random-detect

To enable WRED or Distributed WRED (DWRED), use the **random-detect** interface configuration command. To disable WRED or DWRED, use the **no** form of this command.

random-detect [*weighting*]

no random-detect

Syntax Description

weighting	(Optional) Exponential weighting constant in the range 1 to 16 used to determine the rate that packets are dropped when congestion occurs. The default is 10 (that is, drop 1 packet every 210).

Defaults

WRED and DWRED are disabled by default.

Command Modes

Interface configuration

Command History

Release	Modification
11.1 CC and 11.2	This command was introduced.

Usage Guidelines

WRED is a congestion avoidance mechanism that slows traffic by randomly dropping packets when there is congestion. WRED is only useful with protocols like TCP that respond to dropped packets by decreasing the transmission rate.

The router automatically determines parameters to use in the WRED calculations. To change these parameters, use the **random-detect precedence** command.

The WRED feature is supported on these Cisco router platforms:

- Cisco 1600 series
- Cisco 2500 series
- Cisco 3600 series
- Cisco 4000 series (including 4500 and 4700 series)
- Cisco 7200 series
- Cisco 7500 series with RSP interface card

The DWRED feature is only supported on Cisco 7000 series routers with an RSP7000 card and Cisco 7500 series routers with a VIP2-40 or greater interface processor. A VIP2-50 interface processor is strongly recommended when the aggregate line rate of the port adapters on the VIP is greater than DS3. A VIP2-50 interface processor is required for OC-3 rates. To use DWRED, distributed Cisco Express Forwarding (DCEF) switching must first be enabled on the interface. For more information on DCEF, refer to the *Cisco IOS Switching Services Configuration Guide* and the *Cisco IOS Switching Services Command Reference*.

Examples

The following example configures WRED on the HSSI 0/0/0 interface:

```
router(config)# interface Hssi0/0/0
router(config-if)# random-detect
```

Related Commands

Command	Description
random-detect exponential-weighting-constant	Configures the WRED and DWRED exponential weight factor for the average queue size calculation.
random-detect precedence	Configures WRED and DWRED parameters for a particular IP precedence.
show interfaces	Displays statistics for all interfaces configured on the router or access server.
show queue	Lists fair queueing configuration and statistics for a particular interface.
show queueing	Lists all or selected configured queueing strategies.

random-detect exponential-weighting-constant

To configure the Weighted Random Early Detection (WRED) and Distributed WRED (DWRED) exponential weight factor for the average queue size calculation, use the **random-detect exponential-weighting-constant** interface configuration command. To return the value to the default, use the **no** form of this command.

random-detect exponential-weighting-constant *exponent*

no random-detect exponential-weighting-constant

Syntax Description

exponent	Exponent from 1 to 16 used in the average queue size calculation. The default exponential weight factor is 9.

Defaults

This command is disabled by default.

Command Modes

Interface configuration

Command History

Release	Modification
11.1 CC	This command was introduced.

Usage Guidelines

WRED is a congestion avoidance mechanism that slows traffic by randomly dropping packets when there is congestion. WRED is only useful with protocols like TCP, which respond to dropped packets by decreasing the transmission rate.

Use this command to change the exponent used in the average queue size calculation for the WRED and DWRED services.

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.

The WRED feature is supported on these Cisco router platforms:

- Cisco 1600 series
- Cisco 2500 series
- Cisco 3600 series
- Cisco 4000 series (including 4500 and 4700 series)
- Cisco 7200 series
- Cisco 7500 series with RSP interface card

The DWRED feature is only supported on Cisco 7000 series routers with an RSP7000 card and Cisco 7500 series routers with a VIP2-40 or greater interface processor. A VIP2-50 interface processor is strongly recommended when the aggregate line rate of the port adapters on the VIP is greater than DS3. A VIP2-50 interface processor is required for OC-3 rates. To use DWRED, Distributed Cisco Express Forwarding (DCEF) switching must first be enabled on the interface. For more information on DCEF, refer to the *Cisco IOS Switching Services Configuration Guide* and the *Cisco IOS Switching Services Command Reference*.

Examples

The following example configures WRED on an interface with a weight factor of 10:

```
router(config)# interface Hssi0/0/0
router(config-if)# description 45Mbps to R1
router(config-if)# ip address 200.200.14.250 255.255.255.252
router(config-if)# random-detect
router(config-if)# random-detect exponential-weighting-constant 10
```

Related Commands

Command	Description
random-detect	Enables WRED or DWRED.
random-detect precedence	Configures WRED and DWRED parameters for a particular IP precedence.
show interfaces	Displays statistics for all interfaces configured on the router or access server.
show queue	Lists fair queueing configuration and statistics for a particular interface.
show queueing	Lists all or selected configured queueing strategies.

random-detect precedence

To configure Weighted Random Early Detection (WRED) and Distributed WRED (DWRED) parameters for a particular IP precedence, use the **random-detect precedence** interface configuration command. To return the values to the default for the precedence, use the **no** form of this command.

random-detect precedence *precedence min-threshold max-threshold mark-prob-denominator*

no random-detect precedence *precedence min-threshold max-threshold mark-prob-denominator*

Syntax Description

precedence	IP precedence number. The value range is 0 to 7 and RSVP. For Cisco 7000 series routers with an RSP7000 interface processor and Cisco 7500 series routers with a VIP2-40 interface processor (VIP2-50 interface processor strongly recommended), the precedence value ranges from 0 to 7 only; see Table 379.
min-threshold	Minimum threshold in number of packets. The value range of this argument is 1 to 4096. When the average queue length reaches the minimum threshold, WRED drops all packets with the specified IP precedence.
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 IP precedence.
mark-prob-denominator	Denominator for the fraction of packets dropped when the average queue depth is at the maximum threshold. For example, if the denominator is 512, one out of every 512 packets is dropped when the average queue is at the maximum threshold. The value range is 1 to 65536. The default is 10; one out of every ten packets is dropped at the maximum threshold.

Defaults

For all precedences, the *mark-prob-denominator* is 10, and the *max-threshold* is based on the output buffering capacity and the transmission speed for the interface.

The default *min-threshold* depends on the precedence. The *min-threshold* for IP precedence 0 corresponds to half of the *max-threshold*. The values for the remaining precedences fall between half the *max-threshold* and the *max-threshold* at evenly spaced intervals.

Table 379 lists the default minimum threshold value for each IP precedence.

Table 379 Default WRED and DWRED Minimum Threshold Values

	Minimum Threshold Value (Fraction of Maximum Threshold Value)	
IP Precedence	**WRED**	**DWRED**
0	9/18	8/16
1	10/18	9/16
2	11/18	10/16
3	12/18	11/16

Table 379 Default WRED and DWRED Minimum Threshold Values (continued)

	Minimum Threshold Value (Fraction of Maximum Threshold Value)	
IP Precedence	**WRED**	**DWRED**
4	13/18	12/16
5	14/18	13/16
6	15/18	14/16
7	16/18	15/16
RSVP	17/18	N/A

Command Modes

Interface configuration

Command History

Release	Modification
11.1 CC	This command was introduced.

Usage Guidelines

When you configure the **random-detect** command on an interface, packets are given preferential treatment based on the IP precedence of the packet. Use the **random-detect precedence** command to adjust the treatment for different IP precedences.

If you want WRED to ignore the precedence when determining which packets to drop, enter this command with the same parameters for each precedence. Remember to use reasonable values for the minimum and maximum thresholds.

Note 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.

The WRED feature is supported on these Cisco router platforms:

- Cisco 1600 series
- Cisco 2500 series
- Cisco 3600 series
- Cisco 4000 series (including 4500 and 4700 series)
- Cisco 7200 series
- Cisco 7500 series with RSP interface card

The DWRED feature is only supported on Cisco 7000 series routers with an RSP7000 card and Cisco 7500 series routers with a VIP2-40 or greater interface processor. A VIP2-50 interface processor is strongly recommended when the aggregate line rate of the port adapters on the VIP is greater than DS3. A VIP2-50 interface processor is required for OC-3 rates. To use DWRED, Distributed Cisco Express Forwarding (DCEF) switching must first be enabled on the interface. For more information on DCEF, refer to the *Cisco IOS Switching Services Configuration Guide* and the *Cisco IOS Switching Services Command Reference*.

Examples

The following example enables WRED on the interface and specifies parameters for the different IP precedences:

```
router(config)# interface Hssi0/0/0
router(config-if)# description 45Mbps to R1
router(config-if)# ip address 200.200.14.250 255.255.255.252
router(config-if)# random-detect
router(config-if)# random-detect precedence 0 32 256 100
router(config-if)# random-detect precedence 1 64 256 100
router(config-if)# random-detect precedence 2 96 256 100
router(config-if)# random-detect precedence 3 120 256 100
router(config-if)# random-detect precedence 4 140 256 100
router(config-if)# random-detect precedence 5 170 256 100
router(config-if)# random-detect precedence 6 290 256 100
router(config-if)# random-detect precedence 7 210 256 100
router(config-if)# random-detect precedence rsvp 230 256 100
```

Related Commands

Command	Description
random-detect	Enables WRED or DWRED.
random-detect exponential-weighting-constant	Configures the WRED and DWRED exponential weight factor for the average queue size calculation.
show interfaces	Displays statistics for all interfaces configured on the router or access server.
show queue	Lists fair queueing configuration and statistics for a particular interface.
show queueing	Lists all or selected configured queueing strategies.

rate-limit

To configure committed access rate (CAR) and Distributed CAR (DCAR) policies, use the **rate-limit** interface configuration command. To remove the rate limit from the configuration, use the **no** form of this command.

rate-limit {**input** | **output**} [**access-group** [**rate-limit**] *acl-index*] *bps burst-normal burst-max* **conform-action** *action* **exceed-action** *action*

no rate-limit {**input** | **output**} [**access-group** [**rate-limit**] *acl-index*] *bps burst-normal burst-max* **conform-action** *action* **exceed-action** *action*

Syntax Description

input	Applies this CAR traffic policy to packets received on this interface.
output	Applies this CAR traffic policy to packets sent on this interface.
access-group	(Optional) Applies this CAR traffic policy to the specified access list.
rate-limit	(Optional) The access list is a rate-limit access list.
acl-index	(Optional) Access list number.
bps	Average rate in bits per second. The value must be in increments of 8 kbps.
burst-normal	Normal burst size in bytes. The minimum value is bps divided by 2000.
burst-max	Excess burst size in bytes.
conform-action	Action to take on packets that conform to the rate limit.
action	Action to take on packets. Specify one of the following keywords: • **continue**—Evaluate the next **rate-limit** command. • **drop**—Drop the packet. • **set-prec-continue** *new-prec*—Set the IP precedence and evaluate the next **rate-limit** command. • **set-prec-transmit** *new-prec*—Set the IP precedence and transmit the packet. • **transmit**—Transmit the packet.
exceed-action	Action to take on packets that exceed the rate limit.

Defaults

CAR and DCAR are disabled on the interface.

Command Modes

Interface configuration

Command History

Release	Modification
11.1 CC	This command was introduced.

Usage Guidelines

Use this command to configure your CAR policy on an interface. To specify multiple policies, enter this command once for each policy.

Distributed CAR is only supported on Cisco 7000 series routers with an RSP7000 or Cisco 7500 series routers with VIP2-40 or greater interface processor. A VIP2-50 interface processor is strongly recommended when the aggregate line rate of the port adapters on the VIP is greater than DS3. A VIP2-50 interface processor is required for OC-3 rates.

CAR and DCAR can only be used with IP traffic. Non-IP traffic is not rate limited.

CAR and DCAR can be configured on an interface or subinterface. However, CAR and DCAR are not supported on the Fast EtherChannel, tunnel, or PRI interfaces, nor on any interface that does not support Cisco Express Forwarding (CEF).

CEF must be enabled on the interface before you configure CAR or DCAR.

Examples

The example illustrated below limits the rate by application:

- All World Wide Web traffic is transmitted. However, the IP precedence for Web traffic that conforms to the first rate policy is set to 5. For nonconforming traffic, the IP precedence is set to 0 (best effort).
- FTP traffic is transmitted with an IP precedence of 5 if it conforms to the second rate policy. If the FTP traffic exceeds the rate policy, it is dropped.
- Any remaining traffic is limited to 8 Mbps, with a normal burst size of 16000 bytes and an excess burst size of 24000 bytes. Traffic that conforms is transmitted with an IP precedence of 5. Traffic that does not conform is dropped.

Notice that two access lists are created to classify the Web and FTP traffic so that they can be handled separately by the CAR feature.

```
router(config)# interface Hssi0/0/0
router(config-if)# description 45Mbps to R2
router(config-if)# rate-limit input access-group 101 20000000 24000 32000
  conform-action set-prec-transmit 5 exceed-action set-prec-transmit 0
router(config-if)# rate-limit input access-group 102 10000000 24000 32000
  conform-action set-prec-transmit 5 exceed-action drop
router(config-if)# rate-limit input 8000000 16000 24000 conform-action
  set-prec-transmit 5 exceed-action drop
router(config-if)# ip address 200.200.14.250 255.255.255.252
!
router(config-if)# access-list 101 permit tcp any any eq www
router(config-if)# access-list 102 permit tcp any any eq ftp
```

Related Commands

Command	Description
access-list rate-limit	Configures an access list for use with CAR policies.
show access-lists rate-limit	Displays information about rate-limit access lists.
show interfaces rate-limit	Displays information about CAR for an interface.
show ip rsvp installed	Displays RSVP-related installed filters and corresponding bandwidth information.

set ip precedence

To set the precedence value in the IP header, use the **set ip precedence** route-map configuration command. To leave the precedence value alone, use the **no** form of this command.

set ip precedence [*number* | *name*]

no set ip precedence

Syntax Description

(Optional) A number or name that sets the precedence bits in the IP header. The values for *number* and the corresponding *name* are as follows, listed from least to most important:

number	*name*
0	**routine**
1	**priority**
2	**immediate**
3	**flash**
4	**flash-override**
5	**critical**
6	**internet**
7	**network**

Defaults

This command is disabled by default.

Command Modes

Route-map configuration

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

You can set the precedence using either a number or the corresponding name. Once the IP precedence bits are set, other QoS services such as weighted fair queueing (WFQ) and Weighted Random Early Detection (WRED) then operate on the bit settings.

The network gives priority (or some type of expedited handling) to the marked traffic through the application of WFQ or WRED at points downstream in the network. Typically, you would set IP precedence at the edge of the network (or administrative domain) and have queueing act on it thereafter. WFQ can speed up handling for high precedence traffic at congestion points. WRED ensures high precedence traffic has lower loss rates than other traffic during times of congestion.

The mapping from keywords such as **routine** and **priority** to a precedence value is useful only in some instances. That is, the use of the precedence bit is evolving. You can define the meaning of a precedence value by enabling other features that use the value. In the case of Cisco's high-end Internet QoS, IP precedences can be used to establish classes of service that do not necessarily correspond numerically to better or worse handling in the network.

Use the **route-map** (IP) global configuration command with **match** and **set** route-map configuration commands to define the conditions for redistributing routes from one routing protocol into another, or for policy routing. Each **route-map** command has an associated list of **match** and **set** commands. The **match** commands specify the match criteria—the conditions under which redistribution or policy routing is allowed for the current **route-map** command. The **set** commands specify the set actions—the particular redistribution or policy routing actions to perform if the criteria enforced by the **match** commands are met. The **no route-map** command deletes the route map.

The **set** route-map configuration commands specify the redistribution set actions to be performed when all of a route map's match criteria are met.

Examples

The following example sets the IP precedence to 5 (critical) for packets that pass the route-map match:

```
router(config)# interface serial 0
router(config-if)# ip policy route-map texas

router(config)# route-map texas
router(config)# match length 68 128
router(config)# set ip precedence 5
```

Related Commands

Command	Description
fair-queue	Enables WFQ for an interface.
ip policy route-map	Identifies a route map to use for policy routing on an interface.
random-detect	Enables WRED or DWRED.
rate-limit	Configures CAR and DCAR policies.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
traffic-shape adaptive	Configures a Frame Relay subinterface to estimate the available bandwidth when BECNs are received.
traffic-shape fecn-adapt	Replies to messages with the FECN bit (which are set with TEST RESPONSE messages with the BECN bit set).
traffic-shape group	Enables traffic shaping based on a specific access list for outbound traffic on an interface.
traffic-shape rate	Enables traffic shaping for outbound traffic on an interface.

set ip qos-group

To set a group ID that can be used later to classify packets, use the **set ip qos-group** route-map configuration command. To remove the group ID, use the **no** form of this command.

set ip qos-group *group-id*

no set ip qos-group *group-id*

Syntax Description

group-id	Group ID number in the range 0 to 99.

Defaults

This command is disabled by default. No group ID is specified.

Command Modes

Route-map configuration

Command History

Release	Modification
11.1 CC	This command was introduced.

Usage Guidelines

This command allows you to set a group ID in the routing table that can be used later to classify packets into QoS groups based on prefix, autonomous system, and community string. These packets can then be rate limited or weighted fair queued based on the QoS group ID.

To display QoS group information, use the **show ip cef** command.

Examples

The following example sets the QoS group to 1 for all packets that match community 1. These packets are then rate limited based on the QoS group ID.

```
router# configure terminal
router(config)# route-map precedence-map permit 10
router(config)# match community 1
router(config)# set ip qos-group 1
router(config)# interface hssi0/0/0
router(config-if)# bgp-policy source qos-group
router(config-if)# end
```

show access-lists rate-limit

To display information about rate-limit access lists, use the **show access-lists rate-limit** EXEC command.

show access-lists rate-limit [*acl-index*]

Syntax Description

acl-index	(Optional) Rate-limit access list number from 1 to 199.

Command Modes

EXEC

Command History

Release	Modification
11.1 CC	This command was introduced.

Examples

The following is sample output from the **show access-lists rate-limit** command:

```
Router# show access-lists rate-limit

Rate-limit access list 1
    0
Rate-limit access list 2
    1
Rate-limit access list 3
    2
Rate-limit access list 4
    3
Rate-limit access list 5
    4
Rate-limit access list 6
    5
Rate-limit access list 9
    mask FF
Rate-limit access list 10
    mask 0F
Rate-limit access list 11
    mask F0
Rate-limit access list 100
    1001.0110.1111
Rate-limit access list 101
    00E0.34B8.D840
Rate-limit access list 199
    1111.1111.1111
```

The following is sample output from the **show access-lists rate-limit** command when specific rate-limit access lists are specified:

```
Router# show access-lists rate-limit 1

Rate-limit access list 1
    0

Router# show access-lists rate-limit 9

Rate-limit access list 9
    mask FF

Router# show access-lists rate-limit 101

Rate-limit access list 101
    00E0.34B8.D840
```

Table 380 describes the fields shown in these displays.

Table 380 show access-lists rate-limit Field Descriptions

Field	Description
Rate-limit access list	Rate-limit access list number. A number from 1 to 99 represents a precedence-based access list. A number from 100 to 199 indicates a MAC address-based access list.
0	IP precedence for packets in this rate-limit access list.
mask FF	IP precedence mask for packets in this rate-limit access list.
1001.0110.1111	MAC address for packets in this rate-limit access list.

Related Commands

Command	Description
access-list rate-limit	Configures an access list for use with CAR policies.
show access-lists	Displays the contents of current IP and rate-limit access lists.

show interfaces fair-queue

To display information and all statistics about weighted fair queueing for a VIP-based interface, use the **show interfaces fair-queue** EXEC command.

show interfaces [*interface-type interface-number*] **fair-queue**

Syntax Description

interface-type	(Optional) The name of the interface.
interface-number	(Optional) The number of the interface.

Command Modes

EXEC

Command History

Release	Modification
11.1 CC	This command was introduced.

Examples

The following is sample output from the **show interfaces fair-queue** command:

```
Router# show interfaces fair-queue

Hssi0/0/0 queue size 0
        packets output 1417079, drops 2
 WFQ: aggregate queue limit 54, individual queue limit 27
    max available buffers 54

     Class 0: weight 10 limit 27 qsize 0 packets output 1150 drops 0
     Class 1: weight 20 limit 27 qsize 0 packets output 0 drops 0
     Class 2: weight 30 limit 27 qsize 0 packets output 775482 drops 1
     Class 3: weight 40 limit 27 qsize 0 packets output 0 drops 0
```

Table 381 describes the fields and statistics shown in this display.

Table 381 show interfaces fair-queue Field Descriptions

Field	Description
queue size	Current output queue size for this interface.
packets output	Number of packets transmitted out this interface, or, number of packets in this class transmitted out the interface.
drops	Number of packets dropped, or, number of packets in this class dropped.
aggregate queue limit	Aggregate limit, in number of packets.
individual queue limit	Individual limit, in number of packets.
max available buffers	Available buffer space allocated to aggregate queue limit, in number of packets.
Class	QoS group or ToS class.

Table 381 show interfaces fair-queue Field Descriptions (continued)

Field	Description
weight	Percent of bandwidth allocated to this class during periods of congestion.
limit	Queue limit for this class, in number of packets.
qsize	Current size of the queue for this class.

Related Commands

Command	Description
show interfaces	Displays statistics for all interfaces configured on the router or access server.

show interfaces random-detect

To display information about Weighted Random Early Detection (WRED) for a VIP-based interface, use the **show interfaces random-detect** EXEC command.

show interfaces [*interface-type interface-number*] **random-detect**

Syntax Description

interface-type	(Optional) The name of the interface.
interface-number	(Optional) The number of the interface.

Command Modes

EXEC

Command History

Release	Modification
11.1 CC	This command was introduced.

Examples

The following is sample output from the **show interfaces random-detect** command:

```
Router# show interfaces random-detect

 FastEthernet1/0/0 queue size 0
        packets output 29692, drops 0
 WRED: queue average 0
       weight 1/512
     Precedence 0: 109 min threshold, 218 max threshold, 1/10 mark weight
       1 packets output, drops: 0 random, 0 threshold
     Precedence 1: 122 min threshold, 218 max threshold, 1/10 mark weight
        (no traffic)
     Precedence 2: 135 min threshold, 218 max threshold, 1/10 mark weight
       14845 packets output, drops: 0 random, 0 threshold
     Precedence 3: 148 min threshold, 218 max threshold, 1/10 mark weight
        (no traffic)
     Precedence 4: 161 min threshold, 218 max threshold, 1/10 mark weight
        (no traffic)
     Precedence 5: 174 min threshold, 218 max threshold, 1/10 mark weight
        (no traffic)
     Precedence 6: 187 min threshold, 218 max threshold, 1/10 mark weight
       14846 packets output, drops: 0 random, 0 threshold
     Precedence 7: 200 min threshold, 218 max threshold, 1/10 mark weight
        (no traffic)
```

Table 382 describes the fields shown in this display.

Table 382 show interfaces random-detect Field Descriptions

Field	Description
queue size	Current output queue size for this interface.
packets output	Number of packets transmitted out this interface.
drops	Number of packets dropped.

Table 382 show interfaces random-detect Field Descriptions (continued)

Field	Description
queue average	Average queue length.
weight	Weighting factor used to determine the average queue size.
Precedence	WRED parameters for this precedence.
min threshold	Minimum threshold for this precedence.
max threshold	Maximum length of the queue. When the average queue is this long, any additional packets will be dropped.
mark weight	Probability of a packet being dropped if the average queue is at the maximum threshold.
packets output	Number of packets with this precedence that have been transmitted.
random	Number of packets dropped randomly through the WRED process.
threshold	Number of packets dropped automatically because the average queue was at the maximum threshold length.
(no traffic)	No packets with this precedence.

Related Commands

Command	Description
random-detect	Enables WRED or DWRED.
random-detect exponential-weighting-constant	Configures the WRED and DWRED exponential weight factor for the average queue size calculation.
random-detect precedence	Configures WRED and DWRED parameters for a particular IP precedence.
show interfaces	Displays statistics for all interfaces configured on the router or access server.

show interfaces rate-limit

To display information about committed access rate (CAR) for an interface, use the **show interfaces rate-limit** EXEC command.

show interfaces [*interface-type interface-number*] **rate-limit**

Syntax Description

interface-type	(Optional) The name of the interface.
interface-number	(Optional) The number of the interface.

Command Modes

EXEC

Command History

Release	Modification
11.1 CC	This command was introduced.

Examples

The following is sample output from the **show interfaces rate-limit** command:

```
Router# show interfaces fddi2/1/0 rate-limit

Fddi2/1/0
 Input
  matches: access-group rate-limit 100
   params: 800000000 bps, 64000 limit, 80000 extended limit
   conformed 0 packets, 0 bytes; action: set-prec-continue 1
   exceeded 0 packets, 0 bytes; action: set-prec-continue 0
   last packet: 4737508ms ago, current burst: 0 bytes
   last cleared 01:05:47 ago, conformed 0 bps, exceeded 0 bps
  matches: access-group 101
   params: 80000000 bps, 56000 limit, 72000 extended limit
   conformed 0 packets, 0 bytes; action: set-prec-transmit 5
   exceeded 0 packets, 0 bytes; action: set-prec-transmit 0
   last packet: 4738036ms ago, current burst: 0 bytes
   last cleared 01:02:05 ago, conformed 0 bps, exceeded 0 bps
  matches: all traffic
   params: 50000000 bps, 48000 limit, 64000 extended limit
   conformed 0 packets, 0 bytes; action: set-prec-transmit 5
   exceeded 0 packets, 0 bytes; action: set-prec-transmit 0
   last packet: 4738036ms ago, current burst: 0 bytes
   last cleared 01:00:22 ago, conformed 0 bps, exceeded 0 bps
 Output
  matches: all traffic
   params: 80000000 bps, 64000 limit, 80000 extended limit
   conformed 0 packets, 0 bytes; action: transmit
   exceeded 0 packets, 0 bytes; action: drop
   last packet: 4809528ms ago, current burst: 0 bytes
   last cleared 00:59:42 ago, conformed 0 bps, exceeded 0 bps
```

Table 383 describes the fields shown in this display.

Table 383 show interfaces rate-limit Field Descriptions

Field	Description
Input	These rate limits apply to packets received by the interface.
matches	Packets that match this rate limit.
params	Parameters for this rate limit, as configured by the **rate-limit** command.
bps	Average rate in bits per second.
limit	Normal burst size in bytes.
extended limit	Excess burst size in bytes.
conformed	Number of packets that have conformed to the rate limit.
action	Conform action.
exceeded	Number of packets that have exceeded the rate limit.
action	Exceed action.
last packet	Time since the last packet in milliseconds.
current burst	Instantaneous burst size at the current time.
last cleared	Time since the burst counter was set back to zero by the **clear counters** command.
conformed	Rate of conforming traffic.
exceeded	Rate of exceeding traffic.
Output	These rate limits apply to packets sent by the interface.

Related Commands

Command	Description
access-list rate-limit	Configures an access list for use with CAR policies.
clear counters	Clears the interface counters.
show access-lists	Displays the contents of current IP and rate-limit access lists.
show access-lists rate-limit	Displays information about rate-limit access lists.
show interfaces	Displays statistics for all interfaces configured on the router or access server.

show ip rsvp installed

To display RSVP-related installed filters and corresponding bandwidth information, use the **show ip rsvp installed** EXEC command.

show ip rsvp installed [*interface-type interface-number*]

Syntax Description

interface-type	(Optional) The name of the interface.
interface-number	(Optional) The number of the interface.

Command Modes

EXEC

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

The command displays the current installed RSVP filters and the corresponding bandwidth information for a specified interface or all interfaces.

Examples

The following is sample output from the **show ip rsvp installed** command:

```
Router# show ip rsvp installed

RSVP:
RSVP: Ethernet1: has no installed reservations
RSVP: Serial0:
     kbps   To              From       Protocol DPort Sport Weight Conversation
     0      224.250.250.1   132.240.2.28     UDP 20    30    128   270
     150    224.250.250.1   132.240.2.1      UDP 20    30    128   268
     100    224.250.250.1   132.240.1.1      UDP 20    30    128   267
     200    224.250.250.1   132.240.1.25     UDP 20    30    256   265
     200    224.250.250.2   132.240.1.25     UDP 20    30    128   271
     0      224.250.250.2   132.240.2.28     UDP 20    30    128   269
     150    224.250.250.2   132.240.2.1      UDP 20    30    128   266
     350    224.250.250.3   0.0.0.0          UDP 20    0     128   26
```

Table 384 describes significant fields shown in this display.

Table 384 show ip rsvp installed Field Descriptions

Field	Description
kbps	Reserved rate.
To	IP address of the source device.
From	IP address of the destination device.
Protocol DPort	Protocol type of the destination UDP/TCP port (no longer the usual protocol).

Table 384 show ip rsvp installed Field Descriptions (continued)

Field	Description
Sport	Source UDP/TCP port.
Weight	Weight used in weighted fair queueing (WFQ).
Conversation	WFQ conversation number. If the WFQ is not configured on the interface, weight and conversation will be zero.

show ip rsvp interface

To display RSVP-related interface information, use the **show ip rsvp interface** EXEC command.

show ip rsvp interface [*interface-type interface-number*]

Syntax Description

interface-type	(Optional) The name of the interface.
interface-number	(Optional) The number of the interface.

Command Modes

EXEC

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

Use this command to show the current allocation budget and maximum allocatable bandwidth.

Examples

The following is sample output from the **show ip rsvp interface** command:

```
Router# show ip rsvp interface

interfac allocate i/f max  flow max per/255 UDP  IP   UDP_IP   UDP M/C
Et1      0M       7500K    7500K    0  /255 0    0    0        0
Se0      0M       1158K    1158K    0  /255 0    0    0        0
Se1      30K      1158K    1158K    6  /255 0    1    0        0
```

Table 385 describes significant fields shown in this display.

Table 385 show ip rsvp interface Field Descriptions

Field	Description
interface	Interface name.
allocate	Current allocation budget.
i/f max	Maximum allocatable bandwidth.
flow max	Maximum flow possible on this interface.
per /255	Percent of bandwidth utilized.
UDP	Number of neighbors sending UDP-encapsulated RSVP.
IP	Number of neighbors sending IP-encapsulated RSVP.
UDP_IP	Number of neighbors sending both UDP- and IP-encapsulated RSVP.
UDP M/C	Is router configured for UDP on this interface?

show ip rsvp neighbor

To display current RSVP neighbors, use the **show ip rsvp neighbor** EXEC command.

show ip rsvp neighbor [*interface-type interface-number*]

Syntax Description

interface-type	(Optional) The name of the interface.
interface-number	(Optional) The number of the interface.

Command Modes

EXEC

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

Use this command to show the current RSVP neighbors and identify if the neighbor is using IP, UDP, or RSVP encapsulation for a specified interface or all interfaces.

Examples

The following is sample output from the **show ip rsvp neighbor** command:

```
Router# show ip rsvp neighbor

Interface Neighbor        Encapsulation
Se1       132.240.1.49    RSVP
```

Table 386 describes significant fields shown in this display.

Table 386 show ip rsvp neighbor Field Descriptions

Field	Description
Interface	Interface name.
Neighbor	IP address of the RSVP neighbor.
Encapsulation	The type of encapsulation the neighbor is using: IP, UDP, or RSVP.

show ip rsvp request

To display RSVP-related request information being requested upstream, use the **show ip rsvp request** EXEC command.

show ip rsvp request [*interface-type interface-number*]

Syntax Description

interface-type	(Optional) The name of the interface.
interface-number	(Optional) The number of the interface.

Command Modes

EXEC

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

Use this command to show the RSVP reservations currently being requested upstream for a specified interface or all interfaces. The received reservations may differ from requests because of aggregated or refused reservations.

Examples

The following is sample output from the **show ip rsvp request** command:

```
Router# show ip rsvp request

To            From          Pro DPort Sport Next Hop      I/F   Fi Serv
132.240.1.49  132.240.4.53  1   0     0     132.240.3.53  Et1   FF LOAD
```

Table 387 describes significant fields shown in this display.

Table 387 show ip rsvp request Field Descriptions

Field	Description
To	IP address of the receiver.
From	IP address of the sender.
Pro	Protocol code. Code 1 indicates ICMP.
DPort	Destination port number.
Sport	Source port number.
Next Hop	IP address of the next hop.
I/F	Interface of the next hop.
Fi	Filter (Wild Card Filter, Shared Explicit Filter, or Fixed Filter).
Serv	Service (value can be **rate** or **load**).

show ip rsvp reservation

To display RSVP-related receiver information currently in the database, use the **show ip rsvp reservation** EXEC command.

show ip rsvp reservation [*interface-type interface-number*]

Syntax Description

interface-type	(Optional) The name of the interface.
interface-number	(Optional) The number of the interface.

Command Modes

EXEC

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

Use this command to show the current receiver (RESV) information currently in the database for a specified interface or all interfaces. This information includes reservations aggregated and forwarded from other RSVP routers.

Examples

The following is sample output from the **show ip rsvp reservation** command:

```
Router# show ip rsvp reservation

To            From          Pro DPort Sport Next Hop      I/F   Fi Serv
132.240.1.49  132.240.4.53  1   0     0     132.240.1.49  Se1   FF LOAD
```

Table 388 describes significant fields shown in this display.

Table 388 show ip rsvp reservation Field Descriptions

Field	Descriptions
To	IP address of the receiver.
From	IP address of the sender.
Pro	Protocol code. Code 1 indicates ICMP.
DPort	Destination port number.
Sport	Source port number.
Next Hop	IP address of the next hop.
I/F	Interface of the next hop.
Fi	Filter (Wild Card Filter, Shared Explicit Filter, or Fixed Filter).
Serv	Service (value can be **rate** or **load**).

show ip rsvp sender

To display RSVP PATH-related sender information currently in the database, use the **show ip rsvp sender** EXEC command.

show ip rsvp sender [*interface-type interface-number*]

Syntax Description

interface-type	(Optional) The name of the interface.
interface-number	(Optional) The number of the interface.

Command Modes

EXEC

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

Use this command to show the RSVP sender (PATH) information currently in the database for a specified interface or all interfaces.

Examples

The following is sample output from the **show ip rsvp sender** command:

```
Router# show ip rsvp sender

To              From            Pro DPort Sport Prev Hop        I/F
132.240.1.49    132.240.4.53    1   0     0     132.240.3.53    Et1
132.240.2.51    132.240.5.54    1   0     0     132.240.3.54    Et1
```

Table 389 describes the fields shown in this display.

Table 389 show ip rsvp sender Field Descriptions

Field	Description
To	IP address of the receiver.
From	IP address of the sender.
Pro	Protocol code. Code 1 indicates ICMP.
DPort	Destination port number.
Sport	Source port number.
Prev Hop	IP address of the previous hop.
I/F	Interface of the previous hop.

show queue

To list fair queueing configuration and statistics for a particular interface, use the **show queue** privileged EXEC command.

show queue *interface-type interface-number*

Syntax Description

interface-type	The name of the interface.
interface-number	The number of the interface.

Command Modes

Privileged EXEC

Usage Guidelines

This command displays statistics for interfaces configured with the fair queueing strategy.

Examples

The following is sample output from the **show queue** command. There are two active conversations on the serial 1 interface. Weighted fair queueing ensures that both of these IP data streams, one TCP and other UDP, receive equal bandwidth on the interface while they have messages in the pipeline.

```
Router# show queue serial1

  Input queue: 0/75/0 (size/max/drops); Total output drops: 303628
  Queueing strategy: weighted fair
  Output queue: 64/1000/64/303628 (size/max total/threshold/drops)
     Conversations  2/2/256 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)

  (depth/weight/discards/tail drops/interleaves) 45/4096/1123/0/0
  Conversation 244, linktype: ip, length: 50
  source: 55.1.1.1, destination: 66.1.1.2, id: 0x0000, ttl: 59,
  TOS: 0 prot: 6, source port 55, destination port 55

  (depth/weight/discards/tail drops/interleaves) 19/4096/302541/0/0
  Conversation 185, linktype: ip, length: 118
  source: 55.1.1.1, destination: 66.1.1.2, id: 0x0000, ttl: 59,
  TOS: 0 prot: 17, source port 20, destination port 20
```

Table 390 describes the fields shown in this display.

Table 390 show queue Field Descriptions

Field	Description
Input Queue	Input queue size in packets.
Total output drops	Total output packet drops.
Queueing strategy	Type of queueing active on this interface.
Output queue	Output queue size in packets.
Conversations	WFQ conversation number.

Table 390 show queue Field Descriptions (continued)

Field	Description
Reserved Conversations	Total number of reserved WFQ conversations. Default is 256.
depth	Queue depth for the conversation in packets.
weight	Weight used in WFQ.
discards	Number of packet discards for the conversation.
tail drops	Number of tail drop packets for the conversation.
interleaves	Number of packets interleaved.
linktype	Protocol name.
length	Packet length.
source	Source IP address.
destination	Destination IP address.
id	Packet ID.
ttl	Time to live count.
TOS	IP type of service.
prot	Layer 4 protocol number.

show queueing

To list all or selected configured queueing strategies, use the **show queueing** privileged EXEC command.

show queueing [**custom** | **fair** | **priority** | **red**]

Syntax Description

custom	(Optional) Status of the custom queueing list configuration.
fair	(Optional) Status of the fair queueing configuration.
priority	(Optional) Status of the priority queueing list configuration.
red	(Optional) Status of the Weighted Random Early Detection (WRED) configuration.

Defaults

If no keyword is entered, this command shows the configuration of all interfaces.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.3	This command was introduced.

Examples

The following is sample output from the **show queueing custom** command:

```
Router# show queueing custom
Current custom queue configuration:

       List   Queue  Args
       3      10     default
       3      3      interface Tunnel3
       3      3      protocol ip
       3      3      byte-count 444 limit 3
```

The following is sample output from the **show queueing** command. There are two active conversations in the serial interface 0. Weighted fair queueing ensures that both of these IP data streams—both using TCP—receive equal bandwidth on the interface while they have messages in the pipeline, even though there is more FTP data in the queue than RCP data.

```
Router# show queueing

Current fair queue configuration:

Interface           Discard     Dynamic      Reserved
                    threshold   queue count  queue count
Serial0             64          256          0
Serial1             64          256          0
Serial2             64          256          0
Serial3             64          256          0

Current priority queue configuration:

List   Queue  Args
1      high   protocol cdp
2      medium interface Ethernet1

Current custom queue configuration:

Current RED queue configuration:

Interface: Ethernet3   Exp-weight-constant: 9
  Class    Min-th    Max-th   Mark-prob
  0        20        40       1/10
  1        22        40       1/10
  2        24        40       1/10
  3        26        40       1/10
  4        28        40       1/10
  5        31        40       1/10
  6        33        40       1/10
  7        35        40       1/10
  rsvp     37        40       1/10
```

Related Commands

Command	Description
custom-queue-list	Assigns a custom queue list to an interface.
fair-queue	Enables WFQ for an interface.
priority-group	Assigns the specified priority list to an interface.
priority-list interface	Establishes queueing priorities on packets entering from a given interface.
priority-list queue-limit	Specifies the maximum number of packets that can be waiting in each of the priority queues.
queue-list interface	Establishes queueing priorities on packets entering on an interface.
queue-list queue byte-count	Specifies how many bytes the system allows to be delivered from a given queue during a particular cycle.
random-detect	Enables WRED or DWRED.

show tech-support rsvp

To generate a report of all RSVP-related information, use the **show tech-support rsvp** command.

show tech-support rsvp

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Usage Guidelines

This command is not required for normal use of the operating system. This command is useful when contacting technical support personnel with questions regarding RSVP. The **show tech-support rsvp** command generates a series of reports that can be useful to technical support personnel attempting to solve problems.

Any issues or caveats that apply to the **show tech-support** command also apply to this command. For example, the enable password, if configured, is not displayed in the output of the **show running-config** command.

The **show tech-support rsvp** command is equivalent to issuing the following commands:

show ip rsvp installed
show ip rsvp interface
show ip rsvp neighbor
show ip rsvp request
show ip rsvp reservation
show ip rsvp sender
show running-config
show version

Refer to the displays and descriptions for these commands for information about the **show tech-support rsvp** command display.

show traffic-shape

To display the current traffic-shaping configuration, use the **show traffic-shape** EXEC command.

show traffic-shape [*interface-type*]

Syntax Description

interface-type	(Optional) The name of the interface. If no interface is specified, traffic shaping details for all configured interfaces are shown.

Command Modes

EXEC

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

You must have first enabled traffic shaping using the **traffic-shape rate**, **traffic-shape group**, or **frame-relay traffic-shaping** command to display traffic-shaping information.

Examples

The following is sample output from the **show traffic-shape** command:

```
Router# show traffic-shape

          access Target    Byte   Sustain   Excess    Interval  Increment Adapt
I/F       list   Rate      Limit  bits/int  bits/int  (ms)       (bytes)  Active
Et0       101     1000000  23437  125000    125000    63        7813      -
Et1               5000000  87889  625000    625000    16        9766      -
```

Table 391 describes the fields shown in this display.

Table 391 show traffic-shape Field Descriptions

Field	Description
I/F	Interface.
access list	Number of the access list.
Target Rate	Rate that traffic is shaped to in bps.
Byte Limit	Maximum number of bytes transmitted per internal interval.
Sustain bits/int	Configured sustained bits per interval.
Excess bits/int	Configured excess bits in the first interval.
Interval (ms)	Interval being used internally, which may be smaller than the committed burst divided by the committed information rate, if the router determines that traffic flow will be more stable with a smaller configured interval.
Increment (bytes)	Number of bytes that will be sustained per internal interval.
Adapt Active	Contains “BECN” if Frame Relay has backward explicit congestion notification (BECN) adaptation configured.

Related Commands

Command	Description
frame-relay traffic-shaping	Enables both traffic shaping and per-VC queueing for all PVCs and SVCs on a Frame Relay interface.
show traffic-shape statistics	Displays the current traffic-shaping statistics.
traffic-shape adaptive	Configures a Frame Relay subinterface to estimate the available bandwidth when BECNs are received.
traffic-shape fecn-adapt	Replies to messages with the FECN bit, (which are set with TEST RESPONSE messages with the BECN bit set).
traffic-shape group	Enables traffic shaping based on a specific access list for outbound traffic on an interface.
traffic-shape rate	Enables traffic shaping for outbound traffic on an interface.

show traffic-shape statistics

To display the current traffic-shaping statistics, use the **show traffic-shape statistics** EXEC command.

show traffic-shape statistics [*interface-type*]

Syntax Description

interface-type	(Optional) The name of the interface. If no interface is specified, traffic shaping statistics for all configured interfaces are shown.

Command Modes

EXEC

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

You must have first enabled traffic shaping using the **traffic-shape rate**, **traffic-shape group**, or **frame-relay traffic-shaping** command to display traffic-shaping information.

Examples

The following is sample output from the **show traffic-shape statistics** command:

```
Router# show traffic-shape statistics

          Access Queue     Packets   Bytes     Packets   Bytes     Shaping
I/F       List   Depth                        Delayed   Delayed   Active
Et0       101    0         2         180       0         0         no
Et1              0         0         0         0         0         no
```

Table 392 describes the fields shown in this display.

Table 392 show traffic-shape statistics Field Descriptions

Field	Description
I/F	Interface.
Access List	Number of the access list.
Queue Depth	Number of messages in the queue.
Packets	Number of packets sent through the interface.
Bytes	Number of bytes sent through the interface.
Packets Delayed	Number of packets sent through the interface that were delayed in the traffic shaping queue.
Bytes Delayed	Number of bytes sent through the interface that were delayed in the traffic shaping queue.
Shaping Active	Contains “yes” when timers indicate that traffic shaping is occurring and “no” if traffic shaping is not occurring.

Related Commands

Command	Description
frame-relay traffic-shaping	Enables both traffic shaping and per-VC queueing for all PVCs and SVCs on a Frame Relay interface.
show interfaces	Displays statistics for all interfaces configured on the router or access server.
show ip rsvp interface	Displays RSVP-related interface information.
traffic-shape adaptive	Configures a Frame Relay subinterface to estimate the available bandwidth when BECNs are received.
traffic-shape group	Enables traffic shaping based on a specific access list for outbound traffic on an interface.
traffic-shape rate	Enables traffic shaping for outbound traffic on an interface.

traffic-shape adaptive

To configure a Frame Relay subinterface to estimate the available bandwidth when backward explicit congestion notifications (BECNs) are received, use the **traffic-shape adaptive** interface configuration command. To stop adapting to congestion signals, use the **no** form of this command.

traffic-shape adaptive *bit-rate*

no traffic-shape adaptive

Syntax Description

bit-rate	Lowest bit rate that traffic is shaped to, in bits per second. The default *bit rate* value is 0.

Command Modes

Interface configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

This command specifies the boundaries in which traffic will be shaped when BECNs are received. You must enable traffic shaping on the interface with the **traffic-shape rate** or **traffic-shape group** command before you can use the **traffic-shape adaptive** command.

The bit rate specified for the **traffic-shape rate** command is the upper limit, and the bit rate specified for the **traffic-shape adaptive** command is the lower limit to which traffic is shaped when BECNs are received on the interface. The rate actually shaped to will be between these two bit rates.

You should configure this command and the **traffic-shape fecn-adapt** command on both ends of the connection to ensure adaptive traffic shaping over the connection, even when traffic is flowing primarily in one direction. The **traffic-shape fecn-adapt** command configures the router to reflect forward explicit congestion notification (FECN) signals as BECNs.

Examples

The following example configures traffic shaping on serial interface 0.1 with an upper limit of 128 kbps and a lower limit of 64 kbps. This configuration allows the link to run from 64 to 128 kbps, depending on the congestion level.

```
router(config)# interface serial 0
router(config-if)# encapsulation-frame-relay
router(config)# interface serial 0.1
router(config-if)# traffic-shape rate 128000
router(config-if)# traffic-shape adaptive 64000
router(config-if)# traffic-shape fecn-adapt
```

Related Commands

Command	Description
show traffic-shape	Displays the current traffic-shaping configuration.
show traffic-shape statistics	Displays the current traffic-shaping statistics.

Command	Description
traffic-shape fecn-adapt	Replies to messages with the FECN bit, (which are set with TEST RESPONSE messages with the BECN bit set).
traffic-shape group	Enables traffic shaping based on a specific access list for outbound traffic on an interface.
traffic-shape rate	Enables traffic shaping for outbound traffic on an interface.

traffic-shape fecn-adapt

To reply to messages with the forward explicit congestion notification (FECN) bit, (which are set with TEST RESPONSE messages with the BECN bit set), use the **traffic-shape fecn-adapt** interface configuration command. To stop backward explicit congestion notification (BECN) message generation, use the **no** form of this command.

traffic-shape fecn-adapt

no traffic-shape fecn-adapt

Syntax Description

This command has no arguments or keywords.

Defaults

Traffic shaping is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

Enable traffic shaping on the interface with the **traffic-shape rate** or **traffic-shape group** command. FECN is available only when traffic shaping is configured.

Use this command to reflect FECN bits as BECN bits to notify the other data terminal equipment (DTE) that it is transmitting too fast. Use the **traffic-shape adaptive** command to configure the router to adapt its transmission rate when it receives BECNs.

You should configure this command and the **traffic-shape adaptive** command on both ends of the connection to ensure adaptive traffic shaping over the connection, even when traffic is flowing primarily in one direction.

Examples

The following example configures traffic shaping on serial interface 0.1 with an upper limit of 128 kbps and a lower limit of 64 kbps. This configuration allows the link to run from 64 to 128 kbps, depending on the congestion level. The router reflects FECNs as BECNs.

```
router(config)# interface serial 0
router(config-if)# encapsulation-frame-relay
router(config)# interface serial 0.1
router(config-if)# traffic-shape rate 128000
router(config-if)# traffic-shape adaptive 64000
router(config-if)# traffic-shape fecn-adapt
```

Related Commands

Command	Description
show traffic-shape	Displays the current traffic-shaping configuration.
show traffic-shape statistics	Displays the current traffic-shaping statistics.
traffic-shape adaptive	Configures a Frame Relay subinterface to estimate the available bandwidth when BECNs are received.
traffic-shape group	Enables traffic shaping based on a specific access list for outbound traffic on an interface.
traffic-shape rate	Enables traffic shaping for outbound traffic on an interface.

traffic-shape group

To enable traffic shaping based on a specific access list for outbound traffic on an interface, use the **traffic-shape group** interface configuration command. To disable traffic shaping on the interface for the access list, use the **no** form of this command.

traffic-shape group *access-list bit-rate* [*burst-size* [*excess-burst-size*]]

no traffic-shape group *access-list*

Syntax Description

access-list	Number of the access list that controls the packets that traffic shaping is applied to on the interface.
bit-rate	Bit rate that traffic is shaped to in bits per second. This is the access bit rate that you contract with your service provider, or the service levels you intend to maintain.
burst-size	(Optional) Sustained number of bits that can be transmitted per interval. On Frame Relay interfaces, this is the committed burst size contracted with your service provider.
excess-burst-size	(Optional) Maximum number of bits that can exceed the burst size in the first interval in a congestion event. On Frame Relay interfaces, this is the excess burst-size contracted with your service provider. The default is equal to the *burst-size* argument.

Defaults

This command is not on by default.

Command Modes

Interface configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

Traffic shaping is not supported with optimum, distributed, or flow switching. If you enable this command, all interfaces will revert to fast switching.

Traffic shaping uses queues to limit surges that can congest a network. Data is buffered and then sent into the network in regulated amounts to ensure that traffic will fit within the promised traffic envelope for the particular connection.

The **traffic-shape group** command allows you to specify one or more previously defined access list to shape traffic to on the interface. You must specify one **traffic-shape group** command for each access list on the interface.

The **traffic-shape group** command supports both standard and extended access lists.

Use traffic shaping if you have a network with differing access rates or if you are offering a subrate service. You can configure the values according to your contract with your service provider or the service levels you intend to maintain.

An interval is calculated as follows:

- If the *burst-size* is not equal to zero, the interval is the *burst-size* divided by the *bit-rate*.
- If the *burst-size* is zero, the interval is the *excess-burst-size* divided by the *bit-rate*.

Traffic shaping is supported on all media and encapsulation types on the router. To perform traffic shaping on Frame Relay virtual circuits, you can also use the **frame-relay traffic-shaping** command. For more information on Frame Relay traffic shaping, refer to the "Configuring Frame Relay" chapter in the *Wide-Area Network Configuration Guide*.

If traffic shaping is performed on a Frame Relay network with the **traffic-shape rate** command, you can also use the **traffic-shape adaptive** command to specify the minimum bit rate the traffic is shaped to.

Examples

The following example enables traffic that matches access list 101 to be shaped to a certain rate and traffic matching access list 102 to be shaped to another rate on the interface:

```
router(config)# interface serial 1
router(config-if)# traffic-shape group 101 128000 16000 8000
router(config-if)# traffic-shape group 102 130000 10000 1000
```

Related Commands

Command	Description
access-list (IP Standard)	Defines a standard IP access list.
show traffic-shape	Displays the current traffic-shaping configuration.
show traffic-shape statistics	Displays the current traffic-shaping statistics.
traffic-shape adaptive	Configures a Frame Relay subinterface to estimate the available bandwidth when BECNs are received.
traffic-shape fecn-adapt	Replies to messages with the FECN bit, (which are set with TEST RESPONSE messages with the BECN bit set).
traffic-shape rate	Enables traffic shaping for outbound traffic on an interface.

traffic-shape rate

To enable traffic shaping for outbound traffic on an interface, use the **traffic-shape rate** interface configuration command. To disable traffic shaping on the interface, use the **no** form of this command.

traffic-shape rate *bit-rate* [*burst-size* [*excess-burst-size*]]

no traffic-shape rate

Syntax Description

bit-rate	Bit rate that traffic is shaped to in bits per second. This is the access bit rate that you contract with your service provider, or the service levels you intend to maintain.
burst-size	(Optional) Sustained number of bits that can be transmitted per interval. On Frame Relay interfaces, this is the committed burst size contracted with your service provider.
excess-burst-size	(Optional) Maximum number of bits that can exceed the burst size in the first interval in a congestion event. On Frame Relay interfaces, this is the excess burst-size contracted with your service provider. The default is equal to the *burst-size* argument.

Defaults

Traffic shaping is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

Traffic shaping is not supported with optimum, distributed, or flow switching. If you enable this command, all interfaces will revert to fast switching.

Traffic shaping uses queues to limit surges that can congest a network. Data is buffered and then sent into the network in regulated amounts to ensure that traffic will fit within the promised traffic envelope for the particular connection.

Use traffic shaping if you have a network with differing access rates or if you are offering a subrate service. You can configure the values according to your contract with your service provider or the service levels you intend to maintain.

An interval is calculated as follows:

- If the *burst-size* is not equal to zero, the interval is the *burst-size* divided by the *bit-rate*.
- If the *burst-size* is zero, the interval is the *excess-burst-size* divided by the *bit-rate*.

Traffic shaping is supported on all media and encapsulation types on the router. To perform traffic shaping on Frame Relay virtual circuits, you can also use the **frame-relay traffic-shaping** command. For more information on Frame Relay traffic shaping, refer to the "Configuring Frame Relay" chapter in the *Wide-Area Network Configuration Guide*.

If traffic shaping is performed on a Frame Relay network with the **traffic-shape rate** command, you can also use the **traffic-shape adaptive** command to specify the minimum bit rate to which the traffic is shaped.

Examples

The following example enables traffic shaping on serial interface 0 using the bandwidth required by the service provider:

```
router(config)# interface serial 0
router(config-if)# traffic-shape rate 128000 16000 8000
```

Related Commands

Command	Description
show traffic-shape	Displays the current traffic-shaping configuration.
show traffic-shape statistics	Displays the current traffic-shaping statistics.
traffic-shape adaptive	Configures a Frame Relay subinterface to estimate the available bandwidth when BECNs are received.
traffic-shape fecn-adapt	Replies to messages with the FECN bit, (which are set with TEST RESPONSE messages with the BECN bit set).
traffic-shape group	Enables traffic shaping based on a specific access list for outbound traffic on an interface.