default ip nbar protocol-pack

To load the base version of the protocol pack that is present in the Cisco IOS image of the Cisco router and to remove all other protocol packs, use the **default ip nbar protocol-pack** command in global configuration mode.

default ip nbar protocol-pack [*protocol-pack*]

Syntax Description

protocol-pack	(Optional) Protocol pack file path and name.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.3S	This command was introduced.

Usage Guidelines

The protocol pack is a single compressed file that contains multiple Protocol Description Language (PDL) files and a manifest file. Before the protocol pack was introduced, PDLs had to be loaded separately. Now a set of required protocols can be loaded, which helps network-based application recognition (NBAR) to recognize additional protocols for classification on your network.

When the **default ip nbar protocol-pack** command is used, all protocol packs are removed from the router, except the base version that is provided with the Cisco IOS image in the router.

Examples

The following example shows how to load the default protocol pack and remove all other protocol packs:

```
Router# configure terminal
Router(config)# default ip nbar protocol-pack
```

Related Commands

Command	Description
ip nbar protocol-pack	Loads a protocol pack.
show ip nbar protocol-pack	Displays protocol pack information.

description (class-map)

To add a description to the class map or the policy map, use the **description** command in class-map configuration or policy-map configuration mode. To remove the description from the class map or the policy map, use the **no** form of this command.

description *character-string*

no description

Syntax Description

character-string	Comment or a description that is added to the class map or the policy map. The character-string cannot exceed 161 characters.

Defaults

If this command is not issued, a description does not exist.

Command Modes

Class-map configuration (config-cmap)

Policy-map configuration (config-pmap)

Command History

Release	Modification
12.4(4)T	This command was introduced.
12.2(18)ZY	This command was integrated into Cisco IOS Release 12.2(18)ZY on the Catalyst 6500 series of switches equipped with the Programmable Intelligent Services Accelerator (PISA).

Usage Guidelines

The **description** command is meant solely as a comment to be put in the configuration to help you remember information about the class map or policy map, such as which packets are included within the class map.

Examples

The following example shows how to specify a description within the class map “ip-udp” and the policy map “fpm-policy”:

```
class-map type stack match-all ip-udp
 description "match UDP over IP packets"
 match field ip protocol eq 0x11 next udp
!
policy-map type access-control fpm-policy
 description "drop worms and malicious attacks"
 class ip-udp
 service-policy fpm-udp-policy
!
!
interface gigabitEthernet 0/1
 service-policy type access-control input fpm-policy
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class.
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.

description (service group)

To add a service-group description, use the **description** command in service-group configuration mode. To remove a service-group description, use the **no** form of this command.

description *descriptive-text*

no description

Syntax Description

descriptive-text	Service-group description. Enter up to 240 characters to describe the service group.

Command Default

A service-group description is not added.

Command Modes

Service-group configuration (config-service-group)

Command History

Release	Modification
12.2(33)SRE	This command was introduced.

Usage Guidelines

Use the **description** (service group) command to provide additional information about the service group, such as the account number, location, or subscriber name.

Examples

The following example shows how to create service group 1 and how to add information that identifies the subscriber account number in the description:

```
Router> enable
Router# configure terminal
Router(config)# service-group 1
Router(config-service-group)# description subscriber account number 105AB1
Router(config-service-group)# end
```

df

To change the algorithm for computing the delay factor (DF), use the **df** command in monitor parameters mode. To use the default DF algorithm (rfc4445) use the **no** form of this command.

df ***algorithm_name***

no df *algorithm_name*

Syntax Description

algorithm_name	The algorithm used to compute the delay factor. These algorithms are supported: • **ipdv** • **rfc4445**

Command Default

The rfc4445 algorithm is used.

Command Modes

Monitor parameters (config-map-c-monitor)

Command History

Release	Modification
15.1(1)S	This command was introduced.

Usage Guidelines

Use the **df** command to modify the delay factor algorithm. The configured algorithm is used for both IP-CBR and MDI flows in a class. The ipdv-based algorithm is independent of the flow rate and reports only the delay caused by the network. The rfc4445-based algorithm is rate dependent and uses the configured flow rate. The rfc4445 based algorithm reports the sum of inter packet delay and network introduced delay.

Examples

This example shows how to configure the delay factor to the ipdv-based algorithm:

```
router(config-pmap-c-monitor)# df ipdv
```

Related Commands

Command	Description
show policy-map type performance-traffic	Displays the policy-map information with the DF algorithm used.

disconnect qdm

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

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

Syntax Description

client	(Optional) Specifies that a specific QDM client will be disconnected.
client-id	(Optional) Specifies the specific QDM identification number to disconnect. A QDM identification number can be a number from 0 to 2,147,483,647.

Command Default

This command has no default settings.

Command Modes

EXEC
Privileged EXEC

Command History

Release	Modification
12.1(1)E	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	This command was implemented on the Supervisor Engine 2 and integrated into Cisco IOS Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

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.

Note For the Cisco 7600 series QDM is not supported on Cisco Optical Services Module (OSM) interfaces.

Examples

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

```
Router# disconnect qdm
```

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

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

Related Commands

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

drop

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

drop

no drop

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Policy-map class configuration (config-pmap-c)

Command History

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

Usage Guidelines

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

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

Examples

The following example shows how to create a traffic class called "class1" and configure it for use in a policy map called "policy1". The policy map (service policy) is attached to output serial interface 2/0. All packets that match access-group 101 are placed in class1. Packets that belong to this class are discarded:

```
Router(config)# class-map class1
Router(config-cmap)# match access-group 101
Router(config-cmap)# exit
Router(config)# policy-map policy1
Router(config-pmap)# class class1
Router(config-pmap-c)# drop
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface serial2/0
Router(config-if)# service-policy output policy1
Router(config-if)# end
```

Related Commands

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

dscp

To change the minimum and maximum packet thresholds for the differentiated services code point (DSCP) value, use the **dscp** command in random-detect-group 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 *dscp-value min-threshold max-threshold* [*mark-probability-denominator*]

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

Syntax Description

dscp-value	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.

Command Default

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

Command Modes

Random-detect-group configuration (cfg-red-group)

Command History

Release	Modification
12.1(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

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

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

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

Table 2 dscp Default Settings

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

Examples

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

```
Router> enable
Router# configure terminal
Router(config)# random-detect-group class1 dscp-based
Router(cfg-red-group)# dscp af22 28 40 10
Router(cfg-red-group)# end
```

Related Commands

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

estimate bandwidth

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

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

no estimate bandwidth

Syntax Description

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

Defaults

Disabled

Command Modes

Policy-map class configuration (config-pmap-c)

Command History

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

Usage Guidelines

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

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

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

Examples

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

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

Related Commands

Command	Description
bandwidth (policy-map class)	Specifies or modifies the bandwidth allocated for a class belonging to a policy map.

exponential-weighting-constant

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

exponential-weighting-constant *exponent*

no exponential-weighting-constant

Syntax Description

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

Command Default

The default weight factor is 9.

Command Modes

Random-detect-group configuration (cfg-red-group)

Command History

Release	Modification
11.1(22)CC	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

When 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 shows how to configure the WRED group called sanjose with a weight factor of 10:

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

Related Commands

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

fair-queue (class-default)

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

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

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

Syntax Description

number-of-dynamic-queues	(Optional) A power of 2 that specifies the number of dynamic queues. Range is from 16 to 4096.

Command Default

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

Command Modes

Policy-map class configuration (config-pmap-c)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

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

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

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

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

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

Table 3 Default Number of Dynamic Queues as a Function of Interface Bandwidth (continued)

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

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

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

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

Examples

The following example shows how to configure 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 shows how to configure 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 64
 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 Versatile Interface Processor (VIP) distributed weighted fair queueing (DWFQ), use the **fair-queue** command in interface configuration mode. To disable DWFQ, use the **no** form of this command.

fair-queue

no fair-queue

Syntax Description

This command has no arguments or keywords.

Command Default

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

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

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
11.1	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **fair-queue** (DWFQ) command enables DWFQ on an interface using a VIP2-40 or greater interface processor.

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

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

Table 5 lists the default queue lengths and thresholds.

Table 5 Default Fair Queue Lengths and Thresholds

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

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).

Note The [**no**] **fair-queue** interface configuration command is not a valid configuration for member links of a multilink PPP interface. The command is only valid when configured on the multilink interface itself. Configuring [**no**] **fair-queue** on a member link interface while bidirectional traffic is flowing could result in the output queue becoming stuck on the multilink interface. If this occurs, a **shut/no shut** of the interface or a reload of the router may be required to clear the problem. An example configuration is provided in the "Examples" section to demonstrate the cause of this problem.

Examples

The following example shows how to enable DWFQ on 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
```

The following example shows a basic configuration of two serial interfaces that results in the output queue becoming stuck on the multilink interface because of the **no fair-queue** command:

```
configure terminal
interface serial0/0/0:0
no fair-queue
no max-reserved-bandwidth 90
tx-queue-limit 19
!
interface serial0/0/1:0
no fair-queue
no max-reserved-bandwidth 90
tx-queue-limit 19
```

Note This sample configuration is provided for demonstration of a problem. Do not use this configuration.

Related Commands

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

fair-queue (policy-map class)

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

fair-queue [*dynamic-queues*]

no fair-queue [*dynamic-queues*]

Syntax Description

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

Command Default

No queues are reserved.

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 and implemented on Versatile Interface Processor (VIP)-enabled Cisco 7500 series routers.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T and was implemented on VIP-enabled Cisco 7500 series routers.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

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 shows how to configure 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 shows how to configure 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)

Note Effective with Cisco IOS XE Release 2.6, Cisco IOS Release 15.0(1)S, and Cisco IOS Release 15.1(3)T, the **fair-queue** command is hidden in interface configuration mode. Although this command is still available in Cisco IOS software, the CLI interactive Help does not display it if you attempt to view it by entering a question mark at the command line.

This command will be completely removed in a future release, which means that you will need to use the appropriate replacement command (or sequence of commands). For more information (including a list of replacement commands), see the *Legacy QoS Command Deprecation* feature document in the *Cisco IOS XE Quality of Service Solutions Configuration Guide* or the *Legacy QoS Command Deprecation* feature document in the *Cisco IOS Quality of Service Solutions Configuration Guide*.

Note Effective with Cisco IOS XE Release 3.2S, the **fair-queue** command is replaced by a modular QoS CLI (MQC) command (or sequence of MQC commands). For the appropriate replacement command (or sequence of commands), see the *Legacy QoS Command Deprecation* feature document in the *Cisco IOS XE Quality of Service Solutions Configuration Guide*.

To enable weighted fair queueing (WFQ), use the **fair-queue** command in interface configuration or policy-map class configuration mode. To disable WFQ, 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 range is 1 to 4096 and the default is 64 messages. When a conversation reaches this threshold, new message packets are discarded. **Note** If you have hierarchical queueing framework (HQF) configured, then the values are 16 to 4096.
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 the tables 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).

Command Default

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 you enable custom queueing or priority queueing 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 6 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 6 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 (config-if)
Policy-map class configuration (config-pmap-c)

Command History

Release	Modification
11.0	This command was introduced.
12.2(13)T	This command was modified to remove Apollo, VINES, and XNS from the list of protocols and traffic stream discrimination fields. These protocols were removed because Apollo Domain, Banyan VINES, and Xerox Network Systems (XNS) were removed in this release.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.
12.2(33)SB	This command's behavior was modified on the Cisco 10000 series router for the PRE3 and PRE4.
12.4(20)T	Support was added for HQF and user-defined classes using the Modular Quality of Service (QoS) Command-Line Interface (CLI) (MQC).
Cisco IOS XE Release 2.6	This command was modified. This command was hidden.
15.0(1)S	This command was modified. This command was hidden.

Release	Modification
15.1(3)T	This command was modified. This command was hidden.
Cisco IOS XE Release 3.2S	This command was replaced by an MQC command (or sequence of MQC commands).

Usage Guidelines

High-Level Overview

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 you enable WFQ on 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 you enable WFQ on 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 message attributes that are used to classify traffic into data streams.

Table 6 Weighted Fair Queueing Traffic Stream Discrimination Fields

Forwarder	Fields Used
AppleTalk	• Source net, node, socket • Destination net, node, socket • Type
Connectionless Network Service (CLNS)	• Source network service access point (NSAP) • Destination NSAP
DECnet	• Source address • Destination address
Frame Relay switching	• Data-link connection identified (DLCI) value

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

Forwarder	Fields Used
IP	• Type of service (ToS) • IP protocol • Source IP address (if message is not fragmented) • Destination IP address (if message is not fragmented) • Source TCP/UDP port • Destination TCP/UDP port
Transparent bridging	• Unicast: source MAC, destination MAC • Ethertype Service Advertising Protocol (SAP)/Subnetwork Access Protocol (SNAP) multicast: destination MAC address
Source-route bridging	• Unicast: source MAC, destination MAC • SAP/SNAP multicast: destination MAC address
Novell NetWare	• Source/destination network/host/socket • Level 2 protocol
All others (default)	• Control protocols (one queue per protocol)

IP Precedence

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.

FECN and BECN

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, Custom Queueing, and Priority Queueing

Fair queueing is supported for all LAN and line (WAN) protocols except X.25, including LAPB and SDLC; see the notes in the section "Command Default." 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.

RSVP

When you configure Resource Reservation Protocol (RSVP) 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*.

Cisco 10000 Series Routers

In Cisco IOS Release 12.2(33)SB, the router removes the **no fair-queue** command from serial interfaces.

HQF

Beginning with Cisco IOS Release 12.4(20)T, if your image has HQF support, the **fair-queue** command is not enabled automatically under class default. You should enable the **fair-queue** command and any other supported queueing features before using an HQF-capable image.

Examples

The following example shows how to enable WFQ on serial interface 0, with a congestive threshold of 300. This threshold means that messages are 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 shows how to request 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
```

The following example shows how to apply the **fair-queue** command to a user-defined class:

```
policy-map p1
 class c1
  bandwidth 1000
  fair-queue
```

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.

Command	Description
priority-group	Assigns the specified priority list to an interface.
priority-list default	Assigns a priority queue for those packets that do not match any other rule in the priority list.
show interfaces	Displays statistics for all interfaces configured on the router or access server.
show queue	Displays the contents of packets inside a queue for a particular interface or VC.
show queueing	Lists all or selected configured queueing strategies.
tx-queue-limit	Controls the number of transmit buffers available to a specified interface on the MCI and SCI cards.

fair-queue aggregate-limit

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

fair-queue aggregate-limit *aggregate-packets*

no fair-queue aggregate-limit

Syntax Description

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

Command Default

The total number of packets allowed is based on the transmission rate of the interface and the available buffer space on the VIP.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
11.1 CC	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

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

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

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

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

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

Examples

The following example shows how to set the aggregate limit to 54 packets:

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

Related Commands

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

fair-queue individual-limit

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

fair-queue individual-limit *individual-packet*

no fair-queue individual-limit

Syntax Description

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

Command Default

Half of the aggregate queue limit

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
11.1 CC	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

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

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

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

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

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

Examples

The following example shows how to set the individual queue limit to 27:

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

Related Commands

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

fair-queue limit

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

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

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

Syntax Description

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

Command Default

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 (config-if)

Command History

Release	Modification
11.1 CC	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

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

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

Examples

The following example shows how to set the individual queue limit for ToS group 3 to 20:

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

Related Commands

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

fair-queue qos-group

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

fair-queue qos-group

no fair-queue qos-group

Syntax Description

This command has no arguments or keywords.

Command Default

QoS-group-based DWFQ is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
11.1CC	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

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

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

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

Examples

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

```
interface Hssi0/0/0
 description 45Mbps to R2
 ip address 10.200.14.250 255.255.255.252
 fair-queue qos-group
 fair-queue qos-group 1 weight 5
 fair-queue qos-group 2 weight 5
 fair-queue qos-group 3 weight 10
```

```
fair-queue qos-group 4 weight 10
fair-queue qos-group 5 weight 10
fair-queue qos-group 6 weight 15
fair-queue qos-group 7 weight 20
fair-queue qos-group 8 weight 29
```

Related Commands

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

fair-queue tos

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

fair-queue tos

no fair-queue tos

Syntax Description

This command has no arguments or keywords.

Command Default

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 (config-if)

Command History

Release	Modification
11.1CC	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

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 shows how to enable ToS-based DWFQ on the High-Speed Serial Interface (HSSI) interface 0/0/0:

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

Related Commands

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

fair-queue weight

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

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

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

Syntax Description

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

Command Default

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 (config-if)

Command History

Release	Modification
11.1CC	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

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

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

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

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

For ToS-based DWFQ, remember the following guidelines:

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

Examples

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

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

Related Commands

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

feedback

To enable the context-status feedback messages from the interface or link, use the **feedback** command in IP Header Compression (IPHC)-profile configuration mode. To disable the context-status feedback messages, use the **no** form of this command.

feedback

no feedback

Syntax Description

This command has no arguments or keywords.

Command Default

Context-status feedback messages are enabled.

Command Modes

IPHC-profile configuration (config-iphcp)

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

Intended for Use with IPHC Profiles

The **feedback** command is intended for use as part of an IPHC profile. An IPHC profile is used to enable and configure header compression on your network. For more information about using IPHC profiles to configure header compression, see the "Header Compression" module and the "Configuring Header Compression Using IPHC Profiles" module of the *Cisco IOS Quality of Service Solutions Configuration Guide*, Release 12.4T.

Restriction

There are two types of IPHC profiles: Internet Engineering Task Force (IETF) profiles and van-jacobson profiles. The **feedback** command is supported for IETF IPHC profiles only. The **feedback** command is not supported for van-jacobson IPHC profiles. For more information about IPHC profile types, see the "Header Compression" section of the *Cisco IOS Quality of Service Solutions Configuration Guide*, Release 12.4T.

Prerequisite

Before using the **feedback** command, you must enable either TCP header compression or non-TCP header compression. To enable TCP header compression, use the **tcp** command. To enable non-TCP header compression, use the **non-tcp** command.

Disabling of Context-Status Messages

During header compression, a session context is defined. For each context, the session state is established and shared between the compressor and the decompressor. The context state consists of the full IP/UDP/RTP, IP/UDP, or IP/TCP headers, a few first-order differential values, a link sequence number, a generation number, and a delta encoding table.

When the decompressor loses synchronization with the compressor, the decompressor sends a context status message to the compressor with a list of context IDs to invalidate. The compressor then sends a full-header packet to the decompressor to reestablish a consistent state. Note that all packets for the invalid context IDs are discarded until a full-header packet is received for that context ID.

You can disable the sending of context-status messages either when the time it takes for the packet to traverse the uplink and the downlink portions of the data path is greater than the refresh period (in which case, the sending of the context-status message would not be useful) or when a feedback path does not exist.

Examples

The following is an example of an IPHC profile called profile2. In this example, context-status feedback messages have been disabled.

```
Router> enable
Router# configure terminal
Router(config)# iphc-profile profile2 ietf
Router(config-iphcp)# non-tcp
Router(config-iphcp)# no feedback
Router(config-iphcp)# end
```

Related Commands

Command	Description
iphc-profile	Creates an IPHC profile.
non-tcp	Enables non-TCP header compression within an IPHC profile.
tcp	Enables TCP header compression within an IPHC profile.

frame-relay interface-queue priority

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

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

no frame-relay interface-queue priority

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

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

no frame-relay interface-queue priority

Syntax Description

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

Command Default

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

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

Command Modes

Interface configuration
Map-class configuration

Command History

Release	Modification
12.1(2)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

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

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

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

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

Examples

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

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

Related Commands

Command	Description
debug priority	Displays priority queueing events.
show frame-relay pvc	Displays statistics about PVCs for Frame Relay interfaces.
show interfaces	Displays statistics for all interfaces configured on the router or access server.
show queue	Displays the contents of packets inside a queue for a particular interface or VC.
show queueing	Lists all or selected configured queueing strategies.

frame-relay ip rtp compression-connections

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

frame-relay ip rtp compression-connections *number*

no frame-relay ip rtp compression-connections

Syntax Description

number	Maximum number of RTP header compression connections. The range is from 3 to 256.

Command Default

256 header compression connections

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.1(2)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Before you can configure the maximum number of connections, RTP header compression must be configured on the interface using the **frame-relay ip rtp header-compression** command.

The number of RTP header compression connections must be set to the same value at each end of the connection.

Examples

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

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

Related Commands

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

frame-relay ip rtp header-compression

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

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

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

Syntax Description

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

Command Default

Disabled.

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

Command Modes

Interface configuration

Command History

Release	Modification
11.3	This command was introduced.
12.3(2)T	This command was integrated into Cisco IOS Release 12.3(2)T. This command was modified to include the **periodic-refresh** keyword.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

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

Examples

The following example shows how to enable RTP header compression for all Frame Relay maps on a physical interface:

```
Router> enable
Router# configure terminal
Router(config)# interface Serial2/0.1
```

```
Router(config-if)# frame-relay ip rtp header-compression
Router(config-if)# end
```

The following example shows how to enable RTP header compression, and the optional **periodic-refresh** keyword is specified:

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

Related Commands

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

frame-relay ip rtp priority

Note Effective with Cisco IOS XE Release 2.6, Cisco IOS Release 15.0(1)S, and Cisco IOS Release 15.1(3)T, the **frame-relay ip rtp priority** command is hidden. Although this command is still available in Cisco IOS software, the CLI interactive Help does not display it if you attempt to view it by entering a question mark at the command line.

This command will be completely removed in a future release, which means that you will need to use the appropriate replacement command (or sequence of commands). For more information (including a list of replacement commands), see the *Legacy QoS Command Deprecation* feature document in the *Cisco IOS XE Quality of Service Solutions Configuration Guide* or the *Legacy QoS Command Deprecation* feature document in the *Cisco IOS Quality of Service Solutions Configuration Guide*.

Note Effective with Cisco IOS XE Release 3.2S, the **frame-relay ip rtp priority** command is replaced by a modular QoS CLI (MQC) command (or sequence of MQC commands). For the appropriate replacement command (or sequence of commands), see the *Legacy QoS Command Deprecation* feature document in the *Cisco IOS XE Quality of Service Solutions Configuration Guide*.

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

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

no frame-relay ip rtp priority

Syntax Description

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

Command Default

No default behavior or values

Command Modes

Map-class configuration

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Release	Modification
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.6	This command was modified. This command was hidden.
15.0(1)S	This command was modified. This command was hidden.
15.1(3)T	This command was modified. This command was hidden.
Cisco IOS XE Release 3.2S	This command was replaced by an MQC command (or sequence of MQC commands).

Usage Guidelines

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

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

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

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

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

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

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

Examples

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

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

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

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

Related Commands

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

frame-relay ip tcp compression-connections

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

frame-relay ip tcp compression-connections *number*

no frame-relay ip tcp compression-connections

Syntax Description

number	Maximum number of TCP header compression connections. The range is from 3 to 256.

Command Default

256 header compression connections

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.1(2)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Before you can configure the maximum number of connections, TCP header compression must be configured on the interface using the **frame-relay ip tcp header-compression** command.

The number of TCP header compression connections must be set to the same value at each end of the connection.

Examples

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

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

Related Commands

Command	Description
frame-relay ip tcp header-compression	Enables TCP header compression for all Frame Relay maps on a physical interface.
frame-relay map ip compress	Enables both RTP and TCP header compression on a link.

Command	Description
frame-relay map ip tcp header-compression	Assigns header compression characteristics to an IP map that differ from the compression characteristics of the interface with which the IP map is associated.
show frame-relay ip tcp header-compression	Displays statistics and TCP/IP header compression information for the interface.

frame-relay ip tcp header-compression

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

frame-relay ip tcp header-compression [**passive**]

no frame-relay ip tcp header-compression

Syntax Description

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

Command Default

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

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

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

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

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

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

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

Examples

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

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

Related Commands

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

frame-relay map ip compress

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

frame-relay map ip *ip-address dlci* [**broadcast**] **compress** [**active** | **passive**] [**connections** *number*]

Syntax Description

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

Command Default

RTP and TCP header compression are disabled.

The default maximum number of header compression connections is 256.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
11.3	This command was introduced.
12.1(2)T	This command was modified to enable the configuration of the maximum number of header compression connections.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command does not have a "no" form. That is, a command called **no frame-relay map ip compress** does not exist.

Examples

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

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

Related Commands

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

frame-relay map ip nocompress

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

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

Syntax Description

ip-address	IP address of the destination or next hop.
dlci	Data-link connection identifier (DLCI) number.
broadcast	(Optional) Forwards broadcasts to the specified IP address.

Command Default

No default behaviors or values

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
11.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command does not have a "no" form. That is, a command called **no frame-relay map ip nocompress** does not exist.

Examples

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

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

Related Commands

Command	Description
frame-relay ip rtp header-compression	Enables RTP header compression for all Frame Relay maps on a physical interface.
frame-relay ip tcp header-compression	Enables TCP header compression for all Frame Relay maps on a physical interface.
frame-relay map ip compress	Enables RTP and TCP header compression on a link.

Command	Description
show frame-relay ip rtp header-compression	Displays RTP header compression statistics for Frame Relay.
show frame-relay ip tcp header-compression	Displays statistics and TCP/IP header compression information for the interface.

frame-relay map ip rtp header-compression

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

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

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

Syntax Description

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

Command Default

Disabled.

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

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

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
11.3	This command was introduced.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T. This command was modified to enable the configuration of the maximum number of header compression connections.
12.3(2)T	This command was modified to include the **periodic-refresh** keyword.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

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

Examples

The following example shows how to enable RTP header compression on the Serial1/2.1 subinterface and set the maximum number of RTP header compression connections at 64:

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

The following example shows how to enable RTP header compression on the Serial1/1.0 subinterface and how to use the optional **periodic-refresh** keyword in the configuration:

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

Related Commands

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

group (service group)

To add a member to a service group, use the **group** command in Ethernet service configuration mode. To remove a member from a service group, use the **no** form of this command.

group *service-group-identifier*

no group *service-group-identifier*

Syntax Description

service-group-identifier	Number of an existing service group to which the member will be added or removed.

Command Default

A member is not added.

Command Modes

Ethernet service configuration (config-if-srv)

Command History

Release	Modification
12.2(33)SRE	This command was introduced.

Usage Guidelines

Use the **group** (service group) command to add members (for example, service instances) to service groups and to remove members from service groups.

Cisco 7600 Series Router and Service Instances From Multiple Interfaces Are Not Allowed

The Cisco 7600 series router does not allow service instances to join the same group from multiple interfaces. On the Cisco 7600 series router, group members must come from the same interface, as shown the sample configuration below:

```
interface GigabitEthernet 2/0/0
 service instance 1 ethernet
  group 32
  service-policy output policy3
 service instance 2 ethernet
  group 32
  service instance 3 ethernet
  group 37
interface GigabitEthernet 2/0/1
  service instance 1 ethernet
   group 32 |<--Disallowed because this group has members in g2/0/0 already| |
```

Examples

The following example shows how to add service instance 200 to service group 20:

```
Router> enable
Router# configure terminal
Router# interface GigabitEthernet 1/0/0
Router(config-if)# service instance 200 ethernet
Router(config-if-srv)# group 20
```

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

hw-module slot (ESP Scheduling)

To handle the oversubscription of packets at the ingress side of an Embedded Service Processor (ESP), provide either a minimum bandwidth or a specific weight to a SIP based on which the excess bandwidth is divided among the low priority packets of the SIPs. Execute the **hw-module slot** command in global configuration mode. Use the **no** form of this command to either remove the minimum bandwidth assigned to a SIP or remove the excess weight configured for a SIP.

hw-module slot *slot-number* {**qos input link** {**A** | **B**}} [**bandwidth** *bandwidth_value*] [**weight** *weight_value*]

Syntax Description

slot-number	The slot number of the SIP for which the minimum bandwidth or excess weight needs to be configured.
qos	Enables configuration of the quality of service (QoS) policy to solve the oversubscription problem on the ingress side.
input	Enables the scheduling of packets on the ingress side.
link	Enables the configuration of each ESI link between the SIP and the ESP.
A	Specifies the A input QoS link for configuration of parameters.
B	Specifies the B input QoS link for configuration of parameters.
bandwidth	Provisions the configuration of a committted minimum bandwidth for the specified SIP.
bandwidth_value	The minimum bandwidth value in Kbps to be assigned to the SIP.
weight	Assigns the excess weight available for sharing to the SIP. Based on the excess weight assigned to the SIP, the available bandwidth that is left after processing the high priority packets is divided among the SIPs of low priority packets.
weight_value	The weight value to be assigned to the SIP for dividing the free bandwidth among the SPAs. The valid range for weightage value is 5 to 100.

Defaults

By default, the high priority packets are processed first.

Command Modes

Global configuration mode (config)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced as the **hw-module slot** (QoS) command.
Cisco IOS XE Release 3.1S	The command was modified. The command was changed to the **hw-module slot** (ESP Scheduling) command and the **link A** and **link B** keyword sequences were added.

Usage Guidelines

Oversubscription occurs at the SIP and ESP levels. To handle the oversubscription problem at the ESP level, use the **hw-module slot** command. A minimum bandwidth is assigned to a SIP that is connected through the ESI links, and a weight is assigned to the SIPs to divide the available excess bandwidth among the low priority packets.

To configure the minimum bandwidth service for a SIP, execute the **hw-module slot** *slot-number* **qos input link** *link-index* **bandwidth** *value_in_kbps* command.

To assign a specific weight value to an ESI link connecting a SIP and an ESP, execute the **hw-module slot** *slot-number* **qos input link** *link-index* **weight** *weight-value* command.

Examples

The following example shows how to assign a minimum bandwidth to ESI Link A:

```
Router# config
Router(config)# hw-module slot 1 qos input link A bandwidth 512
```

The following example shows how to assign an excess weight of 150 to a SIP at slot 1 and connected through ESI Link A:

```
Router# config
Router(config)# hw-module slot 1 qos input link A weight 150
```

The following example shows how to display the available link options for ESP40 and SIP40 cards when there are two links configured:

```
Router(config)# hw-module slot 0 qos input link ?

 A  ESI Link A (Bay 0,2)
 B  ESI Link B (Bay 1,3)
```

The following example shows how to display the available link options for ESP40 and SIP10 cards when there is one link configured:

```
Router(config)# hw-module slot 1 qos input link ?

 A  ESI Link A (All Bays)
```

Related Commands

Command	Description
show platform hardware slot {f0 | f1} serdes qos	Displays the excess weight and committed bandwidth settings for ESPs.

hw-module subslot (Channelized SPA Scheduling)

To handle the oversubscription of packets at the ingress side of a SIP for a channelized SPA, assign the excess weight to the entire channelized SPA using the **hw-module subslot** command in global configuration mode. Use the **no** form of this command to remove the excess weight configured for the SIP.

hw-module subslot *slot/subslot* **qos** [**weight** *weightage_value*]

no hw-module subslot *slot/subslot* **qos** [**weight** *weightage_value*]

Syntax Description

slot-subslot	The slot number of the SIP, and the subslot number of the channelized SPA for which the excess weight needs to be configured.
qos	Enables the configuration of the excess weight for low priority packets on a channelized SPA to solve the oversubscription problem on the ingress side.
weight	Assigns the excess weight to the channelized SPA. Based on the excess weight assigned to the channelized SPA, the available bandwidth that is left after processing the high priority packets is divided among the SPAs.
weightage_value	The weightage value to be assigned to the channelized SPA for dividing the excess bandwidth among the channelized SPAs. The valid range for weightage value is 5 to 100.

Defaults

By default, the high priority packets are processed first.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Usage Guidelines

A SIP contains different types of SPAs in each of its slots. To assign the excess weight to a channelized SPA for low priority packets, the **hw-module subslot** *slot-subslot* **qos weight** *weight-value* command has been introduced.

Note The option to configure minimum bandwidth for ‘strict-priority’ queue at port-level (interface-level) is deprecated as it is not applicable to the current mode of operation. Existing configuration will be rejected with an error.

Examples

The following example shows how to assign an excess weight of 200 to a channelized SPA located at slot 1 and subslot 0:

```
Router# config
Router(config)# hw-module subslot 1/0 qos weight 200
```

Related Commands

Command	Description
show platform hardware	Displays excess weight and committed bandwidth settings configured on a SIP or SPA respectively.