

queue-limit

To specify or modify the maximum number of packets the queue can hold for a class policy configured in a policy map, use the **queue-limit** policy-map class configuration command. To remove the queue packet limit from a class, use the **no** form of this command.

queue-limit *number-of-packets*

no queue-limit *number-of-packets*

Syntax Description	<i>number-of-packets</i>	A number in the range 1 to 64 specifying the maximum number of packets that the queue for this class can accumulate.
---------------------------	--------------------------	--

Defaults	64
-----------------	----

Command Modes	Policy-map class configuration
----------------------	--------------------------------

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

Usage Guidelines	Weighted fair queueing (WFQ) creates a queue for every class for which a class map is defined. Packets satisfying the match criteria for a class accumulate in the queue reserved for the class until they are sent, which occurs when the queue is serviced by the fair queueing process. When the maximum packet threshold you defined for the class is reached, enqueueing of any further packets to the class queue causes tail drop or, if Weighted Random Early Detection (WRED) is configured for the class policy, packet drop to take effect.
-------------------------	--

Examples	The following example configures a policy map called policy11 to contain policy for a class called acl203. Policy for this class is set so that the queue reserved for it has a maximum packet limit of 40.
-----------------	---

```
policy-map policy11
  class acl203
    bandwidth 2000
    queue-limit 40
```

Related Commands	Command	Description
	class (policy-map)	Specifies the name of the class whose policy you want to create or change, and the default class (commonly known as the class-default class) before you configure its policy.
	policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.

queue-list default

To assign a priority queue for those packets that do not match any other rule in the queue list, use the **queue-list default** global configuration command. To restore the default value, use the **no** form of this command.

queue-list *list-number* **default** *queue-number*

no queue-list *list-number* **default** *queue-number*

Syntax Description

<i>list-number</i>	Number of the queue list. Any number from 1 to 16 that identifies the queue list.
<i>queue-number</i>	Number of the queue. Any number from 1 to 16. The default number of the queue list is queue number 1.

Defaults

This command is disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

When you use multiple rules, remember that the system reads the **queue-list** commands in order of appearance. When classifying a packet, the system searches the list of rules specified by **queue-list** commands for a matching protocol or interface type. When a match is found, the system assigns the packet to the appropriate queue. The system searches the list in the order specified, and the first matching rule terminates the search.

Queue number 0 is a system queue. It is emptied before any of the other queues are processed. The system enqueues high-priority packets, such as keepalives, to this queue.

Use the **show interfaces** command to display the current status of the output queues.

Examples

In the following example, the default queue for list 10 is set to queue number 2:

```
queue-list 10 default 2
```

Related Commands

Command	Description
custom-queue-list	Assigns a custom queue list to an interface.
queue-list interface	Establishes queuing priorities on packets entering on an interface.
queue-list protocol	Establishes queuing priority based on the protocol type.

Command	Description
queue-list queue byte-count	Specifies how many bytes the system allows to be delivered from a given queue during a particular cycle.
queue-list queue limit	Designates the queue length limit for a queue.
show queue	Displays the contents of packets inside a queue for a particular interface or VC.
show queueing	Lists all or selected configured queueing strategies.

queue-list interface

To establish queueing priorities on packets entering on an interface, use the **queue-list interface** global configuration command. To remove an entry from the list, use the **no** form of this command.

queue-list *list-number* **interface** *interface-type* *interface-number* *queue-number*

no queue-list *list-number* **interface** *interface-type* *interface-number* *queue-number*

Syntax Description

<i>list-number</i>	Number of the queue list. Any number from 1 to 16 that identifies the queue list.
<i>interface-type</i>	Type of the interface.
<i>interface-number</i>	Number of the interface.
<i>queue-number</i>	Number of the queue. Any number from 1 to 16.

Defaults

No queueing priorities are established.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

When you use multiple rules, remember that the system reads the **queue-list** commands in order of appearance. When classifying a packet, the system searches the list of rules specified by **queue-list** commands for a matching protocol or interface type. When a match is found, the system assigns the packet to the appropriate queue. The list is searched in the order specified, and the first matching rule terminates the search.

Examples

In the following example, queue list 4 establishes queueing priorities for packets entering on interface tunnel 3. The queue number assigned is 10.

```
queue-list 4 interface tunnel 3 10
```

Related Commands

Command	Description
custom-queue-list	Assigns a custom queue list to an interface.
queue-list default	Assigns a priority queue for those packets that do not match any other rule in the queue list.
queue-list protocol	Establishes queueing priority based on the protocol type.
queue-list queue byte-count	Specifies how many bytes the system allows to be delivered from a given queue during a particular cycle.

Command	Description
queue-list queue limit	Designates the queue length limit for a queue.
show queue	Displays the contents of packets inside a queue for a particular interface or VC.
show queueing	Lists all or selected configured queueing strategies.

queue-list lowest-custom

To set the lowest number for a queue to be treated as a custom queue, use the **queue-list lowest-custom** command in global configuration mode. To restore the default value, use the **no** form of this command.

queue-list *list-number* **lowest-custom** *queue-number*

no queue-list *list-number* **lowest-custom** *queue-number*

Syntax Description

<i>list-number</i>	Number of the queue list. Any number from 1 to 16 that identifies the queue list.
<i>queue-number</i>	Number of the queue. Any number from 1 to 16.

Defaults

The default number of the lowest custom queue is 1.

Command Modes

Global configuration

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

All queues from queue 0 to the queue prior to the one specified in the **queue-list lowest-custom** command use the priority queue. (Queue 0 has the highest priority.)

All queues from the one specified in the **queue-list lowest-custom** command to queue 16 use a round-robin scheduler.

Use the **show queuing custom** command to display the current custom queue configuration.

Examples

In the following example, the lowest custom value is set to 2 for queue list 4:

```
queue-list 4 lowest-custom 2
```

Related Commands	Command	Description
	custom-queue-list	Assigns a custom queue list to an interface.
	queue-list interface	Establishes queueing priorities on packets entering on an interface.
	queue-list protocol	Establishes queueing priority based on the protocol type.
	queue-list queue byte-count	Specifies how many bytes the system allows to be delivered from a given queue during a particular cycle.
	queue-list queue limit	Designates the queue length limit for a queue.
	show queue	Displays the contents of packets inside a queue for a particular interface or VC.
	show queueing	Lists all or selected configured queueing strategies.

queue-list protocol

To establish queueing priority based upon the protocol type, use the **queue-list protocol** global configuration command. To remove an entry from the list, use the **no** form of this command with the appropriate arguments.

queue-list *list-number* **protocol** *protocol-name* *queue-number* *queue-keyword* *keyword-value*

no queue-list *list-number* **protocol** *protocol-name* *queue-number* *queue-keyword* *keyword-value*

Syntax Description

<i>list-number</i>	Number of the queue list. Any number from 1 to 16.
<i>protocol-name</i>	Protocol type: aarp , apollo , appletalk , arp , bridge (transparent), clns , clns_es , clns_is , cmns , compressedtcp , decnet , decnet_node , decnet_router11 , decnet_router12 , dls , ip , ipx , pad , rsrb , stun , vines , xns , and x25 .
<i>queue-number</i>	Number of the queue. Any number from 1 to 16.
<i>queue-keyword</i> <i>keyword-value</i>	Possible keywords are fragments , gt , list , lt , tcp , and udp . See Table 8 from the priority-list protocol command.

Defaults

No queueing priorities are established.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

When you use multiple rules for a single protocol, remember that the system reads the **queue-list** commands in order of appearance. When classifying a packet, the system searches the list of rules specified by **queue-list** commands for a matching protocol. When a match is found, the system assigns the packet to the appropriate queue. The system searches the list in the order specified, and the first matching rule terminates the search.

The **decnet_router-11** keyword refers to the multicast address for all level 1 routers, which are intra-area routers, and the **decnet_router-12** keyword refers to all level 2 routers, which are interarea routers.

The **dls**, **rsrb**, and **stun** keywords refer only to direct encapsulation.

Use Table 8, Table 9, and Table 10 from the **priority-list protocol** command to configure the queueing priorities for your system.

Examples

The following example assigns 1 as the custom queue list, specifies DECnet as the protocol type, and assigns 3 as a queue number to the packets sent on this interface:

```
queue-list 1 protocol decnet 3
```

The following example assigns DECnet packets with a size greater than 200 bytes to queue number 2:

```
queue-list 2 protocol decnet 2 gt 200
```

The following example assigns DECnet packets with a size less than 200 bytes to queue number 2:

```
queue-list 4 protocol decnet 2 lt 200
```

The following example assigns traffic that matches IP access list 10 to queue number 1:

```
queue-list 1 protocol ip 1 list 10
```

The following example assigns Telnet packets to queue number 2:

```
queue-list 4 protocol ip 2 tcp 23
```

The following example assigns UDP Domain Name Service packets to queue number 2:

```
queue-list 4 protocol ip 2 udp 53
```

The following example assigns traffic that matches Ethernet type code access list 201 to queue number 1:

```
queue-list 1 protocol bridge 1 list 201
```

Related Commands

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

queue-list queue byte-count

To specify how many bytes the system allows to be delivered from a given queue during a particular cycle, use the **queue-list queue byte-count** global configuration command. To return the byte count to the default value, use the **no** form of this command.

queue-list *list-number* **queue** *queue-number* **byte-count** *byte-count-number*

no queue-list *list-number* **queue** *queue-number* **byte-count** *byte-count-number*

Syntax Description

<i>list-number</i>	Number of the queue list. Any number from 1 to 16.
<i>queue-number</i>	Number of the queue. Any number from 1 to 16.
<i>byte-count-number</i>	The average number of bytes the system allows to be delivered from a given queue during a particular cycle.

Defaults

This command is not enabled by default.

The default byte count is 1500 bytes.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Examples

In the following example, queue list 9 establishes the byte count as 1400 for queue number 10:

```
queue-list 9 queue 10 byte-count 1400
```

Related Commands

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

queue-list queue limit

To designate the queue length limit for a queue, use the **queue-list queue limit** global configuration command. To return the queue length to the default value, use the **no** form of this command.

queue-list *list-number* **queue** *queue-number* **limit** *limit-number*

no queue-list *list-number* **queue** *queue-number* **limit** *limit-number*

Syntax Description

<i>list-number</i>	Number of the queue list. Any number from 1 to 16.
<i>queue-number</i>	Number of the queue. Any number from 1 to 16.
<i>limit-number</i>	Maximum number of packets that can be enqueued at any time. The range is 0 to 32767 queue entries. A value of 0 means that the queue can be of unlimited size. The default queue length limit is 20 entries.

Defaults

The default queue length limit for a queue is 20.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Examples

In the following example, the queue length of queue 10 is increased to 40:

```
queue-list 5 queue 10 limit 40
```

Related Commands

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

random-detect (interface)

To enable Weighted Random Early Detection (WRED) or VIP-Distributed WRED (DWRED), use the **random-detect** interface configuration command. To configure WRED as class policy in a policy map, use the **random-detect** policy-map class configuration command. To disable WRED or DWRED, use the **no** form of this command.

random-detect

no random-detect

Syntax Description This command has no arguments or keywords.

Defaults WRED and DWRED are disabled by default.

Command Modes Interface configuration when used on an interface.
Policy-map class configuration when used to specify class policy in a policy map.

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 congestion exists. DWRED is similar to WRED but uses the Versatile Interface Processor (VIP) instead of the Route Switch Processor (RSP). WRED and DWRED are most 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 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*.

WRED in a Policy Map

You can configure WRED as part of the policy for a standard class or the default class. The WRED **random-detect** command and the weighted fair queueing (WFQ) **queue-limit** command are mutually exclusive for class policy. If you configure WRED, its packet drop capability is used to manage the queue when packets exceeding the configured maximum count are enqueued. If you configure the WFQ **queue-limit** command for class policy, tail drop is used.

To configure a policy map and create class policies, use the **policy-map** and **class** (policy-map) commands. When specifying class policy within a policy map, you can use the **random-detect** command with either of the following commands:

- **bandwidth** (policy-map class)
- **fair-queue** (class-default)—for the default class only

Note that if you use WRED packet drop instead of tail drop for one or more classes composing a policy map, you must ensure that WRED is not configured for the interface to which you attach that service policy.

The DWRED feature is not supported for class policy.

Examples

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

```
interface Hssi0/0/0
 random-detect
```

The following example configures the policy map called `policy1` to contain policy specification for the class called `class1`. During times of congestion, WRED packet drop is used instead of tail drop.

! The following commands create the class map called `class1`:

```
class-map class1
 match input-interface FE0/1
```

! The following commands define `policy1` to contain policy specification for `class1`:

```
policy-map policy1
 class class1
  bandwidth 1000
  random-detect
```

Related Commands

Command	Description
random-detect	Configures the WRED and DWRED exponential weight factor for the average queue size calculation.
exponential-weighting-constant	
random-detect flow	Enables flow-based WRED.
random-detect precedence	Configures WRED and DWRED parameters for a particular IP Precedence.
rate-limit	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 queueing	Lists all or selected configured queueing strategies.
show tech-support rsvp	Generates a report of all RSVP-related information.

P Precedence

random-detect (per VC)

To enable per-virtual circuit (VC) Weighted Random Early Detection (WRED) or per-VC VIP-Distributed WRED (DWRED), use the **random-detect** VC submode command. To disable per-VC WRED and per-VC DWRED, use the **no** form of this command.

random-detect [**attach** *group-name*]

no random-detect [**attach** *group-name*]

Syntax Description

attach *group-name* (Optional) The name of the WRED/DWRED group.

Defaults

WRED and DWRED are disabled by default.

Command Modes

VC submode

Command History

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

Usage Guidelines

WRED is a congestion avoidance mechanism that slows traffic by randomly dropping packets when congestion exists. DWRED is similar to WRED but uses the Versatile Interface Processor (VIP) instead of the Route Switch Processor (RSP). WRED and DWRED are most useful with protocols like TCP that respond to dropped packets by decreasing the transmission rate.

WRED and DWRED are configurable at the interface and per-VC levels. The VC-level WRED/DWRED configuration will override the interface-level configuration if WRED/DWRED is also configured at the interface level.

Use this command to configure a single ATM VC or a VC that is a member of a bundle.

Remember the following guidelines when using the **random-detect (per VC)** command:

- If you use this command without the optional **attach** keyword, default WRED/DWRED parameters (such as minimum and maximum thresholds) are used.
- If you use this command with the optional **attach** keyword, the parameters defined by the specified WRED/DWRED parameter group are used. (WRED/DWRED parameter groups are defined through the **random-detect-group** command.) If the specified WRED/DWRED group does not exist, the VC is configured with default WRED/DWRED parameters.

When this command is used to configure an interface-level WRED/DWRED group to include per-VC WRED/DWRED as a drop policy, the configured WRED/DWRED group parameters are inherited under the following conditions:

- All existing VCs—including Resource Reservation Protocol (RSVP) switched virtual circuits (SVCs) that are not specifically configured with a VC-level WRED/DWRED group—will inherit the interface-level WRED or DWRED group parameters.
- Except for the VC used for signalling and the Interim Local Management Interface (ILMI) VC, any VCs created after the configuration of an interface-level DWRED group will inherit the parameters.

When an interface-level WRED/DWRED group configuration is removed, per-VC WRED/DWRED parameters are removed from any VC that inherited them from the configured interface-level WRED/DWRED group.

When an interface-level WRED/DWRED group configuration is modified, per-VC WRED/DWRED parameters are modified accordingly if the WRED/DWRED parameters were inherited from the configured interface-level WRED/DWRED group configuration.

This command is only supported on interfaces that are capable of VC-level queuing. The only currently supported interface is the Enhanced ATM port adapter (PA-A3).

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 per-VC WRED for the permanent virtual circuit (PVC) called cisco. Because the **attach** keyword was not used, WRED uses default parameters.

```
pvc cisco 46
  random-detect
```

The following example creates a DWRED group called Rome and then applies the parameter group to an ATM PVC:

```
! The following commands create the DWRED parameter group Rome:
random-detect-group Rome
precedence rsvp 46 50 10
precedence 1 32 50 10
precedence 2 34 50 10
precedence 3 36 50 10
precedence 4 38 50 10
precedence 5 40 50 10
precedence 6 42 50 10
precedence 7 44 50 10
exit
exit
```

```

! The following commands create a PVC on an ATM interface and then apply the
! DWRED group Rome to that PVC:
interface ATM2/0.23 point-to-point
 ip address 10.9.23.10 255.255.255.0
 no ip mroute-cache
 pvc vc1 201/201
  random-detect attach Rome
  vbr-nrt 2000 1000 200
  encapsulation aal5snap

```

The following **show queueing** command displays the current settings for each of the IP Precedences following configuration of per-VC DWRED:

```

Router# show queueing random-detect interface atm2/0.23 vc 201/201
random-detect group Rome:

exponential weight 9
class      min-threshold  max-threshold  mark-probability
-----
0          30                50              1/10
1          32                50              1/10
2          34                50              1/10
3          36                50              1/10
4          38                50              1/10
5          40                50              1/10
6          42                50              1/10
7          44                50              1/10
rsvp      46                50              1/10

```

Related Commands

Command	Description
class (policy-map)	Specifies the name of the class whose policy you want to create or change, and the default class (commonly known as the class-default class) before you configure its policy.
random-detect exponential-weighting-constant	Configures the WRED and DWRED exponential weight factor for the average queue size calculation.
random-detect-group	Defines the WRED or DWRED parameter group.
random-detect precedence	Configures WRED and DWRED parameters for a particular IP Precedence.
show interfaces	Displays the statistical information specific to a serial interface.
show queue	Displays the contents of packets inside a queue for a particular interface or VC.
show queueing	Lists all or selected configured queueing strategies.

random-detect exponential-weighting-constant

To configure the Weighted Random Early Detection (WRED) and VIP-Distributed WRED (DWRED) exponential weight factor for the average queue size calculation for the queue, use the **random-detect exponential-weighting-constant** interface configuration command. To configure the exponential weight factor for the average queue size calculation for the queue reserved for a class, use the **random-detect exponential-weighting-constant** policy-map class 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	<i>exponent</i>	Exponent from 1 to 16 used in the average queue size calculation.
---------------------------	-----------------	---

Defaults	The default exponential weight factor is 9.
-----------------	---

Command Modes	Interface configuration when used on an interface. Policy-map class configuration when used to specify class policy in a policy map.
----------------------	---

Command History	Release	Modification
	11.1 CC	This command was introduced.
	12.0(5)T	This command was made available as a policy-map class configuration command.

Usage Guidelines	WRED is a congestion avoidance mechanism that slows traffic by randomly dropping packets when congestion exists. DWRED is similar to WRED but uses the Versatile Interface Processor (VIP) instead of the Route Switch Processor (RSP). WRED and DWRED are most useful with protocols like TCP that 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. You can also use this command to configure the exponential weight factor for the average queue size calculation for the queue reserved for a class.



Note

The default WRED/DWRED 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 DWRED feature is not supported for class policy.

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:

```
interface Hssi0/0/0
  description 45Mbps to R1
  ip address 10.200.14.250 255.255.255.252
  random-detect
  random-detect exponential-weighting-constant 10
```

The following example configures the policy map policy1 to contain policy specification for the class called class1. During times of congestion, WRED packet drop is used instead of tail drop. The weight factor used for the average queue size calculation for the queue for class1 is 12.

```
! The following commands create the class map called class1:
class-map class1
  match input-interface FE0/1

! The following commands define policy1 to contain policy specification for class1:
policy-map policy1
  class class1
    bandwidth 1000
    random-detect
    random-detect exponential-weighting-constant 12
```

Related Commands

Command	Description
exponential-weighting-constant	Configures the exponential weight factor for the average queue size calculation for a WRED parameter group.
precedence (VC bundle)	Configures precedence levels for a VC member of a bundle, or for a VC class that can be assigned to a VC bundle.
precedence (WRED group)	Configures a WRED group for a particular IP Precedence.
random-detect (interface)	Enables WRED or DWRED.
random-detect (per VC)	Enables per-VC WRED or per-VC DWRED.
random-detect precedence	Configures WRED and DWRED parameters for a particular IP Precedence.
show policy-map	Displays the configuration of all classes comprising the specified service policy map or all classes for all existing policy maps.
show queue	Displays the contents of packets inside a queue for a particular interface or VC.
show queueing	Lists all or selected configured queueing strategies.

random-detect flow

To enable flow-based Weighted Random Early Detection (WRED), use the **random-detect flow** interface configuration command. To disable flow-based WRED, use the **no** form of this command.

random-detect flow

no random-detect flow

Syntax Description This command has no arguments or keywords.

Defaults Flow-based WRED is disabled by default.

Command Modes Interface configuration

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

Usage Guidelines You must use this command to enable flow-based WRED before you can use the **random-detect flow average-depth-factor** and **random-detect flow count** commands to further configure the parameters of flow-based WRED.

Before you can enable flow-based WRED, you must enable and configure WRED. For complete information, refer to the *Cisco IOS Quality of Service Solutions Configuration Guide*.

Examples The following example enables flow-based WRED on the Serial1 interface:

```
interface Serial1
 random-detect
 random-detect flow
```

Related Commands	Command	Description
	random-detect (interface)	Enables WRED or DWRED.
	random-detect exponential-weighting-constant	Configures the WRED and DWRED exponential weight factor for the average queue size calculation.
	random-detect flow average-depth-factor	Sets the multiplier to be used in determining the average depth factor for a flow when flow-based WRED is enabled.
	random-detect flow count	Sets the flow count for flow-based WRED.
	random-detect precedence	Configures WRED and DWRED parameters for a particular IP Precedence.
	show interfaces	Displays the statistical information specific to a serial interface.
	show queue	Displays the contents of packets inside a queue for a particular interface or VC.
	show queueing	Lists all or selected configured queueing strategies.

random-detect flow average-depth-factor

To set the multiplier to be used in determining the average depth factor for a flow when flow-based Weighted Random Early Detection (WRED) is enabled, use the **random-detect flow average-depth-factor** interface configuration command. To remove the current flow average depth factor value, use the **no** form of this command.

random-detect flow average-depth-factor *scaling-factor*

no random-detect flow average-depth-factor *scaling-factor*

Syntax Description	<i>scaling-factor</i>	The number 2, 4, 8 or 16. The default value is 4.
---------------------------	-----------------------	---

Defaults	The default average depth factor is 4.
-----------------	--

Command Modes	Interface configuration
----------------------	-------------------------

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

Usage Guidelines	Use this command to specify the scaling factor that flow-based WRED should use in scaling the number of buffers available per flow and in determining the number of packets allowed in the output queue for each active flow. This scaling factor is common to all flows. The outcome of the scaled number of buffers becomes the per-flow limit.
-------------------------	---

If this command is not used and flow-based WRED is enabled, the average depth scaling factor defaults to 4.

A flow is considered nonadaptive—that is, it takes up too much of the resources—when the average flow depth times the specified multiplier (scaling factor) is less than the depth for the flow, for example:

$\text{average-flow-depth} * (\text{scaling factor}) < \text{flow-depth}$

Before you use this command, you must use the **random-detect flow** command to enable flow-based WRED for the interface. To configure flow-based WRED, you may also use the **random-detect flow count** command.

Examples	The following example enables flow-based WRED on the Serial1 interface and sets the scaling factor for the average flow depth to 8:
-----------------	---

```
interface Serial1
 random-detect
 random-detect flow
 random-detect flow average-depth-factor 8
```

Related Commands	Command	Description
	random-detect (interface)	Enables WRED or DWRED.
	random-detect exponential-weighting-constant	Configures the WRED and DWRED exponential weight factor for the average queue size calculation.
	random-detect flow	Enables flow-based WRED.
	random-detect flow count	Sets the flow count for flow-based WRED.
	random-detect precedence	Configures WRED and DWRED parameters for a particular IP Precedence.
	show interfaces	Displays the statistical information specific to a serial interface.
	show queue	Displays the contents of packets inside a queue for a particular interface or VC.
	show queueing	Lists all or selected configured queueing strategies.

random-detect flow count

To set the flow count for flow-based Weighted Random Early Detection (WRED), use the **random-detect flow count** interface configuration command. To remove the current flow count value, use the **no** form of this command.

random-detect flow count *number*

no random-detect flow count *number*

Syntax Description	<i>number</i>	Specifies a value from 16 to 2^{15} (32768).
---------------------------	---------------	--

Defaults	256
-----------------	-----

Command Modes	Interface configuration
----------------------	-------------------------

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

Usage Guidelines	Before you use this command, you must use the random-detect flow command to enable flow-based WRED for the interface.
-------------------------	--

Examples	The following example enables flow-based WRED on the Serial1 interface and sets the flow threshold constant to 16:
-----------------	--

```
interface Serial1
 random-detect
 random-detect flow
 random-detect flow count 16
```

Related Commands	Command	Description
	random-detect (interface)	Enables WRED or DWRED.
	random-detect exponential-weighting-constant	Configures the WRED and DWRED exponential weight factor for the average queue size calculation.
	random-detect flow	Enables flow-based WRED.
	random-detect precedence	Configures WRED and DWRED parameters for a particular IP Precedence.
	show interfaces	Displays the statistical information specific to a serial interface.

Command	Description
show queue	Displays the contents of packets inside a queue for a particular interface or VC.
show queueing	Lists all or selected configured queueing strategies.

random-detect-group

To define the Weighted Random Early Detection (WRED) or VIP-Distributed WRED (DWRED) parameter group, use the **random-detect group** global configuration command. To delete the WRED/DWRED parameter group, use the **no** form of this command.

random-detect-group *group-name*

no random-detect-group *group-name*

Syntax Description

<i>group-name</i>	Name for the WRED/DWRED parameter group.
-------------------	--

Defaults

No WRED/DWRED parameter group exists.

Command Modes

Global configuration

Command History

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

Usage Guidelines

WRED is a congestion avoidance mechanism that slows traffic by randomly dropping packets when there is congestion. DWRED is similar to WRED but uses the Versatile Interface Processor (VIP) instead of the Route Switch Processor (RSP). WRED and DWRED are most useful when the traffic uses protocols such as TCP, that respond to dropped packets by decreasing the transmission rate.

The router automatically determines parameters to use in the WRED calculations. If you want to change these parameters for a group, use the **exponential-weighting-constant** or **precedence** command.

Examples

The following example defines the WRED parameter group called sanjose:

```
random-detect-group sanjose
precedence 0 32 256 100
precedence 1 64 256 100
precedence 2 96 256 100
precedence 3 128 256 100
precedence 4 160 256 100
precedence 5 192 256 100
precedence 6 224 256 100
precedence 7 256 256 100
```

Related Commands	Command	Description
	exponential-weighting-constant	Configures the exponential weight factor for the average queue size calculation for a WRED parameter group.
	precedence (WRED group)	Configures a WRED group for a particular IP Precedence.
	random-detect (per VC)	Enables per-VC WRED or per-VC DWRED.
	show queueing	Lists all or selected configured queueing strategies.
	show queueing interface	Displays the queueing statistics of an interface or VC.

random-detect precedence

To configure Weighted Random Early Detection (WRED) and VIP-Distributed WRED (DWRED) parameters for a particular IP Precedence, use the **random-detect precedence** interface configuration command. To configure WRED parameters for a particular IP Precedence for a class policy in a policy map, use the **random-detect precedence** policy-map class 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

<i>precedence</i>	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 range is 0 to 7 only; see Table 12.
<i>min-threshold</i>	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 randomly drops some packets with the specified IP Precedence.
<i>max-threshold</i>	Maximum threshold in number of packets. The value range of this argument is the value of the <i>min-threshold</i> argument to 4096. When the average queue length exceeds the maximum threshold, WRED drops all packets with the specified IP Precedence.
<i>mark-prob-denominator</i>	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* default 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 12 lists the default minimum threshold value for each IP Precedence.

Table 12 Default WRED and DWRED Minimum Threshold Values

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

Table 12 Default WRED and DWRED Minimum Threshold Values (continued)

IP Precedence	Minimum Threshold Value (Fraction of Maximum Threshold Value)	
	WRED	DWRED
3	12/18	11/16
4	13/18	12/16
5	14/18	13/16
6	15/18	14/16
7	16/18	15/16
RSVP	17/18	—

Command Modes

Interface configuration when used on an interface.

Policy-map class configuration when used to specify class policy in a policy map.

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 congestion exists. DWRED is similar to WRED but uses the Versatile Interface Processor (VIP) instead of the Route Switch Processor (RSP).

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 precedences.

If you want WRED/DWRED 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 that if you use the **random-detect precedence** command to adjust the treatment for different precedences within class policy, you must ensure that WRED is not configured for the interface to which you attach that service policy.

**Note**

The default WRED/DWRED 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 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*.

**Note**

The DWRED feature is not supported in a class policy.

Examples

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

```
interface Hssi0/0/0
description 45Mbps to R1
ip address 10.200.14.250 255.255.255.252
random-detect
random-detect precedence 0 32 256 100
random-detect precedence 1 64 256 100
random-detect precedence 2 96 256 100
random-detect precedence 3 120 256 100
random-detect precedence 4 140 256 100
random-detect precedence 5 170 256 100
random-detect precedence 6 290 256 100
random-detect precedence 7 210 256 100
random-detect precedence rsvp 230 256 100
```

The following example configures policy for a class called acl10 included in the policy map called policy10. Class acl101 has these characteristics: a minimum of 2000 kbps of bandwidth are expected to be delivered to this class in the event of congestion and a weight factor of 10 is used to calculate the average queue size. For congestion avoidance, WRED packet drop is used, not tail drop. IP Precedence is reset for levels 0 through 4.

```
policy-map policy10
class acl10
bandwidth 2000
random-detect
random-detect exponential-weighting-constant 10
random-detect precedence 0 32 256 100
random-detect precedence 1 64 256 100
random-detect precedence 2 96 256 100
random-detect precedence 3 120 256 100
random-detect precedence 4 140 256 100
```

Related Commands

Command	Description
bandwidth (policy-map class)	Specifies or modifies the bandwidth allocated for a class belonging to a policy map.
random-detect (interface)	Enables WRED or DWRED.
random-detect (per VC)	Enables per-VC WRED or per-VC DWRED.
random-detect exponential-weighting-constant	Configures the WRED and DWRED exponential weight factor for the average queue size calculation.
show policy-map interface	Displays the configuration of classes configured for service policies on the specified interface or PVC.
show queue	Displays the contents of packets inside a queue for a particular interface or VC.
show queueing	Lists all or selected configured queueing strategies.

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 } [dscp dscp-value] [access-group [rate-limit] acl-index] bps
  burst-normal burst-max conform-action action exceed-action action
```

```
no rate-limit { input | output } [dscp dscp-value] [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.
dscp	(Optional) Allows the rate limit to be applied to any packet matching a specified differentiated services code point (DSCP).
<i>dscp-value</i>	(Optional) The DSCP number; values are 0 to 63.
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.
<i>acl-index</i>	(Optional) Access list number.
<i>bps</i>	Average rate in bits per second. The value must be in increments of 8 kbps.
<i>burst-normal</i>	Normal burst size in bytes. The minimum value is bps divided by 2000.
<i>burst-max</i>	Excess burst size in bytes.
conform-action	Action to take on packets that conform to the rate limit.
<i>action</i>	Action to take on packets. Specify one of the following keywords: <ul style="list-style-type: none"> continue—Evaluate the next rate-limit command. drop—Drop the packet. set-prec-continue <i>new-prec</i>—Set the IP Precedence and evaluate the next rate-limit command. set-prec-transmit <i>new-prec</i>—Set the IP Precedence and send the packet. transmit—Send 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 following example limits the rate by application:

```
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 10.200.14.250 255.255.255.252
  !
  access-list 101 permit tcp any any eq www
  access-list 102 permit tcp any any eq ftp
```

The following points further clarify the example:

- All World Wide Web traffic is sent. 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 sent 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 16,000 bytes and an excess burst size of 24,000 bytes. Traffic that conforms is sent with an IP Precedence of 5. Traffic that does not conform is dropped.
- Two access lists are created to classify the Web and FTP traffic so that they can be handled separately by the CAR feature.

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.

service-policy

To attach a policy map to an input interface or virtual circuit (VC), or an output interface or VC to be used as the service policy for that interface or VC, use the **service-policy** global configuration command. To remove a service policy from an input or output interface or input or output VC, use the **no** form of this command.

```
service-policy {input | output} policy-map
```

```
no service-policy {input | output}
```

Syntax Description		
	input	Attaches the specified policy map to the input interface or input VC.
	output	Attaches the specified policy map to the output interface or output VC.
	<i>policy-map</i>	The name of a service policy map (created using the policy-map command) to be attached.

Defaults No service policy is specified.

Command Modes Global configuration.
 VC submode (for a standalone VC).
 Bundle-vc configuration (for ATM VC bundle members).

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

Usage Guidelines You can attach a single policy map to one or more interfaces or one or more VCs to specify the service policy for those interfaces or VCs.

Currently a service policy specifies class-based weighted fair queueing (CBWFQ). The class policies comprising the policy map are then applied to packets that satisfy the class map match criteria for the class.

To successfully attach a policy map to an interface or a VC, the aggregate of the configured minimum bandwidths of the classes comprising the policy map must be less than or equal to 75 percent of the interface bandwidth or the bandwidth allocated to the VC.

Configuring CBWFQ on a physical interface is only possible if the interface is in the default queueing mode. Serial interfaces at E1 (2.048 Mbps) and below use WFQ by default. Other interfaces use FIFO by default. Enabling CBWFQ on a physical interface overrides the default interface queueing method. Enabling CBWFQ on an ATM permanent virtual circuit (PVC) does not override the default queueing method.

Attaching a service policy and enabling CBWFQ on an interface renders ineffective any commands related to fancy queueing such as commands pertaining to fair queueing, custom queueing, priority queueing, and Weighted Random Early Detection (WRED). You can configure these features only after you remove the policy map from the interface.

You can modify a policy map attached to an interface or a VC, changing the bandwidth of any of the classes comprising the map. Bandwidth changes that you make to an attached policy map are effective only if the aggregate of the bandwidth amounts for all classes comprising the policy map, including the modified class bandwidth, is less than or equal to 75 percent of the interface bandwidth or the VC bandwidth. If the new aggregate bandwidth amount exceeds 75 percent of the interface bandwidth or VC bandwidth, the policy map is not modified.

Examples

The following example attaches the service policy map called policy9 to the input interface Serial1:

```
interface Serial1
service-policy input policy9
```

The following example attaches the service policy map called policy9 to the input PVC called cisco:

```
pvc cisco 0/34
service-policy input policy9
vbr-nt 5000 3000 500
precedence 4-7
```

The following example attaches the policy called policy9 to the output interface serial1 to specify the service policy for the interface and enable CBWFQ on it:

```
interface serial1
service-policy output policy9
```

The following example attaches the service policy map called policy9 to the output PVC called cisco:

```
pvc cisco 0/5
service-policy output policy9
vbr-nt 4000 2000 500
precedence 2-3
```

Related Commands

Command	Description
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
show policy-map	Displays the configuration of all classes comprising the specified service policy map or all classes for all existing policy maps.

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 unchanged, use the **no** form of this command.

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

no set ip precedence

Syntax Description	<i>number</i> <i>name</i>	(Optional) A number or name that sets the precedence bits in the IP header. The values for the <i>number</i> argument and the corresponding <i>name</i> argument are listed in Table 13, from least to most important.
---------------------------	-----------------------------	--

Defaults	This command is disabled by default.
-----------------	--------------------------------------

Command Modes	Route-map configuration
----------------------	-------------------------

Command History	Release	Modification
	11.0	This command was introduced.

Usage Guidelines	Table 13 lists the values for the <i>number</i> argument and the corresponding <i>name</i> argument for precedence values in the IP header. They are listed from least to most important.
-------------------------	---

Table 13 Number and Name Values for IP Precedence

Number	Name
0	routine
1	priority
2	immediate
3	flash
4	flash-override
5	critical
6	internet
7	network

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 the high-end Internet QoS available from Cisco, 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:

```
interface serial 0
 ip policy route-map texas

route-map texas
match length 68 128
set ip precedence 5
```

Related Commands

Command	Description
fair-queue (WFQ)	Enables WFQ for an interface.
ip policy route-map	Identifies a route map to use for policy routing on an interface.
random-detect (interface)	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 BECN signals 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

<i>group-id</i>	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 fairly in the queue 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.

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