



Quality of Service Commands

The following are quality of service (QoS) commands. The commands are arranged alphabetically.

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

<i>acl-index</i>	Access list number. To classify packets by <ul style="list-style-type: none"> 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
<i>precedence</i>	IP precedence. Valid values are numbers from 0 to 7.
<i>mac-address</i>	MAC address.
<i>exp</i>	MPLS experimental field. Valid values are numbers from 0 to 7.
mask <i>mask</i>	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 discovery qos

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

auto discovery qos [trust]

no auto discovery qos

Syntax Description

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

Defaults

No data collection is performed.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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

The **no auto discovery qos** command terminates the Auto-Discovery phase and removes any data collection reports generated.

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

Examples

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

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

```
Router(config-if)# end
```

Related Commands

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

auto qos

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

auto qos

no auto qos

Syntax Description This command has no arguments or keywords.

Defaults No QoS policies are installed.

Command Modes Interface configuration

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

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

The **no auto qos** command removes any AutoQoS-generated class maps and policy maps installed on the interface.

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

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

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

auto qos voip

To configure the AutoQoS — VoIP feature on an interface, use the **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

Disabled

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-atm** keywords are configured.

```
Router> enable
Router# configure terminal
Router(config)# interface serial4/1.2 point-to-point
Router(config-if)# bandwidth 100
Router(config-if)# ip address 192.168.0.0 255.255.255.0
Router(config-if)# frame-relay interface-dlci 102
Router(config-fr-dlci)# auto qos voip trust fr-atm
Router(config-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

<i>bandwidth-kbps</i>	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.
<i>percentage</i>	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.
<i>percentage</i>	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 bandwidth is specified

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 and implemented on Versatile Interface Processor (VIP)-enabled Cisco 7500 series routers.
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 and implemented on VIP-enabled Cisco 7500 series routers.
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 queuing (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.

Specifying Bandwidth as a Percentage

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.

Bandwidth Command Restrictions

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*.

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

Queue Limits

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



Note

Using the **queue-limit** command to modify the default queue-limit is especially important for higher-speed interfaces, in order to meet the minimum bandwidth guarantees required by the interface.

Examples

CBWFQ Bandwidth Guarantee Example

The following example shows 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 serial3/2:
interface serial3/2
  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 serial3/2

Serial3/2

Service-policy output:policy1

Class-map:class1 (match-all)
  0 packets, 0 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
  Match:none
  Weighted Fair 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 serial3/2 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 serial3/2

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 Queuing
  Output Queue:Conversation 266
  Bandwidth remaining 25 (%) Max Threshold 64 (packets)
  (pkts matched/bytes matched) 0/0
  (depth/total drops/no-buffer drops) 0/0/0

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

```

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 <i>precedence-level</i>	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 <i>precedence-level</i> 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

<i>bundle-name</i>	Specifies the name of the bundle to be created. Limit is 16 alphanumeric characters.
--------------------	--

Defaults

No bundle is specified.

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

<i>bundle-name</i>	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 <i>nsap-address</i>	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 (EtherSwitch)

To define a traffic classification for a policy to act on using the class-map name or access group, use the **class** command in policy-map configuration mode. To delete an existing class map, use the **no** form of this command.

```
class class-map-name [access-group acl-index-or-name]
```

```
no class class-map-name
```

Syntax Description

<i>class-map-name</i>	Name of the class map.
access-group <i>acl-index-or-name</i>	(Optional) Number or name of an IP standard or extended access control list (ACL). For an IP standard ACL, the index range is 1 to 99 and 1300 to 1999; for an IP extended ACL, the index range is 100 to 199 and 2000 to 2699.

Defaults

No policy-map class maps are defined.

Command Modes

Policy-map configuration

Command History

Release	Modification
12.1(6)EA2	This command was introduced.
12.2(15)ZJ	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.

Usage Guidelines

Before you use the **class** (EtherSwitch) command, use the **policy-map** global configuration command to identify the policy map and to enter policy-map configuration mode. After you specify a policy map, you can configure a policy for new classes or modify a policy for any existing classes in that policy map. You attach the policy map to an interface by using the **service-policy** interface configuration command; however, you cannot attach one that uses an ACL classification to the egress direction.

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

The **class** (EtherSwitch) command performs the same function as the **class-map** global configuration command. Use the **class** (EtherSwitch) command when a new classification, which is not shared with any other ports, is needed. Use the **class-map** command when the map is shared among many ports.



Note

In a policy map, the class named “class-default” is not supported. The Ethernet switch network module does not filter traffic on the basis of the policy map defined by the **class class-default** policy-map configuration command.

After entering the **class** (EtherSwitch) command, you enter policy-map class configuration mode. When you are in this mode, these configuration commands are available:

- **default**: sets a command to its default.
- **exit**: exits policy-map class configuration mode and returns to policy-map configuration mode.
- **no**: returns a command to its default setting.
- **police**: defines a policer for the classified traffic. The policer specifies the bandwidth limitations and the action to take when the limits are exceeded. For more information, see the **police** command.

To return to policy-map configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command.

**Note**

For more information about configuring IP ACLs, refer to the “Configuring IP Services” chapter in the *Cisco IOS IP Configuration Guide*.

Examples

The following example shows how to create a policy map named “policy1.” When attached to the ingress port, it matches all the incoming traffic defined in class1 and polices the traffic at an average rate of 1 Mbps and bursts at 131072 bytes. Traffic exceeding the profile is dropped.

```
Router(config)# policy-map policy1
Router(config-pmap)# class class1
Router(config-pmap-c)# police 1000000 131072 exceed-action drop
Router(config-pmap-c)# exit
Router(config-pmap)#
```

You can verify your settings by entering the **show policy-map** privileged EXEC command.

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to the class whose name you specify.
match (class-map configuration)	Defines the match criteria to classify traffic.
police	Configures traffic policing.
policy-map	Creates or modifies a policy map that can be attached to multiple 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 QoS policy maps.

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

<i>class-name</i>	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 class is specified.

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

Policy Map Configuration Mode

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

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

Class Characteristics

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

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

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

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

Predefined Default Class

The predefined default class called class-default is available for you to use. The class class-default is the class to which traffic is directed if that traffic does not match any of the match criteria in the configured class maps.

Tail Drop or WRED

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

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

<i>vc-class-name</i>	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 called “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 [match-all | match-any] class-map-name
```

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

Syntax Description

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.

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.

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 either the input or output interface (determined by how the **service-policy** command is configured) are checked against the match criteria configured for a class map to determine if the packet belongs to that class.

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

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

<i>ip-address</i>	(Optional) Frees security associations with a specific neighbor.
<i>hostname</i>	(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	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.
---------------------------	----------------	--

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      Resv      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      Resv      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 reservation

To remove Resource Reservation Protocol (RSVP) RESV-related receiver information currently in the database, use the **clear ip rsvp reservation** command in EXEC mode.

```
clear ip rsvp reservation {session-ip-address sender-ip-address {tcp | udp | ip-protocol}
session-dport sender-sport | *}
```

Syntax Description

<i>session-ip-address</i>	For unicast sessions, this is the address of the intended receiver; for multicast sessions, it is the IP multicast address of the session.
<i>sender-ip-address</i>	The IP address of the sender.
tcp udp <i>ip-protocol</i>	TCP, User Datagram Protocol (UDP), or IP protocol in the range from 0 to 65535.
<i>session-dport</i>	The destination port. Note 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 wildcard filter (wf) reservations, for which the source port is always ignored and can therefore be zero).
<i>sender-sport</i>	The source port. Note 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 wildcard filter (wf) reservations, for which the source port is always ignored and can therefore be zero).
*	Wildcard used to clear all senders.

Command Modes

EXEC

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

Use the **clear ip rsvp reservation** command to remove the RESV-related sender information currently in the database so that when reservation requests arrive, based on the RSVP admission policy, the relevant ones can be reestablished.

Whenever you change the clockrate or bandwidth of an interface, RSVP does not update its database to reflect the change. This is because such a change requires that RSVP reestablish reservations based on the new clockrate or bandwidth value and arbitrarily dropping some reservations while retaining others is not desired. The solution is to clear the RESV state by issuing the **clear ip rsvp reservation** command.

The **clear ip rsvp reservation** command clears the RESV state from the router on which you issued the command and causes the router to send a PATH TEAR message to the upstream routers thereby clearing the RESV state for that reservation on all the upstream routers.

Examples

The following example clears all the RESV-related receiver information currently in the database:

```
Router# clear ip rsvp reservation *
```

The following example clears all the RESV-related receiver information for a specified reservation currently in the database:

```
Router# clear ip rsvp reservation 10.2.1.1 10.1.1.2 udp 10 20
```

Related Commands

Command	Description
clear ip rsvp sender	Removes RSVP PATH-related sender information currently in the database.

clear ip rsvp sender

To remove Resource Reservation Protocol (RSVP) PATH-related sender information currently in the database, use the **clear ip rsvp sender** command in EXEC mode.

```
clear ip rsvp sender {session-ip-address sender-ip-address {tcp | udp | ip-protocol} session-dport sender-sport | * }
```

Syntax Description

<i>session-ip-address</i>	For unicast sessions, this is the address of the intended receiver; for multicast sessions, it is the IP multicast address of the session.
<i>sender-ip-address</i>	The IP address of the sender.
tcp udp <i>ip-protocol</i>	TCP, User Datagram Protocol (UDP), or IP protocol in the range from 0 to 65535.
<i>session-dport</i>	The destination port. Note 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 wildcard filter (wf) reservations, for which the source port is always ignored and can therefore be zero).
<i>sender-sport</i>	The source port. Note 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 wildcard filter (wf) reservations, for which the source port is always ignored and can therefore be zero).
*	Wildcard used to clear all senders.

Command Modes

EXEC

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

Use the **clear ip rsvp sender** command to remove the PATH-related sender information currently in the database so that when reservation requests arrive, based on the RSVP admission policy, the relevant ones can be reestablished.

Whenever you change the clockrate or bandwidth of an interface, RSVP does not update its database to reflect the change. This is because such a change requires that RSVP reestablish reservations based on the new clockrate or bandwidth value and arbitrarily dropping some reservations while retaining others is not desired. The solution is to clear the PATH state by issuing the **clear ip rsvp sender** command.

The **clear ip rsvp sender** command clears the PATH state from the router on which you issued the command and causes the router to send a PATH TEAR message to the downstream routers thereby clearing the PATH state for that reservation on all the downstream routers.

Examples

The following example clears all the PATH-related sender information currently in the database:

```
Router# clear ip rsvp sender *
```

The following example clears all the PATH-related sender information for a specified reservation currently in the database:

```
Router# clear ip rsvp sender 10.2.1.1 10.1.1.2 udp 10 20
```

Related Commands

Command	Description
clear ip rsvp reservation	Removes RSVP RESV-related receiver information currently in the database.

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.

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.

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.

control-plane

To enter control-plane configuration mode, which allows users to associate or modify attributes or parameters that are associated with the control plane of the device, use the **control-plane** command in global configuration mode.

control-plane

Syntax Description This command has no arguments or keywords.

Defaults No control plane service policies are defined.

Command Modes Global configuration

Command History	Release	Modification
	12.2(18)S	This command was introduced.
	12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

Usage Guidelines After you issue the **control-plane** command, you can begin defining aggregate control plane services for your Route Processor (RP); for example, you can associate a service policy to police all traffic that is destined to the control plane.

Examples The following example shows how to configure trusted hosts with source addresses 10.1.1.1 and 10.1.1.2 to forward Telnet packets to the control plane without constraint, while allowing all remaining Telnet packets to be policed at the specified rate:

```
! Allow 10.1.1.1 trusted host traffic.
Router(config)# access-list 140 deny tcp host 10.1.1.1 any eq telnet
! Allow 10.1.1.2 trusted host traffic.
Router(config)# access-list 140 deny tcp host 10.1.1.2 any eq telnet
! Rate limit all other Telnet traffic.
Router(config)# access-list 140 permit tcp any any eq telnet
! Define class-map "telnet-class."
Router(config)# class-map telnet-class
Router(config-cmap)# match access-group 140
Router(config-cmap)# exit
Router(config)# policy-map control-plane-policy
Router(config-pmap)# class telnet-class
Router(config-pmap-c)# police 80000 conform transmit exceed drop
Router(config-pmap-c)# exit
Router(config-pmap)# exit
! Define aggregate control plane service for the active Route Processor.
Router(config)# control-plane
Router(config-cp)# service-policy input control-plane-policy
Router(config-cp)# exit
```

Related Commands

Command	Description
class	Specifies the name of the class whose policy you want to create or change or specifies the default class before you configure its policy.
class-map	Creates a class map to be used for matching packets to a specified class.
drop	Configures a traffic class to discard packets belonging to a specific class.
match access-group	Configures the match criteria for a class map on the basis of the specified ACL.
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
service-policy (control-plane)	Attaches a policy map to a control plane for aggregate control plane services.
show policy-map control-plane	Displays the configuration of a class or all classes for the policy map of a control plane.

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** command in EXEC mode.

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

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

Command Modes EXEC

Command History	Release	Modification
	12.1(1)E	This command was introduced.
	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

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

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

Examples

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

```
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.

estimate bandwidth

To estimate the bandwidth needed per traffic class for given quality of service (QoS) targets based on traffic data, use the **estimate bandwidth** command in policy-map class configuration mode. To disable the estimated bandwidth processing, use the **no** form of this command.

estimate bandwidth [**drop-one-in** *n*] [**delay-one-in** *n* **milliseconds** *n*]

no estimate bandwidth

Syntax Description

drop-one-in <i>n</i>	(Optional) The packet loss rate; for example, a value of 999 means drop no more than one packet out of 999. The range for <i>n</i> is 50 to 1000000 packets.
delay-one-in <i>n</i> milliseconds <i>n</i>	(Optional) The packet delay time and probability; the range for <i>n</i> is 50 to 1000000 packets. The delay threshold; the range for <i>n</i> is 8 to 1000 milliseconds.

Defaults

Disabled

Command Modes

Policy-map class configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

Use the **estimate bandwidth** command to specify the target drop probability, the delay time and probability, and the timeframe.

If you specify a delay time, you must also specify a delay threshold.

If you issue the **estimate bandwidth** command with no keywords, the default target is drop < 2%, which is the same as entering **estimate bandwidth drop-one-in 500**.

Examples

In the following example, the QoS targets are drop no more than one packet in 100, and delay no more than one packet in 100 by more than 50 milliseconds:

```
Router(config-pmap-c)# estimate bandwidth drop-one-in 100 delay-one-in 100 milliseconds 50
```

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

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	<i>exponent</i>	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	<p>When used, this command is issued after the random-detect-group command is entered.</p> <p>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:</p>
------------------	--

$$\text{average} = (\text{old_average} * (1 - 1/2^x)) + (\text{current_queue_size} * 1/2^x)$$

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 queuing (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	<i>dynamic-queues</i>	(Optional) A number specifying the number of dynamic conversation queues. The number can be in the range of 16 to 4096.
---------------------------	-----------------------	---

Defaults	No queues are reserved.
-----------------	-------------------------

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 and implemented on Versatile Interface Processor (VIP)-enabled Cisco 7500 series routers.
	12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T and was implemented on VIP-enabled Cisco 7500 series routers.

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

<i>congestive-discard-threshold</i>	(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.
<i>dynamic-queues</i>	(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.
<i>reservable-queues</i>	(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	<ul style="list-style-type: none"> • Source net, node, socket • Destination net, node, socket • Type
Connectionless Network Service (CLNS)	<ul style="list-style-type: none"> • Source network service access point (NSAP) • Destination NSAP
DECnet	<ul style="list-style-type: none"> • Source address • Destination address
Frame Relay switching	<ul style="list-style-type: none"> • Data-link connection identified (DLCI) value
IP	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • Unicast: source MAC, destination MAC • Ethertype Service Advertising Protocol (SAP)/Subnetwork Access Protocol (SNAP) multicast: destination MAC address
Source-route bridging	<ul style="list-style-type: none"> • Unicast: source MAC, destination MAC • SAP/SNAP multicast: destination MAC address
Novell NetWare	<ul style="list-style-type: none"> • Source/destination network/host/socket • Level 2 protocol
All others (default)	<ul style="list-style-type: none"> • 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 Multiprotocol 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*.

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

<i>aggregate-packets</i>	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 Versatile Interface Processor (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

<i>individual-packet</i>	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 (class-default)	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 Versatile Interface Processor (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 <i>number</i>	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 <i>number</i>	Two low-order IP Precedence bits of the type of service (ToS) field.
<i>class-packet</i>	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 (class-default)	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 Versatile Interface Processor (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 (class-default)	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 Versatile Interface Processor (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 (class-default)	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 Versatile Interface Processor (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 <i>number</i>	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 <i>number</i>	Two low-order IP Precedence bits of the type of service (ToS) field. The value range is from 1 to 3.
<i>weight</i>	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		
<i>high-limit</i>	(Optional) Size of the high priority queue specified in maximum number of packets.	
<i>medium-limit</i>	(Optional) Size of the medium priority queue specified in maximum number of packets.	
<i>normal-limit</i>	(Optional) Size of the normal priority queue specified in maximum number of packets.	
<i>low-limit</i>	(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 compression-connections

To specify the maximum number of Real-Time Transport Protocol (RTP) header compression connections that can exist on a Frame Relay interface, use the **frame-relay ip rtp compression-connections** command in interface configuration mode. To restore the default, use the **no** form of this command.

frame-relay ip rtp compression-connections *number*

no frame-relay ip rtp compression-connections

Syntax Description	<i>number</i>	Maximum number of RTP header compression connections. The range is from 3 to 256.
---------------------------	---------------	---

Defaults	256 header compression connections
-----------------	------------------------------------

Command Modes	Interface configuration
----------------------	-------------------------

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

Usage Guidelines	Before you can configure the maximum number of connections, RTP header compression must be configured on the interface using the frame-relay ip rtp header-compression command.
	The number of RTP header compression connections must be set to the same value at each end of the connection.

Examples	The following example shows the configuration of a maximum of 150 RTP header compression connections on serial interface 0:
-----------------	---

```
interface serial 0
 encapsulation frame-relay
 frame-relay ip rtp header-compression
 frame-relay ip rtp compression-connections 150
```

Related Commands	Command	Description
	frame-relay ip rtp header-compression	Enables RTP header compression for all Frame Relay maps on a physical interface.
	frame-relay map ip compress	Enables both RTP and TCP header compression on a link.
	frame-relay map ip rtp header-compression	Enables RTP header compression per DLCI.
	show frame-relay ip rtp header-compression	Displays RTP header compression statistics for Frame Relay.

frame-relay ip tcp compression-connections

To specify the maximum number of TCP header compression connections that can exist on a Frame Relay interface, use the **frame-relay ip tcp compression-connections** command in interface configuration mode. To restore the default, use the **no** form of this command.

frame-relay ip tcp compression-connections *number*

no frame-relay ip tcp compression-connections

Syntax Description	<i>number</i>	Maximum number of TCP header compression connections. The range is from 3 to 256.
---------------------------	---------------	---

Defaults	256 header compression connections
-----------------	------------------------------------

Command Modes	Interface configuration
----------------------	-------------------------

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

Usage Guidelines	<p>Before you can configure the maximum number of connections, TCP header compression must be configured on the interface using the frame-relay ip tcp header-compression command.</p> <p>The number of TCP header compression connections must be set to the same value at each end of the connection.</p>
-------------------------	--

Examples	The following example shows the configuration of a maximum of 150 TCP header compression connections on serial interface 0:
-----------------	---

```
interface serial 0
 encapsulation frame-relay
 frame-relay ip tcp header-compression
 frame-relay ip tcp compression-connections 150
```

Related Commands	Command	Description
	frame-relay ip tcp header-compression	Enables TCP header compression for all Frame Relay maps on a physical interface.
	frame-relay map ip compress	Enables both RTP and TCP header compression on a link.
	frame-relay map ip tcp header-compression	Assigns header compression characteristics to an IP map that differ from the compression characteristics of the interface with which the IP map is associated.
	show frame-relay ip tcp header-compression	Displays statistics and TCP/IP header compression information for the interface.

frame-relay ip tcp header-compression

To configure an interface to ensure that the associated permanent virtual circuit (PVC) will always carry outgoing TCP/IP headers in compressed form, use the **frame-relay ip tcp header-compression** command in interface configuration mode. To disable compression of TCP/IP packet headers on the interface, use the **no** form of this command.

frame-relay ip tcp header-compression [passive]

no frame-relay ip tcp header-compression

Syntax Description

passive (Optional) Compresses the outgoing TCP/IP packet header only if an incoming packet had a compressed header.

Defaults

Active TCP/IP header compression; all outgoing TCP/IP packets are subjected to header compression.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

This command applies to interfaces that support Frame Relay encapsulation, specifically serial ports and High-Speed Serial Interface (HSSI).

Frame Relay must be configured on the interface before this command can be used.

TCP/IP header compression and Internet Engineering Task Force (IETF) encapsulation are mutually exclusive. If an interface is changed to IETF encapsulation, all encapsulation and compression characteristics are lost.

When you use this command to enable TCP/IP header compression, every IP map inherits the compression characteristics of the interface, unless header compression is explicitly rejected or modified by use of the **frame-relay map ip tcp header compression** command.

We recommend that you shut down the interface prior to changing encapsulation types. Although this is not required, shutting down the interface ensures the interface is reset for the new type.

Examples

The following example configures serial interface 1 to use the default encapsulation (cisco) and passive TCP header compression:

```
interface serial 1
 encapsulation frame-relay
 frame-relay ip tcp header-compression passive
```

Related Commands	Command	Description
	frame-relay map ip tcp header-compression	Assigns header compression characteristics to an IP map different from the compression characteristics of the interface with which the IP map is associated.

frame-relay ip rtp header-compression

To enable Real-Time Transport Protocol (RTP) header compression for all Frame Relay maps on a physical interface, use the **frame-relay ip rtp header-compression** command in interface configuration mode. To disable the compression, use the **no** form of this command.

frame-relay ip rtp header-compression [active | passive] [periodic-refresh]

no frame-relay ip rtp header-compression [active | passive] [periodic-refresh]

Syntax Description

active	(Optional) Compresses all outgoing RTP packets.
passive	(Optional) Compresses the outgoing RTP/User Datagram Protocol (UDP)/IP header only if an incoming packet had a compressed header.
periodic-refresh	(Optional) Indicates that the compressed IP header will be refreshed periodically.

Defaults

Disabled.

By default, whatever type of header compression is configured on the interface will be inherited. If header compression is not configured on the interface, the **active** keyword will be used, but no **header-compression** keyword will appear on the **show running-config** command output.

Command Modes

Interface configuration

Command History

Release	Modification
11.3	This command was introduced.
12.3(2)T	This command was modified to include the periodic-refresh keyword.

Usage Guidelines

When the **frame-relay ip rtp header-compression** command is used on the physical interface, all the interface maps inherit the command; that is, all maps will perform UDP and RTP IP header compression.

Examples

The following example enables RTP header compression for all Frame Relay maps on a physical interface:

```
Router> enable
Router# configure terminal
Router(config)# interface Serial12/0.1
Router(config-if)# frame-relay ip rtp header-compression
Router(config-if)# exit
```

In the following example, RTP header compression is enabled and the optional **periodic-refresh** keyword is specified:

```
Router> enable
Router# configure terminal
Router(config)# interface Serial2/0.2
Router(config-if)# frame-relay ip rtp header-compression periodic-refresh
Router(config-if)# exit
```

Related Commands

Command	Description
frame-relay ip rtp compression-connections	Specifies maximum number of RTP header compression connections on a Frame Relay interface.
frame-relay map ip nocompress	Disables both RTP and TCP header compression on a link.
show frame-relay ip rtp header-compression	Displays RTP header compression statistics for Frame Relay.

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

<i>starting-rtp-port-number</i>	The starting UDP port number. The lowest port number to which the packets are sent. A port number can be a number from 2000 to 65535.
<i>port-number-range</i>	The range of UDP destination ports. Number, which added to the <i>starting-rtp-port-number</i> argument, yields the highest UDP port number. The range can be from 0 to 16383.
<i>bandwidth</i>	Maximum allowed bandwidth, in kbps. The bandwidth can range from 0 to 2000 kbps.

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.

frame-relay map ip compress

To enable both Real-Time Transport Protocol (RTP) and TCP header compression on a link, use the **frame-relay map ip compress** command in interface configuration mode.

```
frame-relay map ip ip-address dldi [broadcast] compress [active | passive]
[connections number]
```

Syntax Description		
<i>ip-address</i>		IP address of the destination or next hop.
<i>dldi</i>		Data-link connection identifier (DLCI) number.
broadcast		(Optional) Forwards broadcasts to the specified IP address.
active		(Optional) Compresses all outgoing RTP and TCP packets. This is the default.
passive		(Optional) Compresses the outgoing RTP and TCP header only if an incoming packet had a compressed header.
connections <i>number</i>		(Optional) Specifies the maximum number of RTP and TCP header compression connections. The range is from 3 to 256.

Defaults

RTP and TCP header compression are disabled.

The default maximum number of header compression connections is 256.

Command Modes

Interface configuration

Command History

Release	Modification
11.3	This command was introduced.
12.1(2)T	This command was modified to enable the configuration of the maximum number of header compression connections.

Examples

The following example enables both RTP and TCP header compression on serial interface 1 and sets the maximum number of RTP and TCP header connections at 16:

```
interface serial 1
 encapsulation frame-relay
 ip address 10.108.175.110 255.255.255.0
 frame-relay map ip 10.108.175.220 180 compress connections 16
```

Related Commands	Command	Description
	frame-relay ip rtp compression-connections	Specifies the maximum number of RTP header compression connections on a Frame Relay interface.
	frame-relay ip tcp header-compression	Enables TCP header compression for all Frame Relay maps on a physical interface.
	frame-relay map ip nocompress	Disables both RTP and TCP header compression on a link.
	frame-relay map ip rtp header-compression	Enables RTP header compression for all Frame Relay maps on a physical interface.
	show frame-relay ip rtp header-compression	Displays RTP header compression statistics for Frame Relay.
	show frame-relay ip tcp header-compression	Displays statistics and TCP/IP header compression information for the interface.

frame-relay map ip nocompress

To disable both Real-Time Transport Protocol (RTP) and TCP header compression on a link, use the **frame-relay map ip nocompress** command in interface configuration mode.

frame-relay map ip *ip-address* *dci* [**broadcast**] **nocompress**

Syntax Description		
	<i>ip-address</i>	IP address of the destination or next hop.
	<i>dci</i>	Data-link connection identifier (DLCI) number.
	broadcast	(Optional) Forwards broadcasts to the specified IP address.

Defaults No default behaviors or values

Command Modes Interface configuration

Command History	Release	Modification
	11.3	This command was introduced.

Examples The following example disables RTP and TCP header compression on DLCI 180:

```
interface serial 1
 encapsulation frame-relay
 frame-relay map ip 10.108.175.220 180 nocompress
```

Related Commands	Command	Description
	frame-relay ip rtp header-compression	Enables RTP header compression for all Frame Relay maps on a physical interface.
	frame-relay ip tcp header-compression	Enables TCP header compression for all Frame Relay maps on a physical interface.
	frame-relay map ip compress	Enables RTP and TCP header compression on a link.
	show frame-relay ip rtp header-compression	Displays RTP header compression statistics for Frame Relay.
	show frame-relay ip tcp header-compression	Displays statistics and TCP/IP header compression information for the interface.

frame-relay map ip rtp header-compression

To enable Real-Time Transport Protocol (RTP) header compression per data-link connection identifier (DLCI), use the **frame-relay map ip rtp header-compression** command in interface configuration mode. To disable RTP header compression per DLCI and delete the DLCI, use the **no** form of this command.

```
frame-relay map ip ip-address dlc [broadcast] rtp header-compression [active | passive]
[periodic-refresh] [connections number]
```

```
no frame-relay map ip ip-address dlc [broadcast] rtp header-compression [active | passive]
[periodic-refresh] [connections number]
```

Syntax Description		
	<i>ip-address</i>	IP address of the destination or next hop.
	<i>dlci</i>	DLCI number.
	broadcast	(Optional) Forwards broadcasts to the specified IP address.
	active	(Optional) Compresses outgoing RTP packets.
	passive	(Optional) Compresses the outgoing RTP/User Datagram Protocol (UDP)/IP header only if an incoming packet had a compressed header.
	periodic-refresh	(Optional) Refreshes the compressed IP header periodically.
	connections <i>number</i>	(Optional) Specifies the maximum number of RTP header compression connections. The range is from 3 to 256.

Defaults

Disabled.

By default, whatever type of header compression is configured on the interface will be inherited. If header compression is not configured on the interface, the **active** keyword will be used, but no **header-compression** keyword will appear on the **show running-config** command output.

The default maximum number of header-compression connections is 256.

Command Modes

Interface configuration

Command History

Release	Modification
11.3	This command was introduced.
12.1(2)T	This command was modified to enable the configuration of the maximum number of header compression connections.
12.3(2)T	This command was modified to include the periodic-refresh keyword.

Usage Guidelines

When this command is configured, the specified maps inherit RTP header compression. You can have multiple Frame Relay maps, with and without RTP header compression. If you do not specify the number of RTP header compression connections, the map will inherit the current value from the interface.

Examples

The following example enables RTP header compression on the Serial1/2.1 subinterface and sets the maximum number of RTP header compression connections at 64:

```
Router> enable
Router# configure terminal
Router(config)# interface Serial1/2.1
Router(config-if)# encapsulation frame-relay
Router(config-if)# ip address 10.108.175.110 255.255.255.0
Router(config-if)# frame-relay map ip 10.108.175.220 180 rtp header-compression
connections 64
Router(config-if)# exit
```

In the following example, RTP header compression is enabled on the Serial1/1.0 subinterface, and the optional **periodic-refresh** keyword is included in the configuration:

```
Router> enable
Router# configure terminal
Router(config)# interface Serial1/1.0
Router(config-if)# encapsulation frame-relay
Router(config-if)# ip address 10.108.175.110 255.255.255.0
Router(config-if)# frame-relay map ip 10.108.175.220 180 rtp header-compression
periodic-refresh
Router(config-if)# exit
```

Related Commands

Command	Description
frame-relay ip rtp compression-connections	Specifies the maximum number of RTP header compression connections on a Frame Relay interface.
frame-relay ip rtp header-compression	Enables RTP header compression for all Frame Relay maps on a physical interface.
frame-relay map ip compress	Enables both RTP and TCP header compression on a link.
show frame-relay ip rtp header-compression	Displays RTP header compression statistics for Frame Relay.

