



Quality of Service Commands

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

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

access-list rate-limit

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

```
access-list rate-limit acl-index {precedence | mac-address | mask prec-mask}
```

```
no access-list rate-limit acl-index {precedence | mac-address | mask prec-mask}
```

Syntax Description

<i>acl-index</i>	Access list number. Use any number from 1 to 99 to classify packets by precedence or precedence mask, and use any number from 100 to 199 to classify by MAC address.
<i>precedence</i>	IP Precedence.
<i>mac-address</i>	Address of the MAC.
mask <i>prec-mask</i>	IP Precedence mask; a two-digit hexadecimal number. Use this option when you want to assign multiple precedences 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.

Usage Guidelines

This command classifies packets by the specified IP Precedence or MAC address for a particular CAR access list. You can then apply CAR policies, using the **rate-limit** command, to individual rate-limit access lists. Thus, packets with different IP Precedences or MAC addresses 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 with the same access list number, the new command will overwrite the previous command.

Use the **mask** keyword to assign multiple IP Precedences to the same rate-limit access list. To determine 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 into an 8-bit number with each bit corresponding to one precedence. For example, an IP Precedence 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 precedences. For example, the mask for precedences 1 and 6 is 01000010.
- Step 4** The command expects hexadecimal format. Convert the binary mask into the corresponding hexadecimal number. For example, 01000010 becomes 42. This value is used in the **access-list rate-limit** command. Any packets that have an IP Precedence of 1 or 6 will match this access list.

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

Examples

The following example assigns any packets with a MAC address of 00e0.34b0.7777 to rate-limit access list 100:

```
access-list rate-limit 100 00e0.34b0.7777
```

The following example assigns packets with an IP Precedence of 0, 1, or 2 to the rate-limit access list 25:

```
access-list rate-limit 25 mask 07
```

Related Commands

Command	Description
show access-lists rate-limit	Displays information about rate-limit access lists.
show ip cef	Displays entries in the FIB that are unresolved or displays a FIB summary.

bandwidth (policy-map class)

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

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

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

Syntax Description

<i>bandwidth-kbps</i>	Amount of bandwidth (in kbps) to be assigned to the class.
percent <i>percent</i>	Percentage of available bandwidth to be assigned to the class.

Defaults

No default behavior.

Command Modes

Policy-map class configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.1(1)	The percent keyword was added.

Usage Guidelines

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

Besides specifying the amount of bandwidth in kbps, you can assign bandwidth as a percentage of the available 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 Resource Reservation Protocol (RSVP), IP RTP Priority, and low latency queueing (LLQ).



Note

It is important to remember that 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 cannot be computed.

Configuring bandwidth in percentages is most useful when the underlying link bandwidth is unknown or the relative class bandwidth distributions are known. For interfaces that have adaptive shaping rates (such as available bit rate [ABR] virtual circuits), CBWFQ can be configured by configuring class bandwidths in percentages.

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

- If the **percent** keyword is used, the sum of the class bandwidth percentages cannot exceed 100 percent.
- 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.
- The IP RTP Priority and RSVP features can only be configured in kbps.
- The priority class inside LLQ can have bandwidth specified only in kbps. The nonpriority classes inside LLQ can have bandwidths specified either in percentages or in kbps, but not a mix of both.

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.

Examples

The following example modifies the bandwidth for a class called acl22. The default class belongs to a service policy map called polmap6.

```
policy-map polmap6
  class acl22
    bandwidth 2000
    queue-limit 30
```

CBWFQ Bandwidth Guarantee

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

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

  class class2
    bandwidth percent 25
    exit
  end

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

The following output from the **show policy-map interface** command shows that 50 percent of the interface bandwidth is guaranteed for class1 and 25 percent is guaranteed for class2:

```
Router# show policy-map interface s3/2
Serial3/2  output :policy1
Class class1
  Weighted Fair Queueing
    Output Queue:Conversation 265
      Bandwidth 50 (%) Packets Matched 0 Max Threshold 64 (packets)
      (discards/tail drops) 0/0
Class class2
  Weighted Fair Queueing
    Output Queue:Conversation 266
      Bandwidth 25 (%) Packets Matched 0 Max Threshold 64 (packets)
      (discards/tail drops) 0/0
```

In this example, the entire interface bandwidth is available for CBWFQ because RSVP, IP RTP Priority, and LLQ are not enabled. If this policy map is attached to a physical interface, the available bandwidth is equal to the link bandwidth. During periods of congestion, 50 percent of the link bandwidth is guaranteed to class1 and 25 percent of the link bandwidth is guaranteed to class2. For example, if this policy map was attached to a 1 Mbps link, class1 would be guaranteed 500 kbps and class2 would be guaranteed 250 kbps during periods of congestion.

CBWFQ and LLQ Bandwidth Allocation

This example illustrates how bandwidth is guaranteed if LLQ is configured with CBWFQ. Remember, the available bandwidth for CBWFQ is the link bandwidth minus the sum of the bandwidths reserved by RSVP, LLQ, and IP RTP Priority.

In this example, LLQ is enabled in a third class called voice1:

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

class class2
  bandwidth percent 25
  exit
end

class voice1
  priority 500
  exit
end

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

The following output from the **show policy-map** command shows that 50 percent of the interface bandwidth is guaranteed for class1, 25 percent is guaranteed for class2, and 500 kbps is guaranteed for voice1:

```
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)
    Class voice1
      Weighted Fair Queueing
        Strict Priority
        Bandwidth 500 (kbps) Max Threshold 64 (packets)
```

Because LLQ reserved 500 kbps of the interface bandwidth, if you attach this policy map to an interface with 2 Mbps, only 1.5 Mbps is available for CBWFQ classes. In this example, 50 percent of 1.5 Mbps (750 kbps) is guaranteed for class1 and 25 percent (375 kbps) is guaranteed for class2. The remaining 25 percent of the available bandwidth (375 kbps) is shared by class1, class2, and any best-effort traffic.

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.
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.

bgp-policy

To enable the Policy Propagation via Border Gateway Protocol (BGP) feature on the interface, use the **bgp-policy** interface configuration command. To disable the Policy Propagation via BGP feature, use the **no** form of this command.

bgp-policy ip-prec-map

no bgp-policy ip-prec-map

Syntax Description

ip-prec-map QoS policy based on the IP Precedence.

Defaults

The Policy Propagation via BGP feature is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
11.1 CC	This command was introduced.

Usage Guidelines

For the Policy Propagation via BGP feature to work, you must enable BGP and either Cisco Express Forwarding (CEF) or distributed CEF (dCEF). In addition, the proper route-map configuration must be in place to specify the IP Precedence (for example, the **set ip precedence** route-map configuration command).



Note

If you specify both **source** and **destination** keywords on the interface, the software looks up the source address in the routing table and classifies the packet based on the source address first; then the software looks up the destination address in the routing table and reclassifies the packet based on the destination address.

To display QoS policy information for the interface, use the **show ip interface** command.

Examples

The following example enables the Policy Propagation via BGP feature on an interface based on the source address and the IP Precedence setting:

```
configure terminal
interface ethernet 4/0/0
  bgp-policy ip-prec-map
end
```

bump

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

To configure the bumping rules for a specific VC member of a bundle, use the **bump** bundle-vc configuration command. To remove the explicit bumping rules for the VC and default it to implicit bumping, use the **no bump explicit** command. To specify that the VC does not accept any bumped traffic, use the **no** form of this command.

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

```
no bump { explicit precedence-level | traffic }
```

Syntax Description		
	implicit	Depending on the mode, applies implicit bumping rules, which is also the default, to a single VC bundle member (bundle-vc mode) or all VCs in the bundle (bundle mode). The (default) implicit bumping rule stipulates that bumped traffic is to be carried by a VC with a lower precedence.
	explicit <i>precedence-level</i>	Specifies the precedence level to which traffic on a VC (bundle-vc mode) will be bumped when the VC goes down. Specifies a single number as the value of <i>precedence-level</i> .
	traffic	In its positive form, specifies that the VC accepts bumped traffic. The no form stipulates that the VC does not accept any bumped traffic.

Defaults	
	Implicit bumping. Bump traffic (VCs accept bumped traffic).

Command Modes	
	VC-class configuration (for a VC class). Bundle-vc configuration (for a VC bundle member).

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

Usage Guidelines	
	Use the bump command in bundle-vc configuration mode to configure bumping rules for a discrete VC bundle member or 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 configured to handle the next lower precedence level. When the original VC that bumped the traffic comes back up, traffic it is configured to carry is restored to it. When no other positive forms of the bump command are configured, the **bump implicit** command takes effect.
- **Explicit bumping:** If you configure a VC with the **bump explicit** command, you can specify the precedence level to which traffic on a VC will be bumped when that VC goes down, and the traffic will be directed to a VC mapped with that precedence level. If the VC that picks up and carries the traffic goes down, the traffic is subject to the bumping rules for that VC. You can specify only one precedence level for bumping.
- **Bumped traffic:** The VC accepts bumped traffic. You can configure bumped traffic explicitly using either the **bump traffic** or the **no bump traffic** command, or let the default take effect by specifying neither.
- **No bumped traffic:** To configure a discrete VC to reject bumped traffic when the traffic is directed to the VC, use the **no bump traffic** command.



Note

When no alternative VC can be found to handle bumped traffic, the bundle is declared down. To avoid this occurrence, configure explicitly the bundle member VC 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 enter the **bundle** command to enact bundle configuration mode for the bundle to which you want to add or modify the VC member to be configured. Then, use the **pvc-bundle** command to specify the VC to be created or modified and enter `bundle-vc` configuration mode.

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 rules (listed in order of next highest precedence):

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

Examples

The following example configures the class `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 explicitly 7
```

Related Commands	Command	Description
	class-vc	Assigns a VC class to an ATM PVC, SVC, or VC bundle member.
	precedence	Configures precedence levels for a VC class that can be assigned to a VC bundle and thus applied to all VC members of that bundle.
	protect	Configures a VC class with protected group or protected VC status for application to a VC bundle member.
	ubr	Configures UBR QoS and specifies the output peak cell rate for an ATM PVC, SVC, VC class, or VC bundle member.
	ubr+	Configures UBR QoS and specifies the output peak cell rate and output minimum guaranteed cell rate for an ATM PVC, SVC, VC class, or VC bundle member.
	vbr-nrt	Configures the VBR-NRT QoS and specifies output peak cell rate, output sustainable cell rate, and output maximum burst cell size for an ATM PVC, SVC, VC class, or VC bundle member.

bundle

To create a bundle or modify an existing bundle to enter bundle configuration mode, use the **bundle** subinterface configuration command. 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

None

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 VC members of the bundle.

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

- VC configuration in bundle-vc mode
- Bundle configuration in bundle mode
- 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 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.

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** policy-map configuration command. 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 default behavior.

Command Modes

Policy-map configuration

Command History

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

Usage Guidelines

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

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

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

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

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

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

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

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

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

Examples

The following example configures three class policies included in the policy map called policy1. Class1 specifies policy for traffic that matches access control list 136. Class2 specifies policy for traffic on the 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.

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 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 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
```

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.
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** bundle configuration command. The **no** form of this command removes the VC class parameters from a VC bundle.

class-bundle *vc-class-name*

no class-bundle *vc-class-name*

Syntax Description	<i>vc-class-name</i>	Name of the VC class you are assigning to your VC bundle.
Defaults	No VC class is assigned to the VC bundle.	
Command Modes	Bundle configuration	
Command History	Release	Modification
	12.0 T	This command was introduced, replacing the class command for configuring ATM VC bundles.

Usage Guidelines

To use this command, you must first enter the **bundle** command to create the bundle and enter 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 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: **oam-bundle**, **broadcast**, **encapsulation**, **protocol**, **oam retry**, and **inarp**.

Bundle-level parameters applied through commands 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 first 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
```

Taking into account hierarchy precedence rules, VCs belonging to the bundle1 bundle will be characterized by these parameters: aal5snap, encapsulation, broadcast on, use of Inverse Address Resolution Protocol (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 either configuring Inverse ARP directly on the PVC, on the VC bundle, or in a VC class (applies to IP and IPX protocols only).
pvc-bundle	Adds a PVC to a bundle as a member of the bundle and enters bundle-vc configuration mode in order to configure that PVC bundle member.

Command	Description
show atm bundle	Displays the bundle attributes assigned to each bundle VC member and the current working status of the VC members.
show atm bundle statistics	Displays statistics on the specified bundle.
show atm map	Displays the list of all configured ATM static maps to remote hosts on an ATM network.
vc-class atm	Configures a VC class for an ATM VC or interface.

class-map

To create a class map to be used for matching packets to the class whose name you specify, use the **class-map** global configuration command. 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	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.
<i>class-map-name</i>	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.

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

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

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

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

Examples

The following example specifies class101 as the name of a class, and it defines a class map for this class. The class101 class 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.
	match access-group	Configures the match criteria for a class map based on the specified ACL number.
	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 based on the specified protocol.
	policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.

clear ip rsvp 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.

custom-queue-list

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

custom-queue-list *list*

no custom-queue-list [*list*]

Syntax Description

list 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** 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
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.

Command	Description
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.

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** random-detect-group configuration command. 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. The default is 9.
---------------------------	-----------------	---

Defaults The weight factor is 9.

Command Modes Random-detect-group configuration

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

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

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

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

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 sanjose with a weight factor of 10:

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

Related Commands

Command	Description
protect	Configures a VC to belong to the protected group of the bundle or to be an individually protected VC 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** policy-map class configuration command. 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 of 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 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 for the default number of dynamic queues used when WFQ or CBWFQ is enabled on an ATM PVC.

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 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

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.

Examples

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

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

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

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

Related Commands

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

fair-queue (DWFQ)

To enable VIP-Distributed weighted fair queueing (DWFQ), use the **fair-queue** interface configuration command. 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.

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

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.

Examples

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

```
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 (WFQ)

To enable weighted fair queueing (WFQ) for an interface, use the **fair-queue** interface configuration command. To disable weighted fair queueing 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 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 3 and Table 4 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; or virtual interfaces. Fair queueing is not an option for these protocols. 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.

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

Table 6 *Weighted Fair Queueing Traffic Stream Discrimination Fields (continued)*

Forwarder	Fields Used
VINES	<ul style="list-style-type: none"> • Source network/host • Destination network/host • Level 2 protocol
Apollo	<ul style="list-style-type: none"> • Source network/host/socket • Destination network/host/socket • Level 2 protocol
Xerox Network Systems (XNS)	<ul style="list-style-type: none"> • Source/destination network/host/socket • Level 2 protocol
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 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 for the Cisco 7000 and 7500 routers with a Route Switch Processor (RSP) card, if you used the **tx-queue-limit** command to set the transmit limit available to an interface on a Multiport Communications Interface (MCI) or serial port communications interface (SCI) card and you configured custom queueing or priority queueing for that interface, the configured transmit limit was automatically overridden and set to 1. With Cisco IOS Release 12.0 and later releases, for WFQ, custom queueing, and priority queueing, the configured transmit limit is derived from the bandwidth value set for the interface using the **bandwidth** 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
clear ip rsvp reservation	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.

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** interface configuration command. 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	<p>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.</p> <p>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.</p> <p>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.</p> <p>In some cases, the total number of packets in all queues put together may exceed the aggregate limit.</p>
-------------------------	--

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 (DWFQ)	Enables 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 DWFQ for a VIP-based interface.

fair-queue individual-limit

To set the maximum individual queue depth for VIP-Distributed weighted fair queueing (DWFQ), use the **fair-queue individual-limit** interface configuration command. 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	<p>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.</p> <p>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.</p> <p>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.</p> <p>In some cases, the total number of packets in all queues put together may exceed the aggregate limit.</p>
-------------------------	--

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

fair-queue limit

To set the maximum queue depth for a specific VIP-Distributed weighted fair queueing (DWFQ) class, use the **fair-queue limit** interface configuration command. 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 Border Gateway Protocol (BGP) policy propagation. 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.



Note

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

Examples

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

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

Related Commands	Command	Description
	fair-queue aggregate-limit	Sets the maximum number of packets in all queues combined for DWFQ.
	fair-queue individual-limit	Sets the maximum individual queue depth 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 DWFQ for a VIP-based interface.

fair-queue qos-group

To enable VIP-Distributed weighted fair queueing (DWFQ) and classify packets based on the internal QoS-group number, use the **fair-queue qos-group** interface configuration command. 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 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 (DWFQ)	Enables DWFQ 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 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 DWFQ for a VIP-based interface.

fair-queue tos

To enable VIP-Distributed weighted fair queueing (DWFQ) and classify packets using the type of service (ToS) field of packets, use the **fair-queue tos** 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) 0/0/0 interface.

```
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 (DWFQ)	Enables DWFQ 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 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 DWFQ for a VIP-based interface.

fair-queue weight

To assign a weight to a class for VIP-Distributed weighted fair queueing (DWFQ), use the **fair-queue weight** interface configuration command. To unallocate the bandwidth 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 Border Gateway Protocol (BGP) policy propagation. The value range is 1 to 99.
tos <i>number</i>	Two low-order IP Precedence bits of the type of service (ToS) field. The value range is 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:

- 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:

- 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 DWFQ for a VIP-based interface.

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** map-class configuration command. 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.
	<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.
	<i>bandwidth</i>	Maximum allowed bandwidth (in kbps).

Defaults This command has 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 only need to configure 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 of 16384 to 32764 (32764 = 16384 + 16380) will be matched and given strict priority service.

Related Commands	Command	Description
	ip rtp priority	Reserves a strict priority queue on a Frame Relay PVC for a set of RTP packet flows belonging to a range of UDP destination ports.
	map-class frame-relay priority	Specifies a map class to define QoS values for an SVC. Gives priority to a class within a policy map.
	show frame-relay pvc	Displays statistics about PVCs for Frame Relay interfaces.
	show traffic-shape queue	Displays information about the elements queued at a particular time at the VC (DLCI) level.
	show queue	Displays the contents of packets inside a queue for a particular interface or VC.

