  Service-policy output: p1

    Class-map: c1 (match-all)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
      Traffic Shaping
        Target/Average      Byte   Sustain    Excess      Interval  Increment  Adapt
        Rate               Limit  bits/int  bits/int    (ms)      (bytes)    Active
         20 %                      10 (ms)    20 (ms)
        201500/201500       1952   7808       7808        38         976       -

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

Table 63 describes the significant fields shown in the display.

Table 63 show policy-map interface Field Descriptions — Configured for Percentage-Based Policing and Shaping (with Traffic Shaping Enabled)[1]

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

Table 63 show policy-map interface Field Descriptions — Configured for Percentage-Based Policing and Shaping (with Traffic Shaping Enabled)[1] (continued)

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 quality of service (QoS) groups. For more information about the variety of match criteria options that are available, refer to the chapter "Configuring the Modular Quality of Service Command-Line Interface" in the *Cisco IOS Quality of Service Solutions Configuration Guide*, Release 12.2.
Traffic Shaping	Indicates that traffic shaping based on a percentage of bandwidth has been enabled.
Target /Average Rate	Rate (percentage) used for shaping traffic and the number of packets meeting that rate.
Byte Limit	Maximum number of bytes that can be transmitted per interval. Calculated as follows: ((Bc+Be) /8) x 1
Sustain bits/int	Committed burst (Bc) rate.
Excess bits/int	Excess burst (Be) rate.
Interval (ms)	Time interval value in milliseconds (ms).
Increment (bytes)	Number of credits (in bytes) received in the token bucket of the traffic shaper during each time interval.
Adapt Active	Indicates whether adaptive shaping is enabled.
Queue Depth	Current queue depth of the traffic shaper.
Packets	Total number of packets that have entered the traffic shaper system.
Bytes	Total number of bytes that have entered the traffic shaper system.
Packets Delayed	Total number of packets delayed in the queue of the traffic shaper before being transmitted.
Bytes Delayed	Total number of bytes delayed in the queue of the traffic shaper before being transmitted.
Shaping Active	Indicates whether the traffic shaper is active. For example, if a traffic shaper is active, and the traffic being sent exceeds the traffic shaping rate, a "yes" appears in this field.

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

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

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

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

 Ethernet4/1
```

```
Service-policy input: mypolicy

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

Table 64 describes the significant fields shown in the display.

Table 64 show policy-map interface Field Descriptions — Configured for Packet Classification Based on Layer 3 Packet Length[1]

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

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

Enhanced Packet Marking show policy-map interface Example

The sample output of the **show table-map** command shows the contents of a table map called "map 1." In "map1", a "to–from" relationship has been established and a default value has been defined. The fields for establishing the "to–from" mappings are further defined by the policy map in which the table map will be configured. (Configuring a policy map is the next logical step after creating a table map.)

For instance, a precedence or DSCP value of 0 could be mapped to a class of service (CoS) value of 1, or vice versa, depending on the how the values are defined in the table map. Any values not explicitly defined in a "to–from" relationship will be set to a default value.

The following sample output of the **show table-map** command displays the contents of a table map called "map1". In this table map, a packet-marking value of 0 is mapped to a packet-marking value of 1. All other packet-marking values are mapped to the default value 3.

```
Router# show table-map map1

 Table Map map1
 from 0 to 1
 default 3
```

Table 65 describes the fields shown in the display.

Table 65 show policy-map interface Field Descriptions — Configured for Enhanced Packet Marking

Field	Description
Table Map	The name of the table map being displayed.
from, to	The values of the "to–from" relationship established by the **table-map** (value mapping) command and further defined by the policy map in which the table map will be configured.
default	The default action to be used for any values not explicitly defined in a "to–from" relationship by the **table-map** (value mapping) command. If a default action is not specified in the table-map (value mapping) command, the default action is "copy".

Related Commands

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

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 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 qdm status

To view the status of the Quality of Service Device Manager (QDM) clients connected to the router, use the **show qdm status** command in EXEC mode.

show qdm status

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 12.1(1)E	This command was introduced.
Release 12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.

Usage Guidelines

Use the **show qdm status** command to obtain the following information:

- Number of connected QDM clients
- Client IDs of the connected QDM clients
- Version of the QDM client software
- IP addresses of the connected QDM clients

Examples

The following example illustrates the **show qdm status** output when two QDM clients are connected to the router:

```
Router# show qdm status

Number of QDM Clients :2
QDM Client v1.0(0.13)-System_1 @ 172.16.0.0 (id:30)
     connected since 09:22:36 UTC Wed Mar 15 2000
QDM Client v1.0(0.12)-System_2 @ 172.31.255.255 (id:29)
     connected since 17:10:23 UTC Tue Mar 14 2000
```

Related Commands

Command	Description
disconnect qdm	Disconnects a QDM client.

show queue

To display the contents of packets inside a queue for a particular interface or virtual circuit (VC), use the **show queue** command in privileged EXEC mode.

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	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 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 **atm vc-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

Privileged EXEC

Command History

Release	Modification
10.2	This command was introduced.

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 **show queue** command arguments to display output for a PVC only on Enhanced ATM port adapters (PA-A3) that support per-VC queueing.

Examples

The following examples show sample output when the **show queue** command is entered and either weighted fair queueing (WFQ), WRED, or flow-based WRED are configured.

WFQ Example

The following is sample output from the **show queue** 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
```

Table 66 describes the significant fields shown in the display.

Table 66 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.
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.

Table 66 show queue Field Descriptions for WFQ (continued)

Field	Description
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.

Flow-Based WRED Example

The following is sample output from the **show queue** 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
```

Table 67 describes the significant fields shown in the display.

Table 67 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.

Table 67 show queue Field Descriptions for Flow-Based WRED (continued)

Field	Description
id	Packet ID.
ttl	Time to live count.
prot	Layer 4 protocol number.
data	Packet data.

WRED Example

The following is sample output from the **show queue** command issued for serial interface 3 on which WRED is configured. The output has been truncated to show only 2 of the 24 packets.

```
Router# show queue Serial3

   Output queue for Serial3 is 24/0

   Packet 1, linktype:ip, length:118, flags:0x88
     source:10.1.3.25, destination:10.1.2.2, id:0x0000, ttl:59,
     TOS:192 prot:17, source port 1, destination port 515
       data:0x0001 0x0203 0x0405 0x0607 0x0809 0x0A0B 0x0C0D
             0x0E0F 0x1011 0x1213 0x1415 0x1617 0x1819 0x1A1B

   Packet 2, linktype:ip, length:118, flags:0x88
     source:10.1.3.26, destination:10.1.2.2, id:0x0000, ttl:59,
     TOS:224 prot:17, source port 1, destination port 515
       data:0x0001 0x0203 0x0405 0x0607 0x0809 0x0A0B 0x0C0D
             0x0E0F 0x1011 0x1213 0x1415 0x1617 0x1819 0x1A1B
```

Related Commands

Command	Description
atm vc-per-vp	Sets the maximum number of VCIs to support per VPI.
custom-queue-list	Assigns a custom queue list to an interface.
fair-queue (class-default)	Specifies the number of dynamic queues to be reserved for use by the class-default class as part of the default class policy.
fair-queue (WFQ)	Enables WFQ for an interface.
priority-group	Assigns the specified priority list to an interface.
random-detect (interface)	Enables WRED or DWRED.
random-detect flow	Enables flow-based WRED.
show frame-relay pvc	Displays information and statistics about WFQ for a VIP-based interface.
show queueing	Lists all or selected configured queueing strategies.

show queueing

To list all or selected configured queueing strategies, use the **show queueing** command in 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.

Defaults

If no keyword is entered, this command shows the configuration of all interfaces.

Command Modes

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 integrated into Cisco IOS Release 12.1(2)T. This command was modified to include information about the Frame Relay PVC Interface Priority Queueing (FR PIPQ) feature.

Examples

FR PIPQ Example

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:
```

Weighted Fair Queueing Example

The following is sample output from the **show queueing** command. There are two active conversations in serial interface 0. Weighted fair queueing (WFQ) ensures that both of these IP data streams—both using TCP—receive equal bandwidth on the interface while they have messages in the pipeline, even though more FTP data is in the queue than remote-procedure call (RCP) data.

```
Router# show queueing

Current fair queue configuration:
Interface           Discard     Dynamic      Reserved
                    threshold   queue count  queue count
  Serial0             64          256          0
  Serial1             64          256          0
  Serial2             64          256          0
  Serial3             64          256          0

Current priority queue configuration:
List   Queue  Args
1      high   protocol cdp
2      medium interface Ethernet1

Current custom queue configuration:

Current random-detect configuration:
  Serial5
    Queueing strategy:random early detection (WRED)
    Exp-weight-constant:9 (1/512)
    Mean queue depth:40
```

```
Class   Random        Tail    Minimum    Maximum     Mark
          drop        drop  threshold  threshold  probability
  0       1401        9066         20         40      1/10
  1          0           0         22         40      1/10
  2          0           0         24         40      1/10
  3          0           0         26         40      1/10
  4          0           0         28         40      1/10
  5          0           0         31         40      1/10
  6          0           0         33         40      1/10
  7          0           0         35         40      1/10
  rsvp       0           0         37         40      1/10
```

Custom Queueing Example

The following is sample output from the **show queueing custom** command:

```
Router# show queueing custom

Current custom queue configuration:
List   Queue  Args
3      10     default
3      3      interface Tunnel3
3      3      protocol ip
3      3      byte-count 444 limit 3
```

Flow-Based WRED Example

The following is sample output from the **show queueing random-detect** command. The output shows that the interface is configured for flow-based WRED to ensure fair packet drop among flows. The **random-detect flow average-depth-factor** command was used to configure a scaling factor of 8 for this interface. The scaling factor is used to scale the number of buffers available per flow and to determine the number of packets allowed in the output queue of each active flow before the queue is susceptible to packet drop. The maximum flow count for this interface was set to 16 by the **random-detect flow count** command.

```
Router# show queueing random-detect

    Current random-detect configuration:
      Serial1
        Queueing strategy:random early detection (WRED)
        Exp-weight-constant:9 (1/512)
        Mean queue depth:29
        Max flow count:16       Average depth factor:8
        Flows (active/max active/max):39/40/16

        Class   Random        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
```

DWRED Example

The following is sample output from the **show queueing random-detect** command for DWRED:

```
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
```

Table 68 describes the significant fields shown in the display.

Table 68 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.
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.

Table 68 show queueing Field Descriptions (continued)

Field	Description
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.
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 or a virtual circuit (VC), use the **show queueing interface** command in privileged EXEC mode.

show queueing interface *interface-number* [**vc** [[*vpi*/] *vci*]]

Syntax Description

interface-number	Specifies the number of the interface.
vc	(Optional) Shows the weighted fair queueing (WFQ) and Weighted Random Early Detection (WRED) parameters associated with a specific 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) 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 Modes

Privileged EXEC

Command History

Release	Modification
11.1(22)CC	This command was introduced.

Examples

The following is sample output from the **show queueing interface** command:

```
Router# show queueing interface atm2/0

  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
```

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 (interface)	Enables WRED or DWRED.
random-detect (per VC)	Enables per-VC WRED or per-VC DWRED.
random-detect flow	Enables flow-based WRED.
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 queueing	Lists all or selected configured queueing strategies.

show table-map

To display the configuration of a specified table map or all table maps, use the **show table-map** command in EXEC mode.

show table-map *table-map-name*

Syntax Description

table-map-name	Name of table map used to map one packet-marking value to another. The name can be a maximum of 64 alphanumeric characters.

Defaults

All existing table map configurations are displayed.

Command Modes

EXEC

Command History

Release	Modification
12.2(13)T	This command was introduced.

Examples

The sample output of the **show table-map** command shows the contents of a table map called "map 1". In "map1", a "to–from" relationship has been established and a default value has been defined. The fields for establishing the "to–from" mappings are further defined by the policy map in which the table map will be configured. (Configuring a policy map is the next logical step after creating a table map.)

For instance, a precedence or differentiated services code point (DSCP) value of 0 could be mapped to a class of service (CoS) value of 1, or vice versa, depending on the how the values are defined in the table map. Any values not explicitly defined in a "to–from" relationship will be set to a default value.

The following sample output of the **show table-map** command displays the contents of a table map called "map1". In this table map, a packet-marking value of 0 is mapped to a packet-marking value of 1. All other packet-marking values are mapped to the default value 3.

```
Router# show table-map map1

 Table Map map1
 from 0 to 1
 default 3
```

Table 69 describes the fields shown in the display.

Table 69 show table-map Field Descriptions

Field	Description
Table Map	The name of the table map being displayed.
from, to	The values of the “to–from” relationship established by the **table-map** (value mapping) command and further defined by the policy map in which the table map will be configured.
default	The default action to be used for any values not explicitly defined in a “to–from” relationship by the **table-map** (value mapping) command. If a default action is not specified in the table-map (value mapping) command, the default action is “copy”.

Related Commands

Command	Description
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
show policy-map	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.
table-map (value mapping)	Creates and configures a mapping table for mapping and converting one packet-marking value to another.

show tech-support rsvp

To generate a report of all Resource Reservation Protocol (RSVP)-related information, use the **show tech-support rsvp** command in privileged EXEC mode.

show tech-support rsvp

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

This command is not required for normal use of the operating system. This command is useful when you contact technical support personnel with questions regarding RSVP. The **show tech-support rsvp** command generates a series of reports that can be useful to technical support personnel attempting to solve problems.

Any issues or caveats that apply to the **show tech-support** command also apply to this command. For example, the enable password, if configured, is not displayed in the output of the **show running-config** command.

The **show tech-support rsvp** command is equivalent to issuing the following commands:

- **show ip rsvp installed**
- **show ip rsvp interface**
- **show ip rsvp neighbor**
- **show ip rsvp policy cops**
- **show ip rsvp reservation**
- **show ip rsvp sender**
- **show running-config**
- **show version**

These commands are documented in various chapters of this book. Refer to the displays and descriptions for the individual commands for information about the **show tech-support rsvp** command display.

show traffic-shape

To display the current traffic-shaping configuration, use the **show traffic-shape** command in EXEC mode.

show traffic-shape [*interface-type interface-number*]

Syntax Description

interface-type	(Optional) The type of the interface. If no interface is specified, traffic-shaping details for all configured interfaces are shown.
interface-number	(Optional) The number of the interface.

Command Modes

EXEC

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

You must have first enabled traffic shaping using the **traffic-shape rate**, **traffic-shape group**, or **frame-relay traffic-shaping** command to display traffic-shaping information.

Examples

The following is sample output from the **show traffic-shape** command:

```
Router# show traffic-shape

Interface   Fa0/0
       Access Target    Byte  Sustain   Excess    Interval  Increment Adapt
VC     List   Rate      Limit bits/int  bits/int  (ms)      (bytes)   Active
-             1000000   6250  25000     25000     25        3125      -
```

Table 70 describes the significant fields shown in the display.

Table 70 show traffic-shape Field Descriptions

Field	Description
Interface	Interface type and number.
VC	Virtual circuit. **Note** If you configure traffic shaping at a VC level instead of an interface level, a number appears in this field.
Access List	Number of the access list, if one is configured.
Target Rate	Rate that traffic is shaped to, in bits per second.
Byte Limit	Maximum number of bytes sent per internal interval.
Sustain bits/int	Configured sustained bits per interval.
Excess bits/int	Configured excess bits in the first interval.

Table 70 show traffic-shape Field Descriptions (continued)

Field	Description
Interval (ms)	Interval (in milliseconds) being used internally, which may be smaller than the committed burst divided by the committed information rate, if the router determines that traffic flow will be more stable with a smaller configured interval.
Increment (bytes)	Number of bytes that will be sustained per internal interval.
Adapt Active	Contains "BECN" if Frame Relay has backward explicit congestion notification (BECN) adaptation configured.

Related Commands

Command	Description
frame-relay cir	Specifies the incoming or outgoing committed information rate (CIR) for a Frame Relay virtual circuit.
frame-relay traffic-rate	Configures all the traffic-shaping characteristics of a virtual circuit (VC) in a single command.
frame-relay traffic-shaping	Enables both traffic shaping and per-VC queueing for all PVCs and SVCs on a Frame Relay interface.
show traffic-shape queue	Displays information about the elements queued by traffic shaping at the interface level or the DLCI level.
show traffic-shape statistics	Displays the current traffic-shaping statistics.
traffic-shape adaptive	Configures a Frame Relay subinterface to estimate the available bandwidth when BECN signals are received.
traffic-shape fecn-adapt	Replies to messages with the FECN bit (which are set with TEST RESPONSE messages with the BECN bit set).
traffic-shape group	Enables traffic shaping based on a specific access list for outbound traffic on an interface.
traffic-shape rate	Enables traffic shaping for outbound traffic on an interface.

show traffic-shape queue

To display information about the elements queued by traffic shaping at the interface level or the data-link connection identifier (DLCI) level, use the **show traffic-shape queue** command in EXEC mode.

show traffic-shape queue [*interface-number* [**dlci** *dlci-number*]]

Syntax Description

interface-number	(Optional) The number of the interface.
dlci	(Optional) The specific DLCI for which you wish to display information about queued elements.
dlci-number	(Optional) The number of the DLCI.

Command Modes

EXEC

Command History

Release	Modification
11.2	This command was introduced.
12.0(3)XG	This command was integrated into Cisco IOS Release 12.0(3)XG. The *dlci* argument was added.
12.0(4)T	This command was integrated into Cisco IOS Release 121.0(4)T. The *dlci* argument was added.
12.0(5)T	This command was integrated into Cisco IOS Release 12.0(5)T. This command was modified to include information on the special voice queue that is created using the **queue** keyword of the **frame-relay voice bandwidth** command.

Usage Guidelines

When no parameters are specified with this command, the output displays information for all interfaces and DLCIs containing queued elements. When a specific interface and DLCI are specified, information is displayed about the queued elements for that DLCI only.

Examples

The following is sample output for the **show traffic-shape queue** command when weighted fair queueing is configured on the map class associated with DLCI 16:

```
Router# show traffic-shape queue Serial1/1 dlci 16

Traffic queued in shaping queue on Serial1.1 dlci 16
  Queueing strategy: weighted fair
  Queueing Stats: 1/600/64/0 (size/max total/threshold/drops)
     Conversations  0/16 (active/max total)
     Reserved Conversations 0/2 (active/allocated)
   (depth/weight/discards) 1/4096/0
  Conversation 5, linktype: ip, length: 608

source: 172.21.59.21, destination: 255.255.255.255, id: 0x0006, ttl: 255,
  TOS: 0 prot: 17, source port 68, destination port 67
```

The following is sample output for the **show traffic-shape queue** command when priority queueing is configured on the map class associated with DLCI 16:

```
Router# show traffic-shape queue Serial1/1 dlci 16

Traffic queued in shaping queue on Serial1.1 dlci 16
  Queueing strategy: priority-group 4
  Queueing Stats: low/1/80/0 (queue/size/max total/drops)

Packet 1, linktype: cdp, length: 334, flags: 0x10000008
```

The following is sample output for the **show traffic-shape queue** command when first-come, first-serve queueing is configured on the map class associated with DLCI 16:

```
Router# show traffic-shape queue Serial1/1 dlci 16

Traffic queued in shaping queue on Serial1.1 dlci 16
  Queueing strategy: fcfs
  Queueing Stats: 1/60/0 (size/max total/drops)

Packet 1, linktype: cdp, length: 334, flags: 0x10000008
```

The following is sample output for the **show traffic-shape queue** command displaying statistics for the special queue for voice traffic that is created automatically when the **frame-relay voice bandwidth** command is entered:

```
Router# show traffic-shape queue serial 1 dlci 45

 Voice queue attached to traffic shaping queue on Serial1 dlci 45
 ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    Voice Queueing Stats: 0/100/0 (size/max/dropped)
    ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
 Traffic queued in shaping queue on Serial1 dlci 45
   Queueing strategy: weighted fair
   Queueing Stats: 0/600/64/0 (size/max total/threshold/drops)
      Conversations  0/16 (active/max total)
      Reserved Conversations 0/2 (active/allocated)
```

Table 71 describes the significant fields shown in the display.

Table 71 show traffic-shape queue Field Descriptions

Field	Description
Queueing strategy	When Frame Relay Traffic Shaping (FRTS) is configured, the queueing type can be weighted fair, custom-queue, priority-group, or fcfs (first-come, first-serve), depending on what is configured on the Frame Relay map class for this DLCI. The default is fcfs for FRTS. When generic traffic shaping is configured, the only queueing type available is weighted fair queueing (WFQ).
Queueing Stats	Statistics for the configured queueing strategy, as follows: • size—Current size of the queue. • max total—Maximum number of packets of all types that can be queued in all queues. • threshold—For WFQ, the number of packets in the queue after which new packets for high-bandwidth conversations will be dropped. • drops—Number of packets discarded during this interval.

Table 71 show traffic-shape queue Field Descriptions (continued)

Field	Description
Conversations active	Number of currently active conversations.
Conversations max total	Maximum allowed number of concurrent conversations.
Reserved Conversations active	Number of currently active conversations reserved for voice.
Reserved Conversations allocated	Maximum configured number of conversations reserved.
depth	Number of packets currently queued.
weight	Number used to classify and prioritize the packet.
discards	Number of packets discarded from queues.
Packet	Number of queued packet.
linktype	Protocol type of the queued packet. (cdp = Cisco Discovery Protocol)
length	Number of bytes in the queued packet.
flags	Number of flag characters in the queued packet.
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. Refer to RFC 943 for a list of protocol numbers. (17 = User Datagram Protocol (UDP))
source port	Port number of source port.
destination port	Port number of destination port.

Related Commands

Command	Description
show frame-relay fragment	Displays Frame Relay fragmentation details.
show frame-relay pvc	Displays statistics about PVCs for Frame Relay interfaces.
show frame-relay vofr	Displays details about FRF.11 subchannels being used on VoFR DLCIs.
show traffic-shape	Displays the current traffic-shaping configuration.
show traffic-shape statistics	Displays the current traffic-shaping statistics.

show traffic-shape statistics

To display the current traffic-shaping statistics, use the **show traffic-shape statistics** command in EXEC mode.

show traffic-shape statistics [*interface-type interface-number*]

Syntax Description

interface-type	(Optional) The type of the interface. If no interface is specified, traffic-shaping statistics for all configured interfaces are shown.
interface-number	(Optional) The number of the interface.

Command Modes

EXEC

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

You must have first enabled traffic shaping using the **traffic-shape rate**, **traffic-shape group**, or **frame-relay traffic-shaping** command to display traffic-shaping information.

Examples

The following is sample output from the **show traffic-shape statistics** command:

```
Router# show traffic-shape statistics

          Access Queue     Packets    Bytes     Packets   Bytes     Shaping
I/F       List   Depth                          Delayed   Delayed   Active
Et0       101    0         2          180       0         0         no
Et1              0         0          0         0         0         no
```

Table 72 describes the significant fields shown in the display.

Table 72 show traffic-shape statistics Field Descriptions

Field	Description
I/F	Interface.
Access List	Number of the access list.
Queue Depth	Number of messages in the queue.
Packets	Number of packets sent through the interface.
Bytes	Number of bytes sent through the interface.
Packets Delayed	Number of packets sent through the interface that were delayed in the traffic-shaping queue.

Table 72 show traffic-shape statistics Field Descriptions (continued)

Field	Description
Bytes Delayed	Number of bytes sent through the interface that were delayed in the traffic-shaping queue.
Shaping Active	Contains "yes" when timers indicate that traffic shaping is occurring and "no" if traffic shaping is not occurring.

Related Commands

Command	Description
frame-relay traffic-shaping	Enables both traffic shaping and per-VC queueing for all PVCs and SVCs on a Frame Relay interface.
show interfaces	Displays statistics for all interfaces configured on the router or access server.
show ip rsvp neighbor	Displays RSVP-related interface information.
traffic-shape adaptive	Configures a Frame Relay subinterface to estimate the available bandwidth when BECN signals are received.
traffic-shape group	Enables traffic shaping based on a specific access list for outbound traffic on an interface.
traffic-shape rate	Enables traffic shaping for outbound traffic on an interface.

svc-bundle

To create or modify a member of a switched virtual circuit (SVC) bundle, use the **svc-bundle** command in SVC-bundle configuration mode. To remove an SVC bundle member from the bundle, use the **no** form of this command.

svc-bundle *svc-handle*

no svc-bundle *svc-handle*

Syntax Description

svc-handle	Unique name for the SVC in the router.

Defaults

No SVCs are members of an SVC bundle.

Command Modes

SVC-bundle configuration

Command History

Release	Modification
12.2(4)T	This command was introduced.

Usage Guidelines

Using this command will cause the system to enter SVC-bundle member configuration mode, in which you can configure characteristics of the member such as precedence, variable bit rate (VBR) traffic shaping, unspecified bit rate (UBR) traffic shaping, UBR+ traffic shaping, an idle timeout, and bumping conditions.

Examples

The following example creates a member of an SVC bundle named "five":

```
svc-bundle five
```

table-map (value mapping)

To create and configure a mapping table for mapping and converting one packet-marking value to another, use the **table-map** (value mapping) command in global configuration mode. To disable the use of this table map, use the **no** form of this command.

table-map *table-map-name* **map from** *from-value* **to** *to-value* [**default** *default-value-or-action*]

no table-map *table-map-name* **map from** *from-value* **to** *to-value* [**default** *default-value-or-action*]

Syntax Description

table-map-name	Name of table map to be created. The name can be a maximum of 64 alphanumeric characters.
map from	Indicates that a "map from" value will be used.
from-value	The "map from" value of the packet-marking category. The value range varies according to the packet-marking category from which you want to map and convert. For more information, see the "Usage Guidelines" section below.
to	Indicates that a "map to" value will be used.
to-value	The "map to" value of the packet-marking category. The value range varies according to the packet-marking category to which you want to map and convert. For more information, see the "Usage Guidelines" section below.
default	(Optional) Indicates that a default value or action will be used.
default-value-or-action	(Optional) The default value or action to be used if a "to–from" relationship has not been explicitly configured. Default actions are "ignore" and "copy". If neither action is specified, "copy" is used.

Defaults

The **default** keyword and *default-value-or-action* argument sets the default value (or action) to be used if a value if not explicitly designated.

If you configure a table map but you do not specify a *default-value-or-action* argument for the **default** keyword, the default action is "copy".

Command Modes

Global configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

This command allows you to create a mapping table. The mapping table, a type of conversion chart, is used for establishing a "to–from" relationship between packet-marking types or categories. For example, a mapping table can be used to establish a "to–from" relationship between the following packet-marking categories:

- Class of service (CoS)
- Precedence

- Differentiated services code point (DSCP)
- Quality of service (QoS) group
- Multiprotocol Label Switching (MPLS) experimental (EXP) imposition
- MPLS EXP topmost

When configuring the table map, you must specify the packet-marking values to be used in the conversion. The values you can enter vary by packet-marking category.

Table 73 lists the valid value ranges you can enter for each packet-marking category.

Table 73 Valid Value Ranges

Packet-Marking Category	Value Ranges
CoS	Specific IEEE 802.1Q number in the range from 0 to 7.
Precedence	Number in the range from 0 to 7.
DSCP	Number in the range from 0 to 63.
QoS Group	Number in the range from 0 to 99.
MPLS EXP imposition	Number in the range from 0 to 7.
MPLS EXP topmost	Number in the range from 0 to 7.

Examples

In the following example, the **table-map** (value mapping) command has been configured to create a table map called “map1”. In “map1”, two “to–from” relationships have been established and a default value has been defined. The fields for establishing the “to–from” mappings are further defined by the policy map in which the table map will be configured. (Configuring a policy map is the next logical step after creating a table map.)

For instance, a precedence or DSCP value of 0 could be mapped to a CoS value of 0, or vice versa, depending on the how the table map is configured. Any values not explicitly defined in a “to–from” relationship will be set to a default value.

```
Router(config)# table-map map1
Router(config-tablemap)# map from 0 to 0
Router(config-tablemap)# map from 2 to 1
Router(config-tablemap)# default 3
Router(config-tablemap)# end
```

Related Commands

Command	Description
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
show policy-map	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 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 table-map	Displays the configuration of a specified table map or all table maps.

traffic-shape adaptive

To configure a Frame Relay subinterface to estimate the available bandwidth when backward explicit congestion notification (BECN) signals are received, use the **traffic-shape adaptive** interface configuration command in interface configuration mode. To disregard the BECN signals and not estimate the available bandwidth, use the **no** form of this command.

traffic-shape adaptive *bit-rate*

no traffic-shape adaptive

Syntax Description

bit-rate	Lowest bit rate that traffic is shaped to, in bits per second. The default *bit rate* value is 0.

Defaults

This command is not enabled by default.

Command Modes

Interface configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

This command specifies the boundaries in which traffic will be shaped when BECN signals are received. You must enable traffic shaping on the interface with the **traffic-shape rate** or **traffic-shape group** command before you can use the **traffic-shape adaptive** command.

The bit rate specified for the **traffic-shape rate** command is the upper limit, and the bit rate specified for the **traffic-shape adaptive** command is the lower limit to which traffic is shaped when BECN signals are received on the interface. The rate actually shaped to will be between these two bit rates.

You should configure this command and the **traffic-shape fecn-adapt** command on both ends of the connection to ensure adaptive traffic shaping over the connection, even when traffic is flowing primarily in one direction. The **traffic-shape fecn-adapt** command configures the router to reflect forward explicit congestion notification (FECN) signals as BECN signals.

Examples

The following example configures traffic shaping on serial interface 0.1 with an upper limit of 128 kbps and a lower limit of 64 kbps. This configuration allows the link to run from 64 to 128 kbps, depending on the congestion level.

```
interface serial 0
 encapsulation-frame-relay
interface serial 0.1
 traffic-shape rate 128000
 traffic-shape adaptive 64000
 traffic-shape fecn-adapt
```

Related Commands

Command	Description
show traffic-shape	Displays the current traffic-shaping configuration.
show traffic-shape statistics	Displays the current traffic-shaping statistics.
traffic-shape fecn-adapt	Replies to messages with the FECN bit (which are set with TEST RESPONSE messages with the BECN bit set).
traffic-shape group	Enables traffic shaping based on a specific access list for outbound traffic on an interface.
traffic-shape rate	Enables traffic shaping for outbound traffic on an interface.

traffic-shape fecn-adapt

To reply to messages with the forward explicit congestion notification (FECN) bit (which are sent with TEST RESPONSE messages with the BECN bit set), use the **traffic-shape fecn-adapt** command in interface configuration mode. To stop backward explicit congestion notification (BECN) signal generation, use the **no** form of this command.

traffic-shape fecn-adapt

no traffic-shape fecn-adapt

Syntax Description

This command has no arguments or keywords.

Defaults

Traffic shaping is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

Enable traffic shaping on the interface with the **traffic-shape rate** or **traffic-shape group** command. FECN is available only when traffic shaping is configured.

Use this command to reflect FECN bits as BECN bits. Reflecting FECN bits as BECN bits notifies the sending DTE that it is transmitting at a rate too fast for the DTE to handle. Use the **traffic-shape adaptive** command to configure the router to adapt its transmission rate when it receives BECN signals.

You should configure this command and the **traffic-shape adaptive** command on both ends of the connection to ensure adaptive traffic shaping over the connection, even when traffic is flowing primarily in one direction.

Examples

The following example configures traffic shaping on serial interface 0.1 with an upper limit of 128 kbps and a lower limit of 64 kbps. This configuration allows the link to run from 64 to 128 kbps, depending on the congestion level. The router reflects FECN signals as BECN signals.

```
interface serial 0
 encapsulation-frame-relay
interface serial 0.1
 traffic-shape rate 128000
 traffic-shape adaptive 64000
 traffic-shape fecn-adapt
```

Related Commands

Command	Description
show traffic-shape	Displays the current traffic-shaping configuration.
show traffic-shape statistics	Displays the current traffic-shaping statistics.
traffic-shape adaptive	Configures a Frame Relay subinterface to estimate the available bandwidth when BECN signals are received.
traffic-shape group	Enables traffic shaping based on a specific access list for outbound traffic on an interface.
traffic-shape rate	Enables traffic shaping for outbound traffic on an interface.

traffic-shape group

To enable traffic shaping based on a specific access list for outbound traffic on an interface, use the **traffic-shape group** command in interface configuration mode. To disable traffic shaping on the interface for the access list, use the **no** form of this command.

traffic-shape group *access-list bit-rate* [*burst-size* [*excess-burst-size*]]

no traffic-shape group *access-list*

Syntax Description

access-list	Number of the access list that controls the packets that traffic shaping is applied to on the interface. Access list numbers can be numbers from 1 to2,699.
bit-rate	Bit rate that traffic is shaped to, in bits per second. This is the access bit rate that you contract with your service provider, or the service levels you intend to maintain. Bit rates can be numbers in the range of 8,000 to 100,000,000 bps.
burst-size	(Optional) Sustained number of bits that can be sent per interval. On Frame Relay interfaces, this is the Committed Burst size contracted with your service provider. Valid entries are numbers in the range of 0 to 100,000,000.
excess-burst-size	(Optional) Maximum number of bits that can exceed the burst size in the first interval in a congestion event. On Frame Relay interfaces, this is the Excess Burst size contracted with your service provider. Valid entries are numbers in the range of 0 to 100,000,000. The default is equal to the *burst-size* argument.

Defaults

Traffic shaping is not on by default.

Command Modes

Interface configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

Generic traffic shaping is not supported on ISDN and dialup interfaces. Is is also not supported on nongeneric routing encapsulation tunnel interfaces. Traffic shaping is not supported with flow switching.

Traffic shaping uses queues to limit surges that can congest a network. Data is buffered and then sent into the network in regulated amounts to ensure that traffic will fit within the promised traffic envelope for the particular connection.

The **traffic-shape group** command allows you to specify one or more previously defined access list to shape traffic on the interface. You must specify one **traffic-shape group** command for each access list on the interface.

The **traffic-shape group** command supports both standard and extended access lists.

Use traffic shaping if you have a network with differing access rates or if you are offering a subrate service. You can configure the values according to your contract with your service provider or the service levels you intend to maintain.

An interval is calculated as follows:

- If the *burst-size* is not equal to zero, the interval is the *burst-size* divided by the *bit-rate*.
- If the *burst-size* is zero, the interval is the *excess-burst-size* divided by the *bit-rate*.

Traffic shaping is supported on all media and encapsulation types on the router. To perform traffic shaping on Frame Relay virtual circuits, you can also use the **frame-relay traffic-shaping** command. For more information on Frame Relay Traffic Shaping, refer to the "Configuring Frame Relay" chapter in the *Cisco IOS Wide-Area Networking Configuration Guide*.

If traffic shaping is performed on a Frame Relay network with the **traffic-shape rate** command, you can also use the **traffic-shape adaptive** command to specify the minimum bit rate to which the traffic is shaped.

Examples

The following example enables traffic that matches access list 101 to be shaped to a certain rate and traffic matching access list 102 to be shaped to another rate on the interface:

```
interface serial 1
 traffic-shape group 101 128000 16000 8000
 traffic-shape group 102 130000 10000 1000
```

Related Commands

Command	Description
access-list (IP Standard)	Defines a standard IP access list.
show traffic-shape	Displays the current traffic-shaping configuration.
show traffic-shape statistics	Displays the current traffic-shaping statistics.
traffic-shape adaptive	Configures a Frame Relay subinterface to estimate the available bandwidth when BECN signals are received.
traffic-shape fecn-adapt	Replies to messages with the FECN bit (which are set with TEST RESPONSE messages with the BECN bit set).
traffic-shape rate	Enables traffic shaping for outbound traffic on an interface.

traffic-shape rate

To enable traffic shaping for outbound traffic on an interface, use the **traffic-shape rate** command in interface configuration mode. To disable traffic shaping on the interface, use the **no** form of this command.

traffic-shape rate *bit-rate* [*burst-size* [*excess-burst-size*][*buffer-limit*]

no traffic-shape rate

Syntax Description

bit-rate	Bit rate that traffic is shaped to, in bits per second. This is the access bit rate that you contract with your service provider, or the service levels you intend to maintain. Bit rates can be in the range of 8,000 to 100,000,000 bps.
burst-size	(Optional) Sustained number of bits that can be sent per interval. On Frame Relay interfaces, this is the Committed Burst size contracted with your service provider. Valid entries are numbers in the range of 0 to 100,000,000.
excess-burst-size	(Optional) Maximum number of bits that can exceed the burst size in the first interval in a congestion event. On Frame Relay interfaces, this is the Excess Burst size contracted with your service provider. Valid entries are numbers in the range of 0 to 100,000,000. The default is equal to the *burst-size* argument.
buffer-limit	(Optional) Maximum buffer limit in bps. Valid entries are numbers in the range of 0 to 4,096.

Defaults

Traffic shaping is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

Generic traffic shaping is not supported on ISDN and dialup interfaces. Is is also not supported on nongeneric routing encapsulation tunnel interfaces. Traffic shaping is not supported with flow switching.

Traffic shaping uses queues to limit surges that can congest a network. Data is buffered and then sent into the network in regulated amounts to ensure that traffic will fit within the promised traffic envelope for the particular connection.

Use traffic shaping if you have a network with differing access rates or if you are offering a subrate service. You can configure the values according to your contract with your service provider or the service levels you intend to maintain.

An interval is calculated as follows:

- If the *burst-size* is not equal to zero, the interval is the *burst-size* divided by the *bit-rate*.
- If the *burst-size* is zero, the interval is the *excess-burst-size* divided by the *bit-rate*.

Traffic shaping is supported on all media and encapsulation types on the router. To perform traffic shaping on Frame Relay virtual circuits, you can also use the **frame-relay traffic-shaping** command. For more information on Frame Relay Traffic Shaping, refer to the "Configuring Frame Relay" chapter in the *Cisco IOS Wide-Area Networking Configuration Guide*.

If traffic shaping is performed on a Frame Relay network with the **traffic-shape rate** command, you can also use the **traffic-shape adaptive** command to specify the minimum bit rate to which the traffic is shaped.

Examples

The following example enables traffic shaping on serial interface 0 using the bandwidth required by the service provider:

```
interface serial 0
 traffic-shape rate 128000 16000 8000
```

Related Commands

Command	Description
show traffic-shape	Displays the current traffic-shaping configuration.
show traffic-shape statistics	Displays the current traffic-shaping statistics.
traffic-shape adaptive	Configures a Frame Relay subinterface to estimate the available bandwidth when BECN signals are received.
traffic-shape fecn-adapt	Replies to messages with the FECN bit (which are set with TEST RESPONSE messages with the BECN bit set).
traffic-shape group	Enables traffic shaping based on a specific access list for outbound traffic on an interface.

tx-ring-limit

To limit the number of packets that can be used on a transmission ring on the digital subscriber line (DSL) WAN interface card (WIC) or interface, use the **tx-ring-limit** command in interface configuration mode. To not limit the number of packets that can be used on a transmission ring on a DSL WIC or interface, use the **no** form of this command.

tx-ring-limit *ring-limit*

no tx-ring-limit *ring-limit*

Syntax Description

ring-limit	Specifies the maximum number of allowable packets that can be placed on the transmission ring. Valid entries can be numbers from 1 to 32767. The default value is 60. On a Cisco 2600 or Cisco 3600 series router, the value can be changed to 3. (The only permitted values are 3 or 60.) A transmission (tx) ring setting of 3 is required for latency-critical traffic.

Defaults

The default value of the *ring-limit* argument is 60.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(7)XE1	This command was introduced.
12.0(9)S	This command was integrated into Cisco IOS Release 12.0 S.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines

When the buffering is reduced by configuring the tx ring limit, the delay experienced by voice packets is reduced by a combination of the tx ring and low latency queueing (LLQ) mechanism.

This command allows you to reduce the size of the first-in, first-out FIFO queue. Reducing the size of the transmit ring in the queue has two benefits:

- It reduces the amount of time packets wait in the FIFO queue before being segmented.
- It accelerates the use of quality of service (QoS) in the Cisco IOS software.

Note For the Cisco IOS 12.2(13)T release, the **tx-ring-limit** command is not supported on the Cisco 1700 series router.

Examples

The following example configures the transmission ring limit to three packets on an ATM interface:

```
Router(config)# interface atm 1/0/0
Router(config-if)# atm pvc 32 0 32 aal5snap 10000 8000 2000 tx-ring-limit 3
```

The following example configures the transmission ring limit to 60 packets on an ATM permanent virtual circuit (PVC) subinterface:

```
Router(config)# interface ATM1/0/0.1 point-to-point
Router(config-subif)# pvc 2/200
Router(config-if-atm-vc)# tx-ring-limit 60
```

Related Commands

Command	Description
show atm vc	Displays all ATM PVCs and traffic information.
tx-queue-limit	Controls the number of transmit buffers available to a specified interface or the MCI and SCI cards.

vc-hold-queue

To configure the per-virtual circuit (VC) hold queue on an ATM adapter, use the **vc-hold-queue** command in interface configuration mode. To return to the default value of the per-VC hold queue, use the **no** form of this command.

vc-hold-queue *number-of-packets*

no vc-hold-queue *number-of-packets*

Syntax Description

number-of-packets	Specifies number of packets that can be configured for the per-VC hold queue. Number of packets can be a minimum of 5 to a maximum of 1024.

Defaults

The default value of the hold queue is set by the queueing mechanism in use.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(5)T	This command was introduced.

Usage Guidelines

This command can only be used on Cisco 7200 series routers and on Cisco 2600 and 3600 adapters that support per-VC queueing.

This command is configurable at the VC level only.

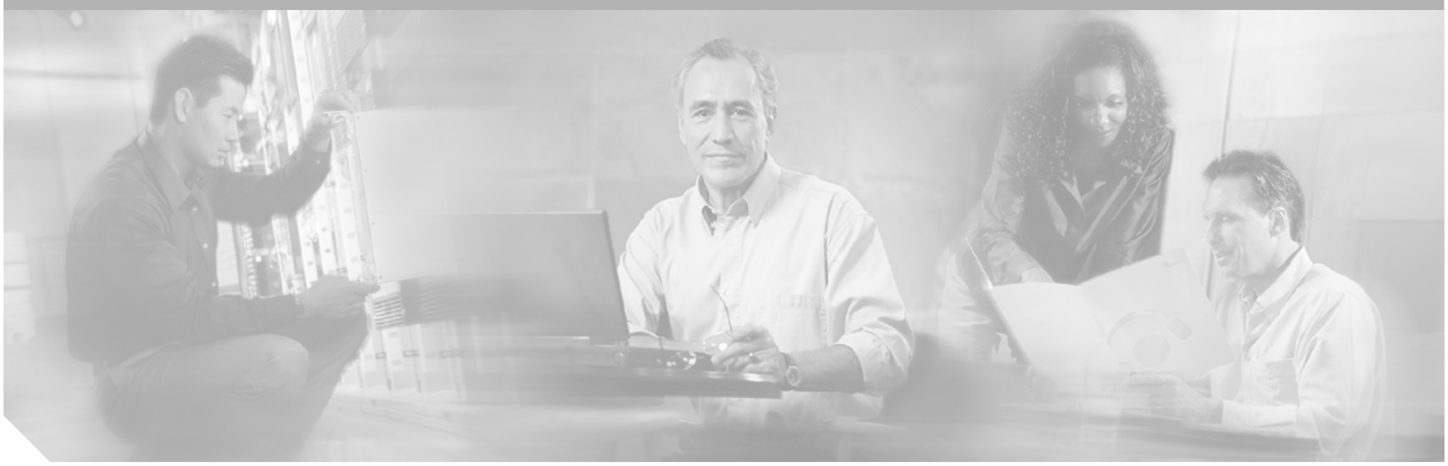
Examples

The following example sets the per-VC hold queue to 55:

```
interface atm2/0.1
 pvc 1/101
  vc-hold-queue 55
```

Related Commands

Command	Description
hold-queue	Specifies the hold-queue limit of an interface.
show interfaces	Displays statistics for all interfaces configured on the router or access server.
show queueing interface	Displays the queueing statistics of an interface or VC.



Index

INDEX

B1R	Cisco IOS Bridging and IBM Networking Command Reference, Volume 1 of 2
B2R	Cisco IOS Bridging and IBM Networking Command Reference, Volume 2 of 2
D1R	Cisco IOS Dial Technologies Command Reference, Volume 1 of 2
D2R	Cisco IOS Dial Technologies Command Reference, Volume 2 of 2
DB	Cisco IOS Debug Command Reference
FR	Cisco IOS Configuration Fundamentals Command Reference
IP1R	Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services
IP2R	Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols
IP3R	Cisco IOS IP Command Reference, Volume 3 of 3: Multicast
IR	Cisco IOS Interface Command Reference
MWR	Cisco IOS Mobile Wireless Command Reference
P2R	Cisco IOS AppleTalk and Novell IPX Command Reference
P3R	Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Command Reference
QR	Cisco IOS Quality of Service Solutions Command Reference
SR	Cisco IOS Security Command Reference
TR	Cisco IOS Terminal Services Command Reference
VR	Cisco IOS Voice, Video, and Fax Command Reference
WR	Cisco IOS Wide-Area Networking Command Reference
XR	Cisco IOS Switching Services Command Reference

Symbols

A

B

C

D

E

F

H

I

Q

R

S

T

U

V

W