Committed Access Rate

Feature Summary

The Committed Access Rate (CAR) feature performs the following functions:

- Limits the input or output transmission rate on an interface or subinterface based on a flexible set of criteria.
- Classifies packets by setting the IP precedence or QoS group. A QoS group is a QoS class identifier internal to the router.

Note QoS group classification is only available for Cisco IOS Release 11.1(20)CC and later 11.1 CC releases.

CAR can be used to rate-limit traffic based on certain matching criteria, such as incoming interface, IP precedence, QoS group, or IP access list criteria. CAR provides configurable actions, such as transmit, drop, set precedence, or set QoS group, when traffic conforms to or exceeds the rate limit.

Benefits

CAR performs two quality of service (QoS) functions:

- Bandwidth management through rate limiting. This function allows you to control the maximum rate for traffic transmitted or received on an interface. CAR is often configured on interfaces at the edge of a network to limit traffic into or out of the network. Traffic that falls within the rate parameters is transmitted, while packets that exceed the acceptable amount of traffic are dropped or transmitted with a different priority.
- Packet classification through IP precedence and QoS group setting. This function allows you to partition your network into multiple priority levels or classes of service (CoS).
  - Use CAR to set the IP precedence for packets entering the network. Networking devices within your network can then use the adjusted IP precedence to determine how the traffic is treated. For example, DWRED uses the IP precedences to determine the probability a packet will be dropped.
  - Use CAR to assign packets to a QoS group. The router uses the QoS group to determine how it treats packets.

List of Terms

average rate—Maximum long-term average rate of conforming traffic.

Committed Access Rate (CAR)—QoS feature that performs rate limiting and packet classification.

conform action—Action to take on packets below the rate allowed by the rate limit.

Distributed CAR (DCAR)—An implementation of CAR. DCAR performs all of the functions of CAR, but all of the processing takes place on the VIP.

exceed action—Action to take on packets above the rate allowed by the rate limit.

excess burst size—Bytes allowed in a burst before all packets will exceed the rate limit.

normal burst size—Bytes allowed in a burst before some packets will exceed the rate limit. Larger bursts are more likely to exceed the rate limit.

QoS group—Internal QoS group ID for a packet used to determine rate-limiting or weighted fair queuing characteristics for that packet.

rate limit—Traffic descriptor defined by the average rate, normal burst size, and excess burst size.

rate policy—The rate limit, conform actions, and exceed actions that apply to traffic matching a certain criteria.

Versatile Interface Processor (VIP)—Interface card used by Cisco 7500 series and Cisco 7000 series with RSP7000 routers.

Restrictions

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

CAR or DCAR can be configured on an interface or subinterface. However, CAR and DCAR are not supported on the following:

- Fast EtherChannel interfaces
- Tunnel interfaces
- PRI interfaces
- Any interface that does not support CEF

DCAR is not supported on ATM subinterfaces.

DCAR is not supported with the ATM encapsulations AAL5-MUX and AAL5-NLPID.

Platforms

CAR is supported on these platforms:

- Cisco 7000 series with RSP7000
- Cisco 7200 series
- Cisco 7500 series

DCAR is only supported on Cisco 7000 series with RSP7000 or Cisco 7500 series routers with a VIP2-40 or better. A VIP2-50 card is strongly recommended when the aggregate line rate of the port adapters on the VIP is greater than DS-3. A VIP2-50 card is required for OC-3 rates.

Prerequisites

Distributed CEF switching must be enabled on any interface that uses DCAR, even when only output CAR is configured. In order to use CAR, CEF must be enabled on the interface.

Refer to the Cisco Express Forwarding feature documentation for configuration information.

Supported MIBs and RFCs

This feature supports the CISCO-CAR-MIB.

For descriptions of supported MIBs and how to use MIBs, see Cisco's MIB website on CCO at http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml.

No RFCs are supported by this feature.

Functional Description

This section describes the following aspects of the Committed Access Rate (CAR) feature:

- Matching Criteria
- Rate Limits
- Conform and Exceed Actions
- Multiple Rate Policies

Matching Criteria

Rate policies can be associated with one of the following:

- All IP traffic
- IP precedence (defined by a rate-limit access list)
- QoS group
- MAC address (defined by a rate-limit access list)
- IP access list (standard and extended)

Matching to IP access lists is more processor-intensive than matching based on other criteria.

Rate Limits

Rate limits define which packets conform or exceed based on the three parameters: average rate, normal burst size, and excess burst size:

- The average rate determines the long-term average transmission rate. Traffic that falls under this rate will always conform.
- The normal burst size determines how large traffic bursts can be before some traffic exceeds the rate limit.
- The excess burst size determines how large traffic bursts can be before all traffic exceeds the rate limit.

- Traffic that falls between the normal burst size and the excess burst size exceeds the rate limit with a probability that increases as the burst size increases.

CAR propagates bursts. It does no smoothing or shaping of traffic.

Conform and Exceed Actions

Once the packet has been classified as conforming or exceeding a particular rate limit, the router performs one of the following actions on the packet:

- Transmit—The packet is transmitted.
- Drop—The packet is dropped.
- Set precedence and transmit—The IP precedence bits in the packet header are rewritten. The packet is then transmitted.
- Set QoS group and transmit—The packet is assigned to a QoS group and transmitted.
- Continue—The packet is evaluated using the next rate policy. If there is not another rate policy, the packet is transmitted.
- Set precedence and continue—The IP precedence bits in the packet header are rewritten. The packet is evaluated using the next rate policy. If there is not another rate policy, the packet is transmitted.
- Set QoS group and continue—The packet is assigned to a QoS group. The packet is evaluated using the next rate policy. If there is not another rate policy, the packet is transmitted.

Multiple Rate Policies

One rate policy includes information about the rate limit, conform actions, and exceed actions.

Each interface can have multiple CAR policies, corresponding to different types of traffic. For example, low priority traffic may be limited to a lower rate than high priority traffic. Additionally, you can classify and set IP precedences or QoS groups based on different criteria for use by other QoS features (such as WRED or WFQ).

With multiple rate policies, the router examines each policy in the order entered until the packet matches. If a match is not found, the default action is to transmit.

The rate policies can be independent; each rate policy deals with a different type of traffic. Alternatively, rate policies can be cascading; a packet may be compared to multiple different rate policies in succession.

You can configure up to 20 rate policies on a subinterface.

Configuration Tasks

To configure CAR or DCAR, perform the following tasks beginning in global configuration mode:

Task	Command
(Optional) Specify a rate-limit access list. Repeat this command if you wish to specify a new access list.	**access-list rate-limit** *acl-index* {*precedence* | *mac-address* | **mask** *prec-mask*}

Task	Command
(Optional) Specify a standard or extended access list. Repeat this command to further configure the access list or specify a new access list.	**access-list** *acl-index* {**deny** | **permit**} *source* [*source-wildcard*] **access-list** *acl-index* {**deny** | **permit**} *protocol source source-wildcard destination destination-wildcard* [**precedence** *precedence*] [**tos** *tos*] [**log**]
Specify the interface or subinterface. This task puts the router in interface configuration mode.	**interface** *type number*
Specify the rate policy for each particular class of traffic. Repeat this command for each different class of traffic.	**rate-limit** {**input** | **output**} [**access-group** [**rate-limit**] *acl-index* | **qos-group** *number*] *bps burst-normal burst-max* **conform-action** *action* **exceed-action** *action*
Exit configuration mode.	**end**
Verify the configuration.	**show interfaces rate-limit**

Refer to the “Configuration Examples” section for example configurations.

Configuration Examples

The following sections provide examples of ways you might use CAR to control traffic into and out of your network:

- Input and Output Rate-Limiting on an Interface Example
- Rate-Limiting and Precedence-Setting Example
- Internet Exchange Point Example

Input and Output Rate-Limiting on an Interface Example

In this example, a customer is connected to an ISP by a T3 link. The ISP wants to rate-limit the customer’s transmissions to 20 Mbps of the 45 Mbps. In addition, the customer is allowed to transmit bursts of 24000 bytes. All exceeding packets dropped. The following commands are configured on the ISP’s HSSI interface connected to the customer:

```
interface Hssi0/0/0
 description 45Mbps to R1
 rate-limit input 20000000 24000 24000 conform-action transmit exceed-action drop
 ip address 200.200.14.250 255.255.255.252
 rate-limit output 20000000 24000 24000 conform-action transmit exceed-action drop
```

To verify the configuration and monitor CAR statistics, use the **show interfaces rate-limit** command:

```
Router# show interfaces hssi 0/0/0 rate-limit

Hssi0/0/0 45Mbps to R1
 Input
  matches: all traffic
   params: 20000000 bps, 24000 limit, 24000 extended limit
   conformed 8 packets, 428 bytes; action: transmit
   exceeded 0 packets, 0 bytes; action: drop
   last packet: 8680ms ago, current burst: 0 bytes
   last cleared 00:03:59 ago, conformed 0 bps, exceeded 0 bps
 Output
  matches: all traffic
   params: 20000000 bps, 24000 limit, 24000 extended limit
   conformed 0 packets, 0 bytes; action: transmit
   exceeded 0 packets, 0 bytes; action: drop
   last packet: 8680ms ago, current burst: 0 bytes
   last cleared 00:03:59 ago, conformed 0 bps, exceeded 0 bps
```

Rate-Limiting and Precedence-Setting Example

The following example limits the rate by application.

- All Web traffic is transmitted. However, the IP precedence for Web traffic that conforms to the first rate policy is set to 5. For non-conforming Web 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.

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

To verify the configuration and monitor CAR statistics, use the **show interfaces rate-limit** command:

```
Router# show interfaces hssi 0/0/0 rate-limit

Hssi0/0/0 45Mbps to R2
 Input
  matches: access-group 101
   params: 20000000 bps, 24000 limit, 32000 extended limit
   conformed 3 packets, 189 bytes; action: set-prec-transmit 5
   exceeded 0 packets, 0 bytes; action: set-prec-transmit 0
   last packet: 309100ms ago, current burst: 0 bytes
   last cleared 00:08:00 ago, conformed 0 bps, exceeded 0 bps
  matches: access-group 102
   params: 10000000 bps, 24000 limit, 32000 extended limit
   conformed 0 packets, 0 bytes; action: set-prec-transmit 5
   exceeded 0 packets, 0 bytes; action: drop
   last packet: 19522612ms ago, current burst: 0 bytes
   last cleared 00:07:18 ago, conformed 0 bps, exceeded 0 bps
  matches: all traffic
   params: 8000000 bps, 16000 limit, 24000 extended limit
   conformed 5 packets, 315 bytes; action: set-prec-transmit 5
   exceeded 0 packets, 0 bytes; action: drop
   last packet: 9632ms ago, current burst: 0 bytes
   last cleared 00:05:43 ago, conformed 0 bps, exceeded 0 bps
```

Internet Exchange Point Example

This example uses rate-limiting to control traffic in an Internet Exchange Point (IXP). Since the IXP is comprised of many neighbors around a FDDI ring, MAC address rate-limit access lists are used to control traffic from a particular ISP. Traffic from one ISP (at 00e0.34b0.7777) is compared to a rate-limit of 80 Mbps of the 100 Mbps available on the FDDI connection. Traffic that conforms to this rate is transmitted. Non-conforming traffic is dropped.

```
interface Fddi2/1/0
 rate-limit input access-group rate-limit 100 800000000 64000 80000 conform-action
  transmit exceed-action drop
 ip address 200.200.6.1 255.255.255.0
!
access-list rate-limit 100 00e0.34b0.7777
```

To verify the configuration and monitor the CAR statistics, use the **show interfaces rate-limit**:

```
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: transmit
   exceeded 0 packets, 0 bytes; action: drop
   last packet: 4737508ms ago, current burst: 0 bytes
   last cleared 01:05:47 ago, conformed 0 bps, exceeded 0 bps
```

Command Reference

This section documents new or modified commands. All other commands used with this feature are documented in the Cisco IOS Release 11.1 command references or the Cisco Express Forwarding feature documentation.

- **access-list rate-limit**
- **rate-limit**
- **show access-lists**
- **show access-lists rate-limit**
- **show interfaces rate-limit**

access-list rate-limit

To configure an access list for use with Committed Access Rate (CAR) policies, use the **access-list rate-limit** global configuration command. The **no** form of this command removes the access list from the configuration.

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

Syntax Description

acl-index	Access list number. Use a number from 1 to 99 to classify packets by precedence or precedence mask, and use a number from 100 to 199 to classify by MAC address.
precedence	IP precedence.
mac-address	MAC address.
mask *prec-mask*	IP precedence mask; a two-digit hexadecimal number. Use this option when you want to assign multiple precedences to the same rate-limit access list.

Default

No CAR access lists are configured.

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.1 CC.

This command classifies packets with the specified IP precedence or MAC address into a particular CAR access list. You can then apply CAR policies, using the **rate-limit** command, to individual rate-limit access lists. Thus, packets with different IP precedences or MAC addresses are treated differently by the CAR process.

You can only specify one command for each rate-limit access list. If you enter this command multiple times with the same access list number, the new command will overwrite the previous command.

Use the **mask** keyword to assign multiple IP precedences to the same rate-limit list. To determine the mask value, perform the following steps:

Step 1 Decide which precedences you want to assign to this rate-limit access list.

Step 2 Convert the precedences into an 8-bit numbers with each bit corresponding to one precedence. For example, an IP precedence of 0 corresponds to 00000001, 1 corresponds to 00000010, 6 corresponds to 01000000, and 7 corresponds to 10000000.

Step 3 Add the 8-bit numbers for the selected precedences together. For example, the mask for precedences 1 and 6 is 01000010.

Step 4 Convert the binary mark into the corresponding hexadecimal number. For example, 01000010 becomes 0x42. This value is used in the **access-list rate-limit** command. Any packets that have an IP precedence of 1 or 6 will match this access list.

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

Example

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

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

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

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

Related Commands

rate-limit
show access-lists rate-limit
show interfaces rate-limit

rate-limit

To configure Committed Access Rate (CAR) policies, use the **rate-limit** interface configuration command. The **no** form of this command removes the rate limit from the configuration.

rate-limit {**input** | **output**} [**access-group** [**rate-limit**] *acl-index* | **qos-group** *qos-number*] *bps burst-normal burst-max* **conform-action** *action* **exceed-action** *action*
no rate-limit {**input** | **output**} [**access-group** [**rate-limit**] *acl-index* | **qos-group** *qos-number*] *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.
qos-group *qos-number*	(Optional) Applies this CAR traffic policy to the specified QoS group. Packets are assigned to QoS groups through previous **rate-limit** commands or QoS Policy Propagation via BGP.
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. • **set-qos-continue** *new-qos*—Set the QoS group and evaluate the next **rate-limit** command. • **set-qos-transmit** *new-qos*—Set the QoS group and transmit the packet. • **transmit—**Transmit the packet.

exceed-action	Action to take on packets that exceed the rate limit.

Default

CAR is disabled.

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.1 CC.

Use this command to configure your CAR policy on an interface. To specify multiple policies, enter this command once for each policy. For each policy, provide the following information:

- Whether the policy applies to packets input or output on the interface.
- (Optional) An access list, rate-limit access list, or QoS group to associate with the policy. The policy is only applied to packets that match the access list or group.
- Average rate. Traffic that falls under this rate will always conform.
- Normal burst size.
- Excess burst size.
- Action to take when a packet conforms to the rate limit.
- Action to take when a packet exceeds the rate limit.

Example

The following example limits the rate by application.

- All Web traffic is transmitted. However, the IP precedence for Web traffic that conforms to the first rate policy is set to 5. For non-conforming 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.

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

Related Commands

access-list rate-limit
show interfaces rate-limit

show access-lists

To display the contents of current IP and rate-limit access lists, use the **show access-lists** privileged EXEC command.

show access-lists [*access-list-number*]

Syntax Description

access-list-number	(Optional) Access list number to display. The range is 1 to 1199. The system displays all access lists by default.

Default

The system displays all access lists.

Command Mode

Privileged EXEC

Usage Guidelines

This command appeared before Cisco IOS Release 10.0.

Sample Display

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

```
Router# show access-lists

Standard IP access list 1
    permit any
Standard IP access list 1300
    permit any
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** command when access lists numbered 1 are displayed:

```
Router# show access-lists 1

Standard IP access list 1
    permit any
Rate-limit access list 1
    0
```

The following is sample output from the **show access-lists** command when an extended access list is configured:

```
Router# show access-lists 101

Extended IP access list 101
    permit tcp host 198.92.32.130 any established (4304 matches)
    permit udp host 198.92.32.130 any eq domain (129 matches)
    permit icmp host 198.92.32.130 any
    permit tcp host 198.92.32.130 host 171.69.2.141 gt 1023
    permit tcp host 198.92.32.130 host 171.69.2.135 eq smtp (2 matches)
    permit tcp host 198.92.32.130 host 198.92.30.32 eq smtp
    permit tcp host 198.92.32.130 host 171.69.108.33 eq smtp
    permit udp host 198.92.32.130 host 171.68.225.190 eq syslog
    permit udp host 198.92.32.130 host 171.68.225.126 eq syslog
    deny   ip 150.136.0.0 0.0.255.255 224.0.0.0 15.255.255.255
    deny   ip 171.68.0.0 0.1.255.255 224.0.0.0 15.255.255.255 (2 matches)
    deny   ip 172.24.24.0 0.0.1.255 224.0.0.0 15.255.255.255
    deny   ip 192.82.152.0 0.0.0.255 224.0.0.0 15.255.255.255
    deny   ip 192.122.173.0 0.0.0.255 224.0.0.0 15.255.255.255
    deny   ip 192.122.174.0 0.0.0.255 224.0.0.0 15.255.255.255
    deny   ip 192.135.239.0 0.0.0.255 224.0.0.0 15.255.255.255
    deny   ip 192.135.240.0 0.0.7.255 224.0.0.0 15.255.255.255
    deny   ip 192.135.248.0 0.0.3.255 224.0.0.0 15.255.255.255
    deny   ip 192.150.42.0 0.0.0.255 224.0.0.0 15.255.255.255
```

An access list counter counts how many packets are allowed by each line of the access list. This number is displayed as the number of matches.

Related Commands

access-list (extended)
access-list (standard)
access-list rate-limit
clear access-list counters
clear access-temp
ip access-list
show access-lists rate-limit
show ip access-list

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 Mode

EXEC

Usage Guidelines

This command first appeared in Cisco IOS Release 11.1 CC.

Sample Display

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 1 describes the fields shown in these displays.

Table 1 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

access-list rate-limit
rate-limit

show interfaces rate-limit

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

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

Syntax Description

interface	(Optional) Type and number of the interface.

Command Mode

EXEC

Usage Guidelines

This command first appeared in Cisco IOS Release 11.1 CC.

Sample Display

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 2 describes the fields shown in this display.

Table 2 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 with 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	Number of packets conforming since the counter last cleared with the **clear counters** command.
exceeded	Number of packets exceeding since the counter last cleared with the **clear counters** command.
Output	These rate limits apply to packets sent by the interface.

Related Commands

access-list rate-limit
clear counters
rate-limit