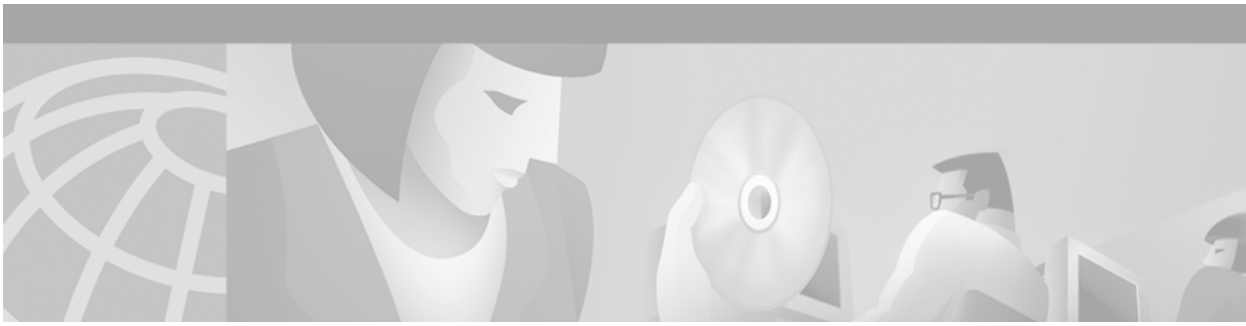

Quality of Service Commands

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* | *exp* **mask** *mask*}

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

Syntax Description

acl-index	Specifies the access list number. Classification options are as follows: • For IP precedence, use any number from 1 to 99. • For MAC address, use any number from 100 to 199. • For MPLS experimental field, use any number from 200 to 299.
precedence	Specifies the IP precedence. Valid values are from 0 to 7.
mac-address	Specifies the MAC address.
exp	Specifies the MPLS experimental field. Value values are from 0 to 7.
mask *mask*	Specifies the 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.

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 list causing packets with different IP precedences, MAC addresses, or MPLS experimental field values to be 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 overwrites the previous command.

Use the **mask** keyword to assign multiple IP precedences or MPLS experimental field values 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 or MPLS experimental field values into an 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 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 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

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
```

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

```
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:

```
interface atm4/0.1 mpls
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.

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

bandwidth-kbps	Amount of bandwidth, in kbps, to be assigned to the class.
percent *percent*	Percentage of available bandwidth to be assigned to the class.

Defaults

This command has no default behavior or values.

Command Modes

Policy-map class configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(5)XE	This command was integrated into Cisco IOS Release 12.0(5)XE. Support for the Versatile Interface Processor (VIP)-enabled Cisco 7500 series routers was added.
12.1(1)	The **percent** keyword was added.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T. Support for VIP-enabled Cisco 7500 series routers was added.

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.

Specifying Bandwidth as a Percentage

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 in kbps 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.

Bandwidth Command Restrictions

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. However, the unit for the **priority** command in the priority class can be different from the bandwidth unit of the low priority class.
- The IP RTP Priority and RSVP features can be configured in kbps only.

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

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

The following 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 10
  exit

 class class2
  bandwidth percent 20
  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 the class called class1, 25 percent is guaranteed for the class called class2, and 500 kbps is guaranteed for the class called 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.
class class-default	Specifies the default class whose bandwidth is to be configured or modified.
class-map	Creates a class map to be used for matching packets to a specified class.
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 configuration of all classes configured for all service policies on the specified interface or displays the classes for the service policy for a specific PVC on the interface.

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 *precedence-level*	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 the *precedence-level* argument.
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 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 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 (VC bundle)	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.
pvc-bundle	Adds a PVC to a bundle as a member of the bundle and enters bundle-vc configuration mode in order to configure that PVC bundle member.
ubr	Configures UBR QoS and specifies the output peak cell rate for an ATM PVC, SVC, VC class, or VC bundle member.
ubr+	Configures UBR QoS and specifies the output peak cell rate and output minimum guaranteed cell rate for an ATM PVC, SVC, VC class, or VC bundle member.
vbr-nrt	Configures the VBR-NRT QoS and specifies output peak cell rate, output sustainable cell rate, and output maximum burst cell size for an ATM PVC, SVC, VC class, or VC bundle member.
vc-class atm	Configures a VC class or an ATM VC or interface.

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

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

Defaults

This command has no default behavior or values.

Command Modes

Subinterface configuration

Command History

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

Usage Guidelines

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

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

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

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

Examples

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

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

Related Commands

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

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** QoS 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

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

Defaults

This command has no default behavior or values.

Command Modes

QoS policy-map configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(5)XE	This command was integrated into Cisco IOS Release 12.0(5)XE.
12.0(7)S	This command was integrated into Cisco IOS Release 12.0(7)S.
12.1(1)E	This command was integrated into Cisco IOS Release 12.1(1)E.

Usage Guidelines

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** bundle configuration command. To remove the VC class parameters from a VC bundle, use the **no** form of this command.

class-bundle *vc-class-name*

no class-bundle *vc-class-name*

Syntax Description

vc-class-name	Name of the VC class 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 (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 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.
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 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

This command has 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 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

session-ip-address	For unicast sessions, this is the address of the intended receiver; for multicast sessions, it is the IP multicast address of the session.
sender-ip-address	The IP address of the sender.
tcp | **udp** | *ip-protocol*	TCP, User Datagram Protocol (UDP), or IP protocol in the range from 0 to 65535.
session-dport	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).
sender-sport	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

session-ip-address	For unicast sessions, this is the address of the intended receiver; for multicast sessions, it is the IP multicast address of the session.
sender-ip-address	The IP address of the sender.
tcp | **udp** | *ip-protocol*	TCP, User Datagram Protocol (UDP), or IP protocol in the range from 0 to 65535.
session-dport	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).
sender-sport	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-number*]

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

Syntax Description

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

Defaults

No custom queue list is assigned.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

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

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

Examples

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

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

Related Commands

Command	Description
priority-list interface	Establishes queueing priorities on packets entering from a given interface.
queue-list default	Assigns a priority queue for those packets that do not match any other rule in the queue list.
queue-list interface	Establishes queueing priorities on packets entering on an interface.
queue-list queue byte-count	Specifies how many bytes the system allows to be delivered from a given queue during a particular cycle.
queue-list queue limit	Designates the queue length limit for a queue.
show interfaces	Displays statistics for all interfaces configured on the router or access server.
show queue	Displays the contents of packets inside a queue for a particular interface or VC.
show queueing	Lists all or selected configured queueing strategies.

disconnect qdm

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

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

Syntax Description

client	(Optional) Specifies that a specific QDM client will be disconnected.
client-id	(Optional) Specifies the specific QDM identification number to disconnect.

Defaults

This command has no default behavior or values.

Command Modes

EXEC

Command History

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

Usage Guidelines

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

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

Examples

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

```
Router# disconnect qdm
```

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

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

Related Commands

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

dscp

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

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

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

Syntax Description

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

Defaults

If WRED is using the DSCP value to calculate the drop probability of a packet, all entries of the DSCP table are initialized with the default settings shown in Table 3 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 3 lists the dscp default settings used by the **dscp** command. Table 3 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 3 dscp Default Settings

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

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

```
dscp af22 28 40 10
```

Related Commands

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

exponential-weighting-constant

To configure the exponential weight factor for the average queue size calculation for a Weighted Random Early Detection (WRED) parameter group, use the **exponential-weighting-constant** 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

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

Defaults

The default weight factor is 9.

Command Modes

Random-detect-group configuration

Command History

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

Usage Guidelines

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

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

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

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

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

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

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

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

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

Examples

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

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

Related Commands

Command	Description
protect	Configures a VC class with a protected group or protected VC status for application to a 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 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 4 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 5 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 4 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 4 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 5 lists the default number of dynamic queues used when WFQ or CBWFQ is enabled on an ATM PVC.

Table 5 Default Number of Dynamic Queues As a Function of ATM PVC Bandwidth

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

Examples

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

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

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

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

Related Commands

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

fair-queue (DWFQ)

To enable VIP-distributed weighted fair queueing (DWFQ), use the **fair-queue** 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 (MLP).

See Table 6 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 6 lists the default queue lengths and thresholds.

Table 6 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)

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

fair-queue [**queue-limit** *queue-value*]

no fair-queue [**queue-limit** *queue-value*]

Syntax Description

queue-limit	(Optional) A keyword used to specify or modify the maximum number of packets that a per-flow queue can hold.
queue-value	(Optional) A number specifying the maximum number of packets that each per-flow queue can accumulate.

Defaults

This command has no default behavior or values.

Command Modes

QoS policy-map configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(5)XE	This command was integrated into Cisco IOS Release 12.0(5)XE. Support for Versatile Interface Processor (VIP)-enabled Cisco 7500 series routers was added.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T. Support for VIP-enabled Cisco 7500 series routers was added.

Usage Guidelines

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

Examples

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

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

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

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

Related Commands

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

fair-queue (WFQ)

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

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

no fair-queue

Syntax Description

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

Defaults

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

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

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

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

The number of dynamic queues is derived from the interface or ATM permanent virtual circuit (PVC) bandwidth. See Table 4 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 5 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 7 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 7 shows the attributes of a message that are used to classify traffic into data streams.

Table 7 Weighted Fair Queueing Traffic Stream Discrimination Fields

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

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

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

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

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

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

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

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.