

qos pre-classify

To enable quality of service (QoS) preclassification, use the **qos pre-classify** command in interface configuration mode. To disable the QoS preclassification feature, use the **no** form of this command.

qos pre-classify

no qos pre-classify

Syntax Description This command has no arguments or keywords.

Defaults Disabled

Command Modes Interface configuration

Command History	Release	Modification
	12.0(5)XE3	This command was introduced.
	12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
	12.2(2)T	This command was implemented on the Cisco 2600 and Cisco 3600 series routers.

Usage Guidelines This command is restricted to tunnel interfaces, virtual templates, and crypto maps. The **qos pre-classify** command is unavailable on all other interface types.

The **qos pre-classify** command can be enabled for IP packets only.

Examples The following example enables the QoS for Virtual Private Networks (VPNs) feature on tunnel interfaces and virtual templates:

```
Router(config-if)# qos pre-classify
```

The following example enables the QoS for VPNs feature on crypto maps:

```
Router(config-crypto-map)# qos pre-classify
```

Related Commands	Command	Description
	show interfaces	Displays statistics for the interfaces configured on a router or access server.
	show queue	Displays the contents of packets inside a queue for a particular interface or VC.

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** command in policy-map class configuration mode. 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 from 1 to 64 specifying the maximum number of packets that the queue for this class can accumulate.
--------------------------	---

Defaults

On the Versatile Interface Processor (VIP)-based platforms, the default value is chosen as a function of the bandwidth assigned to the traffic class. The default value is also based on available buffer memory. If sufficient buffer memory is available, the default **queue-limit** value is equal to the number of 250-byte packets that would lead to a latency of 500 milliseconds (ms) when the packets are delivered at the configured rate. For example, if two 250-byte packets are required to lead to a latency of 500 ms, the default *number-of-packets* value would be 2.

On all other platforms, the default is 64.

Command Modes

Policy-map class configuration

Command History

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

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.

Overriding Queue Limits Set by the Bandwidth Command

The **bandwidth** command can be used with the Modular Command-Line Interface (MQC) to specify the bandwidth for a particular class. When used with the MQC, the **bandwidth** command uses a default queue limit for the class. This queue limit can be modified using the **queue-limit** command, thereby overriding the default set by the **bandwidth** command.

**Note**

Using the **queue-limit** command to modify the default queue-limit is especially important for higher-speed interfaces, in order to meet the minimum bandwidth guarantees required by the interface.

Examples

The following example 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.
class class-default	Specifies the default traffic class whose bandwidth is to be configured or modified.
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** command in global configuration mode. 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.

Defaults

Disabled

The default number of the queue list is queue number 1.

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 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 interface

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

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 , appletalk , arp , bridge (transparent), clns , clns_es , clns_is , cmns , compressedtcp , decnet , decnet_node , decnet_router11 , decnet_router12 , dlsw , ip , ipx , pad , rsrb , stun and x25 .
<i>queue-number</i>	Number of the queue. Any number from 1 to 16.
<i>queue-keyword keyword-value</i>	Possible keywords are fragments , gt , list , lt , tcp , and udp . See Table 9 of 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.
12.2(13)T	This command was modified to remove apollo, vines, and xns from the list of protocol types. These protocols were removed because Apollo Domain, Banyan VINES, and Xerox Network Systems (XNS) were removed in Release 12.2(13)T.

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

Use [Table 9](#), [Table 10](#), and [Table 11](#) in the **priority-list protocol** command section 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 User Datagram Protocol (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** command in global configuration mode. 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 disabled 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 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 queue limit

To designate the queue length limit for a queue, use the **queue-list queue limit** command in global configuration mode. 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 from 0 to 32767 queue entries. A value of 0 means that the queue can be of unlimited size.

Defaults

The default queue length limit is 20 entries.

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 discard-class

To configure the weighted random early detection (WRED) parameters for a discard-class value for a class policy in a policy map, use the **random-detect discard-class** command in policy-map class configuration mode. To disable this feature, use the **no** form of this command.

random-detect discard-class *value min-threshold max-threshold mark-prob-denominator*

no random-detect discard-class *value min-threshold max-threshold mark-prob-denominator*

Syntax Description

<i>value</i>	Discard class. Valid values are 0 to 7.
<i>min-threshold</i>	Minimum threshold in number of packets. Valid values are 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. Valid values are 1 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, 1 out of every 512 packets is dropped when the average queue is at the maximum threshold. Valid values are 1 to 65535. The default is 10; 1 out of every 10 packets is dropped at the maximum threshold.

Defaults

To return the values to the default for the discard class, use the **no** form of this command.

Command Modes

Policy-map class configuration

Command History

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

Usage Guidelines

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

Examples

The following example shows that if the discard class is 2, there is a 10 percent chance that packets will be dropped if there are more packets than the minimum threshold of 100 packets or there are fewer packets than the maximum threshold of 200 packets:

```
policy-map set-MPLS-PHB
class IP-AF11
  bandwidth percent 40
  random-detect discard-class-based
  random-detect-discard-class 2 100 200 10
```

Related Commands	Command	Description
	bandwidth (policy-map class)	Specifies or modifies the bandwidth allocated for a class belonging to a policy map.
	fair-queue (class-default)	Specifies the number of dynamic queues to be reserved for use by the class-default class as part of the default class policy.
	random-detect discard-class-based	Bases WRED on the discard class value of a packet.
	show policy-map interface	Displays the configuration of all classes configured for all service policies on the specified interface or displays the classes for the service policy for a specific PVC on the interface.

random-detect discard-class-based

To base weighted random early detection (WRED) on the discard class value of a packet, use the **random-detect discard-class-based** command in policy-map class configuration mode. To disable this feature, use the **no** form of this command.

random-detect discard-class-based

no random-detect discard-class-based

Syntax Description This command has no arguments or keywords.

Defaults The defaults are router-dependent.

Command Modes Policy-map class configuration

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

Usage Guidelines Enter this command so that WRED is based on the discard class instead of on the IP precedence field.

Examples The following example shows that random detect is based on the discard class value of a packet:

```
policy-map name
  class-name
    bandwidth percent 40
    random-detect discard-class-based
```

Related Commands	Command	Description
	match discard-class	Matches packets of a certain discard class.

random-detect dscp

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

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

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

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

Defaults If WRED is using the DSCP value to calculate the drop probability of a packet, all entries of the DSCP table are initialized with the default settings shown in [Table 13](#) in the “Usage Guidelines” section of this command.

Command Modes Interface configuration

Command History	Release	Modification
	12.1(5)T	This command was introduced.

Usage Guidelines The **random-detect dscp** command allows you to specify the DSCP value. The DSCP value can be a number from 0 to 63, or it can be one of the following keywords: **ef**, **af11**, **af12**, **af13**, **af21**, **af22**, **af23**, **af31**, **af32**, **af33**, **af41**, **af42**, **af43**, **cs1**, **cs2**, **cs3**, **cs4**, **cs5**, or **cs7**.

This command must be used in conjunction with the **random-detect** (interface) command.

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

Table 13 lists the default settings used by the **random-detect dscp** command for the DSCP value specified. Table 13 lists the DSCP value, and its corresponding minimum threshold, maximum threshold, and mark probability. The last row of the table (the row labeled “default”) shows the default settings used for any DSCP value not specifically shown in the table.

Table 13 *random-detect dscp Default Settings*

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

Examples

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

```
random-detect dscp af22 20 40 10
```

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

random-detect (interface)

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

random-detect [*dscp-based* | *prec-based*]

no random-detect [*dscp-based* | *prec-based*]

Syntax Description

<i>dscp-based</i>	(Optional) Specifies that WRED is to use the differentiated services code point (DSCP) value when it calculates the drop probability for a packet.
<i>prec-based</i>	(Optional) Specifies that WRED is to use the IP Precedence value when it calculates the drop probability for a packet.

Defaults

WRED and DWRED are disabled by default.

If you choose not to use either the *dscp-based* or the *prec-based* argument, WRED uses the IP Precedence value (the default method) to calculate drop probability for the packet.

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.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T. Arguments were added to support Differentiated Services (DiffServ) and Assured Forwarding (AF) Per Hop Behavior (PHB).

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 supported only 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.

Two Methods for Calculating the Drop Probability of a Packet

This command includes two optional arguments, *dscp-based* and *prec-based*, that determine the method WRED uses to calculate the drop probability of a packet.

Note the following points when deciding which method to instruct WRED to use:

- With the *dscp-based* argument, WRED uses the DSCP value (that is, the first six bits of the IP type of service (ToS) byte) to calculate the drop probability.
- With the *prec-based* argument, WRED will use the IP Precedence value to calculate the drop probability.
- The *dscp-based* and *prec-based* arguments are mutually exclusive.
- If neither argument is specified, WRED uses the IP Precedence value to calculate the drop probability (the default method).

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 fastethernet0/1
```

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

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

The following example enables WRED to use the DSCP value 8. The minimum threshold for the DSCP value 8 is 24 and the maximum threshold is 40. This configuration was performed at the interface level.

```
Router(config)# interface serial10/0
Router(config-if)# random-detect dscp-based
Router(config-if)# random-detect dscp 8 24 40
```

The following example enables WRED to use the DSCP value 8 for class c1. The minimum threshold for DSCP value 8 is 24 and the maximum threshold is 40. The last line attaches the service policy to the output interface or virtual circuit (VC) p1.

```
Router(config-if)# class-map c1
Router(config-cmap)# match access-group 101
Router(config-if)# policy-map p1
Router(config-pmap)# class c1
Router(config-pmap-c)# bandwidth 48
Router(config-pmap-c)# random-detect dscp-based
Router(config-pmap-c)# random-detect dscp 8 24 40
Router(config-if)# service-policy output p1
```

Related Commands

Command	Description
random-detect dscp	Changes the minimum and maximum packet thresholds for the DSCP value.
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 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.

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** command in VC submode mode. 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 or 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 or DWRED configuration will override the interface-level configuration if WRED or 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.

Note the following points when using the **random-detect** (per VC) command:

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

When this command is used to configure an interface-level WRED or DWRED group to include per-VC WRED or DWRED as a drop policy, the configured WRED or 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 or 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 or DWRED group configuration is removed, per-VC WRED or DWRED parameters are removed from any VC that inherited them from the configured interface-level WRED or DWRED group.

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

This command is only supported on interfaces that are capable of VC-level queueing. 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 ecn

To enable explicit congestion notification (ECN), use the **random-detect ecn** command in policy-map class configuration mode. To disable ECN, use the **no** form of this command.

random-detect ecn

no random-detect ecn

Syntax Description This command has no arguments or keywords.

Defaults By default, ECN is disabled.

Command Modes Policy-map class configuration

Command History	Release	Modification
	12.2(8)T	This command was introduced.

Usage Guidelines If ECN is enabled, ECN can be used whether Weighted Random Early Detection (WRED) is based on the IP precedence value or the differentiated services code point (DSCP) value.

Examples The following example enables ECN in a policy map called “poll”:

```
Router(config)# policy-map poll
Router(config-pmap)# class class-default
Router(config-pmap)# bandwidth per 70
Router(config-pmap-c)# random-detect
Router(config-pmap-c)# random-detect ecn
```

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

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 for the queue, use the **random-detect exponential-weighting-constant** command in interface configuration mode. 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** command in policy-map class configuration mode. 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, or when used in the Modular Quality of Service Command-Line Interface (MQC)

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.
12.0(5)XE	This command was integrated into Cisco IOS Release 12.0(5)XE and implemented on VIP-enabled Cisco 7500 series routers.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T and implemented on VIP-enabled Cisco 7500 series routers.

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 or 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 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 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
```

The following example configures policy for a traffic class named int10 to configure the exponential weight factor as 12. This is the weight factor used for the average queue size calculation for the queue for traffic class int10. WRED packet drop is used for congestion avoidance for traffic class int10, not tail drop.

```
policy-map policy12
  class int10
    bandwidth 2000
    random-detect exponential-weighting-constant 12
```

Related Commands	Command	Description
	bandwidth (policy-map class)	Specifies or modifies the bandwidth allocated for a class belonging to a policy map.
	exponential-weighting-constant	Configures the exponential weight factor for the average queue size calculation for a WRED parameter group.
	fair-queue (class-default)	Specifies the number of dynamic queues to be reserved for use by the class-default class as part of the default class policy.
	precedence	Configures precedence levels for a VC or PVC class that can be assigned to a VC or PVC bundle and thus applied to all of the members of that bundle.
	precedence (WRED group)	Configures a WRED group for a particular IP Precedence.
	random-detect dscp	Changes the minimum and maximum packet thresholds for the DSCP value.
	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 for a specified service policy map or all classes for all existing policy maps.
	show policy-map interface	Displays the configuration of all classes configured for all service policies on the specified interface or displays the classes for the service policy for a specific PVC on the interface.
	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** command in interface configuration mode. 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

Command History

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 serial interface 1:

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

Related Commands	Command	Description
	random-detect dscp	Changes the minimum and maximum packet thresholds for the DSCP value.
	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** command in interface configuration mode. 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

scaling-factor The scaling factor can be a number from 1 to 16.

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:

average-flow-depth * (scaling factor) < 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 serial interface 1 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 dscp	Changes the minimum and maximum packet thresholds for the DSCP value.
	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** command in interface configuration mode. 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 serial interface 1 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 dscp	Changes the minimum and maximum packet thresholds for the DSCP value.
	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.
	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 distributed WRED (DWRED) parameter group, use the **random-detect group** command in global configuration mode. To delete the WRED or DWRED parameter group, use the **no** form of this command.

random-detect-group *group-name* [**dscp-based** | **prec-based**]

no random-detect-group *group-name* [**dscp-based** | **prec-based**]

Syntax Description

<i>group-name</i>	Name for the WRED or DWRED parameter group.
dscp-based	(Optional) Specifies that WRED is to use the differentiated services code point (DSCP) value when it calculates the drop probability for a packet.
prec-based	(Optional) Specifies that WRED is to use the IP Precedence value when it calculates the drop probability for a packet.

Defaults

No WRED or DWRED parameter group exists.

If you choose not to use either the **dscp-based** or the **prec-based** keywords, WRED uses the IP Precedence value (the default method) to calculate drop probability for the packet.

Command Modes

Global configuration

Command History

Release	Modification
11.1(22)CC	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T. Keywords dscp-based and prec-based were added to support Differentiated Services (DiffServ) and Assured Forwarding (AF) Per Hop Behavior (PHB).

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.

Two Methods for Calculating the Drop Probability of a Packet

This command includes two optional arguments, **dscp-based** and **prec-based**, that determine the method WRED uses to calculate the drop probability of a packet.

Note the following points when deciding which method to instruct WRED to use:

- With the **dscp-based** keyword, WRED uses the DSCP value (that is, the first six bits of the IP type of service (ToS) byte) to calculate the drop probability.
- With the **prec-based** keyword, WRED will use the IP Precedence value to calculate the drop probability.
- The **dscp-based** and **prec-based** keywords are mutually exclusive.
- If neither argument is specified, WRED uses the IP Precedence value to calculate the drop probability (the default method).

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
```

The following example enables WRED to use the DSCP value 9. The minimum threshold for the DSCP value 9 is 20 and the maximum threshold is 50. This configuration can be attached to other virtual circuits (VCs) as required.

```
Router(config)# random-detect-group sanjose dscp-based
Router(cfg-red-grp)# dscp 9 20 50
Router(config-subif-vc)# random-detect attach sanjose
```

Related Commands

Command	Description
dscp	Changes the minimum and maximum packet thresholds for the DSCP value.
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-group	Defines the WRED or DWRED parameter group.
show queueing	Lists all or selected configured queueing strategies.
show queueing interface	Displays the queueing statistics of an interface or VC.

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** command in interface configuration mode. To configure WRED parameters for a particular IP Precedence for a class policy in a policy map, use the **random-detect precedence** command in policy-map class configuration mode. To return the values to the default for the precedence, use the **no** form of this command.

random-detect precedence {*precedence* | **rsvp**} *min-threshold max-threshold*
mark-prob-denominator

no random-detect precedence {*precedence* | **rsvp**} *min-threshold max-threshold*
mark-prob-denominator

Syntax Description

<i>precedence</i>	IP Precedence number. The value range is from 0 to 7. 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 from 0 to 7 only; see Table 14 in the “Usage Guidelines” section of this command.
rsvp	Indicates Resource Reservation Protocol (RSVP) traffic.
<i>min-threshold</i>	Minimum threshold in number of packets. The value range of this argument is from 1 to 4096. When the average queue length reaches the minimum threshold, 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 from 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 minimum threshold. For example, if the denominator is 512, 1 out of every 512 packets is dropped when the average queue is at the minimum threshold. The value range is from 1 to 65536. The default is 10; 1 out of every 10 packets is dropped at the minimum 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. See [Table 14](#) in the “Usage Guidelines” section of this command for a list of the default minimum threshold values for each IP Precedence.

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 or 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.

Table 14 lists the default minimum threshold value for each IP Precedence.

Table 14 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
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	—

**Note**

The default WRED or 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 supported only 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 a 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.
	fair-queue (class-default)	Specifies the number of dynamic queues to be reserved for use by the class-default class as part of the default class policy.
	random-detect dscp	Changes the minimum and maximum packet thresholds for the DSCP value.
	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.
	random-detect flow count	Sets the flow count for flow-based WRED.
	show policy-map interface	Displays the configuration of all classes configured for all service policies on the specified interface or displays the classes for the service policy for a specific PVC on the interface.
	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 committed access rate (DCAR) policies, use the **rate-limit** command in interface configuration mode. To remove the rate limit from the configuration, use the **no** form of this command.

```
rate-limit {input | output} {bps | access-group acl-index | [rate-limit] rate-limit-acl-index} |
dscp dscp-value | qos-group qos-group-number} burst-normal burst-max conform-action
conform-action exceed-action exceed-action
```

```
no rate-limit {input | output} {bps | access-group acl-index | [rate-limit] rate-limit-acl-index} |
dscp dscp-value | qos-group qos-group-number} burst-normal burst-max conform-action
conform-action exceed-action exceed-action
```

Syntax Description

input	Applies this CAR traffic policy to packets received on this input interface.
output	Applies this CAR traffic policy to packets sent on this output interface.
<i>bps</i>	Average rate, in bits per second (bps). The value must be in increments of 8 kbps. The value is a number from 8000 to 2000000000.
access-group	(Optional) Applies this CAR traffic policy to the specified access list.
<i>acl-index</i>	(Optional) Access list number. Values are numbers from 1 to 2699.
rate-limit	(Optional) The access list is a rate-limit access list.
<i>rate-limit-acl-index</i>	(Optional) Rate-limit access list number. Values are numbers from 0 to 99.
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 numbers from 0 to 63.
qos-group	(Optional) Allows the rate limit to be applied to any packet matching a specified qos-group number. Values are numbers from 0 to 99.
<i>qos-group-number</i>	(Optional) The qos-group number. Values are numbers from 0 to 99.
<i>burst-normal</i>	Normal burst size, in bytes. The minimum value is bps divided by 2000. The value is a number from 1000 to 512000,000.
<i>burst-max</i>	Excess burst size, in bytes. The value is a number from 2000 to 1024000000.

conform-action <i>conform-action</i>	<p>Action to take on packets that conform to the specified rate limit. Specify one of the following keywords:</p> <ul style="list-style-type: none"> • continue—Evaluate the next rate-limit command. • drop—Drop the packet. • set-dscp-continue—Set the differentiated services codepoint (DSCP) (0 to 63) and evaluate the next rate-limit command. • set-dscp-transmit—Transmit the DSCP and transmit the packet. • set-mpls-exp-imposition-continue—Set the Multiprotocol Label Switching (MPLS) experimental bits (0 to 7) during imposition and evaluate the next rate-limit command. • set-mpls-exp-imposition-transmit—Set the MPLS experimental bits (0 to 7) during imposition and transmit the packet. • set-prec-continue—Set the IP precedence (0 to 7) and evaluate the next rate-limit command. • set-prec-transmit—Set the IP precedence (0 to 7) and transmit the packet. • set-qos-continue—Set the quality of service (QoS) group ID (1 to 99) and evaluate the next rate-limit command. • set-qos-transmit—Set the QoS group ID (1 to 99) and transmit the packet. • transmit—Transmit the packet.
exceed-action <i>exceed-action</i>	<p>Action to take on packets that exceed the specified rate limit. Specify one of the following keywords:</p> <ul style="list-style-type: none"> • continue—Evaluate the next rate-limit command. • drop—Drop the packet. • set-dscp-continue—Set the DSCP (0 to 63) and evaluate the next rate-limit command. • set-dscp-transmit—Transmit the DSCP and transmit the packet. • set-mpls-exp-imposition-continue—Set the MPLS experimental bits (0 to 7) during imposition and evaluate the next rate-limit command. • set-mpls-exp-imposition-transmit—Set the MPLS experimental bits (0 to 7) during imposition and transmit the packet. • set-prec-continue—Set the IP precedence (0 to 7) and evaluate the next rate-limit command. • set-prec-transmit—Set the IP precedence (0 to 7) and transmit the packet. • set-qos-continue—Set the QoS group ID (1 to 99) and evaluate the next rate-limit command. • set-qos-transmit—Set the QoS group ID (1 to 99) and transmit the packet. • transmit—Transmit the packet.

Defaults CAR and DCAR are disabled.

Command Modes Interface configuration

Command History	Release	Modification
	11.1 CC	This command was introduced.
	12.1(5)T	The conform and exceed keywords for the MPLS experimental field were added.
	12.2(4)T	This command was implemented on the Cisco MGX 8850 switch and the MGX 8950 switch with a Cisco MGX RPM-PR card.
	12.2(4)T2	This command was implemented on the Cisco 7500 series.

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

CAR and DCAR can be configured on an interface or subinterface.

Policing Traffic with CAR

CAR embodies a rate-limiting feature for policing traffic. When policing traffic with CAR, Cisco recommends the following values for the normal and extended burst parameters:

normal burst = configured rate * (1 byte)/(8 bits) * 1.5 seconds

extended burst = 2 * normal burst

With the listed choices for parameters, extensive test results have shown CAR to achieve the configured rate. If the burst values are too low, then the achieved rate is often much lower than the configured rate.

For more information about using CAR to police traffic, see the “Policing with CAR” section of the “Policing and Shaping Overview” in the *Cisco IOS Quality of Service Configuration Guide*.

Examples In the following example, the rate is limited by the application in question:

- All World Wide Web traffic is transmitted. However, the MPLS experimental field 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). See the following commands in the example:

```
rate-limit input rate-limit access-group 101 20000000 24000 32000 conform-action
set-mpls-exp-transmit 5 exceed-action set-mpls-exp-transmit 0
access-list 101 permit tcp any any eq www
```

- FTP traffic is transmitted with an MPLS experimental field value of 5 if it conforms to the second rate policy. If the FTP traffic exceeds the rate policy, it is dropped. See the following commands in the example:

```
rate-limit input access-group 102 10000000 24000 32000
conform-action set-mpls-exp-transmit 5 exceed-action drop
access-list 102 permit tcp any any eq ftp
```

- 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 MPLS experimental field value of 5. Traffic that does not conform is dropped. See the following command in the example:

```
rate-limit input 8000000 16000 24000 conform-action set-mpls-exp-transmit 5
exceed-action drop
```

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 rate-limit access-group 101 20000000 24000 32000
conform-action set-mpls-exp-transmit 5 exceed-action set-mpls-exp-transmit 0
Router(config-if)# rate-limit input access-group 102 10000000 24000 32000
conform-action set-mpls-exp-transmit 5 exceed-action drop
Router(config-if)# rate-limit input 8000000 16000 24000 conform-action
set-mpls-exp-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
```

In the following example, the MPLS experimental field is set, and the packet is transmitted:

```
Router(config)# interface FastEthernet1/1/0
Router(config-if)# rate-limit input 8000 1000 1000 access-group conform-action
set mpls-exp-transmit 5 exceed-action set-mpls-exp-transmit 5
```

In the following example, any packet with a DSCP of 1 can apply the rate limit:

```
Router(config)# interface serial6/1/0
Router(config-if)# rate-limit output dscp 1 8000 1000 1000 conform-action transmit
exceed-action drop
```

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 a specified interface.