qos police order parent-first

To change the Quality of Service (QoS) policing action from child first, then parent (the default) to parent first, then child, use the **qos police order parent-first** command in global configuration mode. To disable the parent-first order and restore the default behavior, use the **no** form of this command.

qos police order parent-first

no qos police order parent-first

Syntax Description

This command has no arguments or keywords.

Command Default

If the **qos police order parent-first** command is not entered, the child policing action is done first, followed by the parent policing action.

Command Modes

Global configuration (#)

Command History

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

Usage Guidelines

Prior to Cisco IOS Release 15.1(1)S, in a hierarchical policing policy map (a parent policy with policing configured under a class that has a child policy also with policing configured), the parent policing action was done first, followed by the child policing action.

Beginning in Cisco IOS Release 15.1(1)S, the order is reversed. By default, the child policing action is done first, followed by the parent policing action. This change applies only to software dataplane policer implementations (Cisco 7200, Cisco 7301, and Cisco 7600 FlexWAN and SIP200 line cards).

This new behavior improves the results for transmit-and-drop actions because the child policing action occurs first. However, if the parent and child policers are performing conflicting mark-and-transmit actions, the parent mark takes effect rather than the child because the parent action happens last.

Use of the **qos police order parent-first** command is necessary only if you need to revert to the police order that was in effect prior to Release 15.1(1)S.

Examples

The following example shows how to change the police order from child first (default) to parent first, then child:

```
Router# qos police order parent-first
```

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.

Command Default

QoS preclassification is disabled.

Command Modes

Interface configuration (config-if)

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.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.1	This command was implemented on Cisco ASR 1000 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.

You can enable the **qos pre-classify** command for IP packets only.

Note QoS preclassification is not supported for all fragmented packets. If a packet is fragmented, each fragment might receive different preclassifications.

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
```

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-depth

To configure the number of incoming packets that the Open Shortest Path First (OSPF) process can keep in its queue, use the **queue-depth** command in router configuration mode. To set the queue depth to its default value, use the **no** form of the command.

queue-depth {**hello** | **update**} {*queue-size* | **unlimited**}

no queue-depth {**hello** | **update**}

Syntax Description

hello	Specifies the queue depth of the OSPF hello process.
update	Specifies the queue depth of the OSPF router process queue.
queue-size	Maximum number of packets in the queue. The range is 1 to 2147483647.
unlimited	Specifies an infinite queue depth.

Command Default

If you do not set a queue size, the OSPF hello process queue depth is unlimited and the OSPF router process (update) queue depth is 200 packets.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
12.2(25)S	This command was introduced.

Usage Guidelines

All incoming OSPF packets are initially enqueued in the hello queue. OSPF hello packets are processed directly from this queue, while all other OSPF packet types are subsequently enqueued in the update queue.

If you configure a router with many neighbors and a large database, use the **queue-depth** command to adjust the size of the hello and router queues. Otherwise, packets might be dropped because of queue limits, and OSPF adjacencies may be lost.

Examples

The following example shows how to configure the OSPF update queue to 1500 packets:

```
Router> enable
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# router ospf 1
Router(config-router)# queue-depth update 1500
```

Related Commands

Command	Description
queue-limit	Specifies or modifies the queue limit (size) for a class in bytes, milliseconds (ms), or packets.
queue-list queue limit	Designates the queue length limit for a queue.

queue-limit

To specify or modify the queue limit (size) for a class in bytes, milliseconds (ms), or packets, use the **queue-limit** command in QoS policy-map class configuration mode. To remove the queue limit from a class, use the **no** form of this command.

queue-limit *queue-limit-size* [**bytes** | **ms** | **packets**]

no queue-limit

Cisco 7600 Series Routers

queue-limit *queue-limit-size* [**packets**]

no queue-limit

Cisco ASR 1000 Series Router

queue-limit *queue-limit-size* [**bytes** | **packets**]

no queue-limit

Syntax Description

queue-limit-size	The maximum size of the queue. The maximum varies according to the optional unit of measure keyword specified (**bytes**, **ms**, or **packets**). **Note** If an optional unit of measure is not indicated, the default unit of measure is packets. **Note** For Cisco ASR 1000 Aggregation Services Routers, bytes is the preferred mode.
bytes	(Optional) Indicates that the unit of measure is bytes. Valid range for bytes is a number from 1 to 8192000. **Note** The **bytes** keyword is not supported on Cisco 7600 series routers. **Note** For Cisco ASR 1000 Series Routers, the valid range for bytes is a number from 1 to 64000000.
ms	(Optional) Indicates that the unit of measure is milliseconds. Valid range for milliseconds is a number from 1 to 3400. **Note** The **ms** keyword is not supported on Cisco 7600 and ASR 1000 series routers.

packets	(Optional) Indicates that the unit of measure is packets. Valid range for packets is a number from 1 to 32768 but can also vary by platform and release as follows: • For ESR-PRE1—The queue size limit for packets is a number from 32 to 16384; the number must be a power of 2. If the number that you specify is not a power of 2, the router converts the number to the nearest power of 2. • For Cisco IOS Release 12.2(15)BX, 12.2(16)BX, and later releases—The queue size limit for packets is a number from 32 to 16384. The number does not need to be a power of 2. • For Cisco IOS Release 12.3(7)XI and later releases—If the interface has less than 500 MB of memory, the queue size limit for packets is a number from 8 to 4096; the number must be a power of 2. If the interface has more than 500 MB of memory, the *queue-limit-size* for packets is a number from 128 to 64000 and must be a power of 2; if it is not, the router converts the number to the nearest power of 2. • For Cisco IOS Release 12.2(31)SB2 and later releases—The queue size limit for packets is a number from 16 to 32767. • For Cisco IOS XE Release 2.1 and later releases—The queue size limit for packets is a number from 1 to 8192000.

Command Default

The default behavior of the **queue-limit** command for class queues with and without Weighted Random Early Detection (WRED) is as follows:

- Class queues with WRED—The router uses the default queue limit of two times the largest WRED maximum threshold value, rounded to the nearest power of 2.

  Note For Cisco IOS Release 12.2(16)BX, the router does not round the value to the nearest power of 2.

- Priority queues and class queues without WRED—The router has buffers for up to 50 ms of 256-byte packets at line rate, but not fewer than 32 packets.

Command Modes

QoS policy-map class configuration (config-pmap-c)

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.
12.0(17)SL	This command was implemented on the Cisco 10000 series router.
12.1(5)T	This command was implemented on the VIP-enabled Cisco 7500 series routers.
12.2(16)BX	This command was introduced on the ESR-PRE2.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Release	Modification
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.3(7)XI	This command was integrated into Cisco IOS Release 12.3(7)XI.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(20)T	The following argument and keyword combinations were added: • *queue-limit-size* **bytes** • *queue-limit-size* **ms** • *queue-limit-size* **packets** **Note** The **bytes** keyword is not supported on Cisco 7600 series routers and **ms** keyword is not supported on Cisco 7600 and ASR 1000 Series Routers.
Cisco IOS XE Release 2.1	This command was implemented on Cisco ASR 1000 Series Routers.
15.0(1)S1	This command was modified to improve qlimit and min/max threshold calculation.
15.0(1)M5	This command was modified to improve Hierarchical Queueing Framework (HQF) capability.

Usage Guidelines

Weighted Fair Queueing

Weighted fair queueing (WFQ) creates a queue for every class for which a class map is defined. Packets that satisfy the match criterion 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 that you defined for the class is reached, enqueueing of any further packets to the class queue causes tail drop or, if WRED is configured for the class policy, packet drop to take effect.

Changes in Cisco IOS Release 15.0(1)S1

Prior to Cisco IOS Release 15.0(1)S1, if no queue limit was configured, the queue limit for the current class was based on the parent values for available buffers and current class allocated bandwidth. In the implicit WRED min/max scenario, thresholds were calculated from the available buffers.

Thresholds were calculated from the available aggregate queue limit for each class. The WRED min/max threshold values would not be adjusted if there was a user-defined queue-limit configuration. The min/max threshold would still be derived from the “visible_bw” value seen by this traffic class. The WRED functionality could fail because of this inconsistent qlimit and min/max threshold calculation.

Beginning in Cisco IOS Release 15.0(1)S1, the queue limit is always calculated from the parent queue limit and allocated bandwidth in the current class. When you use the **queue-limit** command to explicitly configure the values, these values are used as the definition of the queue limit.

To ensure optimum functionality, use the **queue-limit** command to configure the proper min/max threshold for each WRED class based on the queue-limit configuration.

Overriding Queue Limits Set by the bandwidth Command

Use the **bandwidth** command with the modular quality of service (QoS) CLI) (MQC) to specify the bandwidth for a particular class. When used with MQC, the **bandwidth** command has 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.

Prior to the deployment of the Hierarchical Queueing Framework (HQF), the default maximum queue limit on a subinterface was 512 if no hold queue was configured on the main interface.

As part of HQF, this restriction was removed beginning in Cisco IOS Release 15.0(1)M5. Now the maximum queue limit can be set as high as the hold-queue size on the main interface.

If no hold queue is configured on the main interface, the aggregate queue limit can go up to 1000. If the hold-queue is explicitly configured on the main interface, then the aggregate queue limit can go up to the hold-queue value. There is no limit per subinterface.

The maximum configurable hold-queue value of 4096 was increased to 240,000 for users who want to configure higher aggregate queue-limit values. However, configuring high queue-limit and hold-queue values is not recommended.

Examples

The following example configures a policy map called policy11. The policy11 policy map contains a class called acl203. The policy map for this class is configured so that the queue reserved for the class has a maximum queue size of 40 packets.

```
Router(config)# policy-map policy11
Router(config-pmap)# class acl203
Router(config-pmap-c)# bandwidth 2000
Router(config-pmap-c)# queue-limit 40 packets
```

Related Commands

Command	Description
bandwidth	Specifies the maximum aggregate bandwidth for H.323 traffic and verifies the available bandwidth of the destination gatekeeper.
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-limit atm clp

To specify the maximum size (in cells, microseconds, or milliseconds) of a queue for a specific traffic class, use the **queue-limit atm clp** command in policy-map class configuration mode. To remove the queue limit atm cell loss priority (clp) value from a class, use the **no** form of this command.

queue-limit atm clp *queue-size* {**cells** | **ms** | **us**}

no queue-limit atm clp

Syntax Description

queue-size	Threshold value. The range is 1 to 262144.
cells | **ms** | **us**	Unit of measure for the queue size; ms = milliseconds; us = microseconds.

Command Default

No default behavior or values

Command Modes

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

Command History

Release	Modification
12.0(30)S	This command was introduced.

Usage Guidelines

You can use the **queue-limit atm clp** command only with other queuing features, such as weighted fair queuing (WFQ). WFQ creates a queue for every class for which you define a class map. You can apply the policy map that you created with the atm clp based **queue-limit** command only to ATM interfaces on Cisco 12000 Series Routers.

Use the **queue-limit atm clp** command only after you have issued the **queue-limit** command using the same traffic class.

Use the **no queue-limit** command to remove both the global queue-limit queue-size value and the queue-limit atm clp queue-size value if you configured it.

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 weighted fair queuing process. When the defined maximum packet threshold for the class is reached, enqueuing of additional packets to the class queue causes tail drop.

You can specify the CLP queue-limit threshold in cells, milliseconds (ms), or microseconds (us). However, the unit of measure cannot be mixed. For example, if you specify the CLP queue-limit threshold in milliseconds, then you must also specify the global queue-limit threshold in milliseconds.

Note When you specify the queue-limit threshold as cells, milliseconds, or microseconds, it is internally converted to cells by using the visible bandwidth that is available to the class or the ATM virtual circuit (VC).

Examples

The following example shows how to create a policy map called POLICY-ATM that contains a class called CLASS-ATM. The bandwidth for this class is specified as a percentage (20), and the **queue-limit** command sets the global queue-limit threshold to 1000 cells. The **queue-limit atm clp** command sets the queue-limit threshold for ATM CLP data to 100 cells:

```
Router> enable
Router# configure terminal
Router(config)# policy-map POLICY_ATM
Router(config-pmap)# class CLASS-ATM
Router(config-pmap-c)# bandwidth percent 20
Router(config-pmap-c)# queue-limit 1000 cells
Router(config-pmap-c)# queue-limit atm clp 100 cells
Router(config-pmap-c)# exit
```

Related Commands

Command	Description
bandwidth (policy-map class)	Specifies or modifies the bandwidth allocated for a class belonging to a policy map.
class class-default	Specifies the default traffic class whose bandwidth is to be configured or modified.
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-limit	Specifies or modifies the maximum number of packets the queue can hold for a class configured in a policy map.

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

list-number	Number of the queue list. Any number from 1 to 16 that identifies the queue list.
queue-number	Number of the queue. Any number from 1 to 16.

Command Default

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

Usage Guidelines

When 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

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

Command Default

No queueing priorities are established.

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

list-number	Number of the queue list. Any number from 1 to 16 that identifies the queue list.
queue-number	Number of the queue. Any number from 1 to 16.

Command Default

The default number of the lowest custom queue is 1.

Command Modes

Global configuration

Command History

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

Usage Guidelines

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.

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 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

list-number	Number of the queue list. Any number from 1 to 16.
protocol-name	Protocol type: **aarp**, **appletalk**, **arp**, **bridge** (transparent), **clns**, **clns_es**, **clns_is**, **cmns**, **compressedtcp**, **decnet**, **decnet_node**, **decnet_routerl1**, **decnet_routerl2**, **dlsw**, **ip**, **ipx**, **pad**, **rsrb**, **stun** and **x25**.
queue-number	Number of the queue. Any number from 1 to 16.
queue-keyword keyword-value	Possible keywords are **fragments, gt, list, lt, tcp**, and **udp**. See the **priority-list protocol** command for more information about this keyword.

Command Default

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

Usage Guidelines

When 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-l1** keyword refers to the multicast address for all level 1 routers, which are intra-area routers, and the **decnet_router-l2** keyword refers to all level 2 routers, which are interarea routers.

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

Use the tables listed in the **priority-list protocol** command documention 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

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

Command Default

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

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.

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.

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

list-number	Number of the queue list. Any number from 1 to 16.
queue-number	Number of the queue. Any number from 1 to 16.
limit-number	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.

Command Default

The default queue length limit is 20 entries.

Command Modes

Global configuration

Command History

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

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

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

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

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

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

no random-detect

Syntax Description

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.

Command Default

WRED and DWRED are disabled by default.

Command Modes

Interface configuration when used on an interface (config-if)
Policy-map class configuration when used in a policy map (config-pmap-c)

Command History

Release	Modification
11.1CC	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).
12.1(5a)E	This command was integrated into Cisco IOS Release 12.1(5a)E in policy map class configuration mode only. This command was implemented on Versatile Interface Processor (VIP)-enabled Cisco 7500 series routers and Catalyst 6000 family switches with a FlexWAN module.
12.0(15)S	This command was integrated into Cisco IOS Release 12.0(15)S in policy-map class configuration mode only.

Release	Modification
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.0(28)S	This command was integrated into Cisco IOS Release 12.0(28)S in policy map class configuration mode.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB in policy map class configuration mode.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(20)T	Support was added for hierarchical queueing framework (HQF) using the Modular Quality of Service (QoS) Command-Line Interface (CLI) (MQC).
15.0(1)S	This command was modified. This command was hidden in interface configuration mode.
15.1(3)T	This command was modified. This command was hidden in interface configuration mode.

Usage Guidelines

Keywords

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 the drop probability for the packet.

Availability

The **random-detect** command is not available at the interface level for Cisco IOS Releases 12.1E or 12.0S. The **random-detect** command is available in policy-map class configuration mode only for Cisco IOS Releases 12.1E, 12.0S, and later.

WRED Functionality

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 Transport Control Protocol (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.

Platform Support for DWRED

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 map 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. 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, tail drop is used.

To configure a policy map and create class policies, use the **policy-map** and **class** (policy-map) commands. When creating a class 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 If you use WRED packet drop instead of tail drop for one or more classes in a policy map, you must ensure that WRED is not configured on the interface to which you attach that policy map.

Note DWRED is not supported for classes in a policy map.

Two Methods for Calculating the Drop Probability of a Packet

This command includes two optional keywords, **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 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 serial0/0
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-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface serial0/0
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)

Note Effective with Cisco IOS Release 15.1(3)T, the **random-detect** (per VC) command is hidden. Although this command is still available in Cisco IOS software, the CLI interactive Help does not display it if you attempt to view it by entering a question mark at the command line.

This command will be completely removed in a future release. For more information, see the *Legacy QoS Command Deprecation* feature document in the *Cisco IOS Quality of Service Solutions Configuration Guide*.

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) Name of the WRED or DWRED group.

Command Default

WRED and DWRED are disabled by default.

Command Modes

VC submode

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)T	This command was modified. This command was hidden.

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 aggregate

To enable aggregate Weighted Random Early Detection (WRED), use the **random-detect aggregate** command in policy-map class configuration mode. To disable aggregate WRED, use the **no** form of this command.

random-detect [**precedence-based | dscp-based**] **aggregate** [**minimum-thresh** *min-thresh* **maximum-thresh** *max-thresh* **mark-probability** *mark-prob*]

no random-detect [**precedence-based | dscp-based**] **aggregate**

Syntax Description

precedence-based	(Optional) Enables aggregate WRED based on IP precedence values. This is the default.
dscp-based	(Optional) Enables aggregate WRED based on differentiated services code point (DSCP) values.
minimum-thresh *min-thresh*	(Optional) Default minimum threshold (in number of packets) to be used for all subclasses (IP precedence or DSCP values) that have not been specifically configured. Valid values are from 1 to 12288.
maximum-thresh *max-thresh*	(Optional) Default maximum threshold (in number of packets) to be used for all subclasses (IP precedence or DSCP values) that have not been specifically configured. Valid values are from the minimum threshold argument to 12288.
mark-probability *mark-prob*	(Optional) Default denominator for the fraction of packets dropped when the average queue depth is at the maximum threshold. This value is used for all subclasses (IP precedence or DSCP values) that have not been specifically configured. Valid values are from 1 to 255.

Command Default

If no **precedence-based** or **dscp-based** keyword is specified in the command, the default is **precedence-based**.

If optional parameters for a default aggregate class are not defined, all subclass values that are not explicitly configured will use plain (non-weighted) RED drop behavior. This is different from standard random-detect configuration where the default is to always use WRED behavior.

Command Modes

Policy-map class configuration

Command History

Release	Modification
12.2(18)SXE	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2 on the Cisco 10000 series router for the PRE3.

Usage Guidelines

For ATM interfaces, the Aggregate WRED feature requires that the ATM SPA cards are installed in a Cisco 7600 SIP-200 carrier card or a Cisco 7600 SIP-400 carrier card.

To configure WRED on an ATM interface, you must use the random-detect aggregate commands; the standard random-detect commands are no longer supported on ATM interfaces.

The **precedence-based** and **dscp-based** keywords are mutually exclusive. If you do not specify either keyword, **precedence-based** is the default.

Defining WRED profile parameter values for the default aggregate class is optional. If defined, WRED profile parameters applied to the default aggregate class will be used for all subclasses that have not been explicitly configured. If all possible IP precedence or DSCP values are defined as subclasses, a default specification is unnecessary. If the optional parameters for a default aggregate class are not defined and packets with an unconfigured IP precedence or DSCP value arrive at the interface, plain (non-weighted) RED drop behavior will be used.

Use this command with a **random-detect precedence** (aggregate) or **random-detect dscp** (aggregate) command within a policy map configuration to configure aggregate Weighted Random Early Detection (WRED) parameters for specific IP precedence or DSCP value(s).

After the policy map is defined, the policy map must be attached at the VC level.

Use the **show policy-map interface** command to display the statistics for aggregated subclasses.

Examples

The following example shows a precedence-based aggregate WRED configuration for an ATM interface. Note that first a policy map named prec-aggr-wred is defined for the default class, then precedence-based Aggregate WRED is enabled with the **random-detect aggregate** command, then subclasses and WRED parameter values are assigned in a series of **random-detect precedence** (aggregate) commands, and, finally, the policy map is attached at the ATM VC level using the **interface** and **service-policy** commands.

```
Router(config)# policy-map prec-aggr-wred
Router(config-pmap)# class class-default
Router(config-pmap-c)# random-detect aggregate
Router(config-pmap-c)# random-detect precedence values 0 1 2 3 minimum thresh 10
maximum-thresh 100 mark-prob 10
Router(config-pmap-c)# random-detect precedence values 4 5 minimum-thresh 40
maximum-thresh 400 mark-prob 10
Router(config-pmap-c)# random-detect precedence values 6 minimum-thresh 60 maximum-thresh
600 mark-prob 10
Router(config-pmap-c)# random-detect precedence values 7 minimum-thresh 70 maximum-thresh
700 mark-prob 10
Router(config-pmap-c)# interface ATM4/1/0.10 point-to-point
Router(config-subif)# ip address 10.0.0.2 255.255.255.0
Router(config-subif)# pvc 10/110
Router(config-subif)# service-policy output prec-aggr-wred
```

The following example shows a DSCP-based aggregate WRED configuration for an ATM interface. Note that first a policy map named dscp-aggr-wred is defined for the default class, then dscp-based Aggregate WRED is enabled with the **random-detect dscp-based aggregate** command, then subclasses and WRED parameter values are assigned in a series of **random-detect dscp** (aggregate) commands, and, finally, the policy map is attached at the ATM VC level using the **interface** and **service-policy** commands.

```
Router(config)# policy-map dscp-aggr-wred
Router(config-pmap)# class class-default
Router(config-pmap-c)# random-detect dscp-based aggregate minimum-thresh 1 maximum-thresh
10 mark-prob 10
```

```
Router(config-pmap-c)# random-detect dscp values 0 1 2 3 4 5 6 7 minimum-thresh 10
maximum-thresh 20 mark-prob 10
Router(config-pmap-c)# random-detect dscp values 8 9 10 11 minimum-thresh 10
maximum-thresh 40 mark-prob 10
Router(config)# interface ATM4/1/0.11 point-to-point
Router(config-subif)# ip address 10.0.0.2 255.255.255.0
Router(config-subif)# pvc 11/101
Router(config-subif)# service-policy output dscp-aggr-wred
```

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.
interface	Configures an interface type and enters interface configuration mode.
policy-map	Creates a policy map that can be attached to one or more interfaces to specify a service policy.
random-detect precedence (aggregate)	Configures aggregate WRED parameters for specific IP precedence values.
random-detect dscp (aggregate)	Configures aggregate WRED parameters for specific DSCP values.
service-policy	Attaches a policy map to an input interface or VC, or an output interface or VC, to be used as the service policy for that interface or VC.
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 atm-clp-based

To enable weighted random early detection (WRED) on the basis of the ATM cell loss priority (CLP) of a packet, use the **random-detect atm-clp-based** command in policy-map class configuration mode. To disable WRED, use the **no** form of this command.

random-detect atm-clp-based *clp-value*

no random-detect atm-clp-based

Cisco 10000 Series Router

random-detect atm-clp-based *min-thresh-value max-thresh-value mark-probability-denominator-value*

no random-detect atm-clp-based

Syntax Description

clp-value	CLP value. Valid values are 0 or 1.
min-thresh-value	Minimum threshold in number of packets. Valid values are 1 to 4096.
max-thresh-value	Maximum threshold in number of packets. Valid values are 1 to 4096.
max-probability-denominator-value	Denominator for the fraction of packets dropped when the average queue depth is at the maximum threshold. Valid values are 1 to 65535.

Command Default

When WRED is configured, the default minimum and maximum thresholds are determined on the basis of output buffering capacity and the transmission speed for the interface.

The default maximum probability denominator is 10.

On the Cisco 10000 series router, the default is disabled.

Command Modes

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

Command History

Release	Modification
12.0(28)S	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SB	This command was introduced on the PRE3 and PRE4 for the Cisco 10000 series router.
12.4(20)T	Support was added for hierarchical queueing framework (HQF) using the Modular Quality of Service (QoS) Command-Line Interface (CLI) (MQC).

Usage Guidelines

You cannot use the **random-detect atm-clp-based** command with the **random-detect cos-based** command in the same HQF configuration. You must use the **no random-detect cos-based** command to disable it before you configure the **random-detect atm-clp-based** command.

Examples

In the following example, WRED is configured on the basis of the ATM CLP. In this configuration, the **random-detect atm-clp-based** command has been configured and an ATM CLP of 1 has been specified.

```
Router> enable
Router# configure terminal
Router(config)# policy-map policymap1
Router(config-pmap)# class class1
Router(config-pmap-c)# random-detect atm-clp-based 1
Router(config-pmap-c)# end
```

Related Commands

Command	Description
random-detect clp	Specifies the ATM CLP value of a packet, the minimum and maximum thresholds, and the maximum probability denominator used for enabling WRED.
random-detect cos	Specifies the CoS value of a packet, the minimum and maximum thresholds, and the maximum probability denominator used for enabling WRED.
random-detect cos-based	Enables WRED on the basis of the CoS value of a packet.
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 cos-based

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

random-detect cos-based *cos-value*

no random-detect cos-based

Syntax Description

cos-value	Specific IEEE 802.1Q CoS values from 0 to 7.

Command Default

When WRED is configured, the default minimum and maximum thresholds are determined on the basis of output buffering capacity and the transmission speed for the interface.

The default maximum probability denominator is 10.

Command Modes

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

Command History

Release	Modification
12.0(28)S	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.4(20)T	Support was added for hierarchical queueing framework (HQF) using the Modular Quality of Service (QoS) Command-Line Interface (CLI) (MQC).

Usage Guidelines

You cannot use the **random-detect cos-based** command with the **random-detect atm-clp-based** command in the same HQF configuration. You must use the **no random-detect atm-clp-based** command to disable it before you configure the **random-detect cos-based** command.

Examples

In the following example, WRED is configured on the basis of the CoS value. In this configuration, the **random-detect cos-based** command has been configured and a CoS value of 2 has been specified.

```
Router> enable
Router# configure terminal
Router(config)# policy-map policymap1
Router(config-pmap)# class class1
Router(config-pmap-c)# random-detect cos-based 2
Router(config-pmap-c)# end
```

Related Commands

Command	Description
random-detect atm-clp-based	Enables WRED on the basis of the ATM CLP of a packet.
random-detect clp	Specifies the ATM CLP value of a packet, the minimum and maximum thresholds, and the maximum probability denominator used for enabling WRED.
random-detect cos	Specifies the CoS value of a packet, the minimum and maximum thresholds, and the maximum probability denominator used for enabling WRED.
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 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 QoS policy-map class configuration mode. To disable the discard-class values, use the **no** form of this command.

random-detect discard-class *value min-threshold max-threshold max-probability-denominator*

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

Syntax Description

value	Discard class. This is a number that identifies the drop eligibility of a packet. Valid values are 0 to 7.
min-threshold	Specifies the minimum number of packets allowed in the queue. When the average queue length reaches the minimum threshold, WRED randomly drops some packets with the specified DSCP, IP precedence, or discard-class value. Valid minimum threshold values are 1 to 16384.
max-threshold	Specifies the maximum number of packets allowed in the queue. When the average queue length exceeds the maximum threshold, WRED drops all packets with the specified DSCP, IP precedence, or discard-class value. Valid maximum threshold values are 1 to 16384.
max-probability-denominator	Denominator for the fraction of packets dropped when the average queue depth is at the maximum threshold. For example, if the denominator is 512, 1 out of every 512 packets is dropped when the average queue is at the maximum threshold. Valid values are 1 to 65535.

Command Default

For all precedence levels, the *max-probability-denominator* default is 10 packets; 1 out of every 10 packets is dropped at the maximum threshold.

Command Modes

QoS policy-map class configuration

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB and implemented on the Cisco 10000 series router.

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.

Cisco 10000 Series Router

You must first enable the drop mode using the **random-detect discard-class-based** command. You can then set the drop probability profile using the **random-detect discard-class** command.

Table 27 lists the default drop thresholds for WRED based on differentiated services code point (DSCP), IP precedence, and discard class. The drop probability indicates that the router drops one packet for every 10 packets.

Table 27 WRED Default Drop Thresholds

DSCP, Precedence, and Discard-Class Values	Minimum Threshold (Times the Queue Size)	Maximum Threshold (Times the Queue Size)	Drop Probability
All DSCPs	1/4	1/2	1/10
0	1/4	1/2	1/10
1	9/32	1/2	1/10
2	5/16	1/2	1/10
3	11/32	1/2	1/10
4	3/8	1/2	1/10
5	13/32	1/2	1/10
6	7/16	1/2	1/10
7	15/32	1/2	1/10

Examples

The following example shows how to configure discard class 2 to randomly drop packets when the average queue reaches the minimum threshold of 100 packets and 1 in 10 packets are dropped when the average queue is at 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
```

Cisco 10000 Series Router

The following example shows how to enable discard-class-based WRED. In this example, the configuration of the class map named Silver indicates to classify traffic based on discard class 3 and 5. Traffic that matches discard class 3 or 5 is assigned to the class named Silver in the policy map named Premium. The Silver configuration includes WRED packet dropping based on discard class 5 with a minimum threshold of 500, maximum threshold of 1500, and a mark-probability-denominator of 200. The QoS policy is applied to PVC 1/81 on point-to-point ATM subinterface 2/0/0.2 in the outbound direction.

```
Router(config)# class-map Silver
Router(config-cmap)# match discard-class 3 5
Router(config-cmap)# exit
Router(config)# policy-map Premium
Router(config-pmap)# class Silver
Router(config-pmap-c)# bandwidth percent 30
Router(config-pmap-c)# random-detect discard-class-based
Router(config-pmap-c)# random-detect discard-class 5 500 1500 200
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface atm 2/0/0
```

```
Router(config-if)# atm pxf queuing
Router(config-if)# interface atm 2/0/0.2 point-to-point
Router(config-subif)# pvc 1/81
Router(config-subif-atm-vc)# ubr 10000
Router(config-subif-atm-vc)# service-policy output Premium
```

Related Commands

Command	Description
bandwidth (policy-map class)	Specifies or modifies the bandwidth allocated for a class belonging to a policy map.
match discard-class	Matches packets of a certain discard-class.
random-detect discard-class-based	Bases WRED on the discard class value of a packet.
random-detect exponential-weighting-constant	Configures the WRED and DWRED exponential weight factor for the average queue size calculation.
random-detect precedence	Configures WRED and DWRED parameters for a particular IP precedence.
show 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.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

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

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

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

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

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

Syntax Description

dscp-value	The DSCP value. The DSCP value can be a number from 0 to 63, or it can be one of the following keywords: **af11**, **af12**, **af13**, **af21**, **af22**, **af23**, **af31**, **af32**, **af33**, **af41**, **af42**, **af43**, **cs1**, **cs2**, **cs3**, **cs4**, **cs5**, **cs7, ef**, or **rsvp**.
min-threshold	Minimum threshold in number of packets. The value range of this argument is from 1 to 4096. When the average queue length reaches the minimum threshold, Weighted Random Early Detection (WRED) or distributed WRED (dWRED) randomly drops some packets with the specified DSCP value.
max-threshold	Maximum threshold in number of packets. The value range of this argument is from the value of the *min-threshold* argument to 4096. When the average queue length exceeds the maximum threshold, WRED or dWRED drops all packets with the specified DSCP value.
max-probability-denominator	(Optional) Denominator for the fraction of packets dropped when the average queue depth is at the maximum threshold. For example, if the denominator is 512, 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.

Command Default

The default values for the **random-detect dscp** command are different on Versatile Interface Processor (VIP)-enabled Cisco 7500 series routers and Catalyst 6000 family switches with a FlexWAN module (dWRED). All other platforms running WRED have another set of default values. For more information about **random-detect dscp** defaults, see the "Usage Guidelines" section.

Command Modes

Interface configuration
Policy-map class configuration

Command History

Release	Modification
12.1(5)T	This command was introduced.
12.1(5a)E	This command was integrated into Cisco IOS Release 12.1(5a)E in policy-map class configuration mode only. The command was introduced for VIP-enabled Cisco 7500 series routers and Catalyst 6000 family switches with a FlexWAN module.
12.0(15)S	This command was integrated into Cisco IOS Release 12.0(15)S in policy-map class configuration mode only.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)T	This command was modified. This command was hidden in interface configuration mode.

Usage Guidelines

Use the **random-detect dscp** command in conjunction with the **random-detect** command in interface configuration mode.

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

Note The **random-detect dscp** command is not available at the interface level for Cisco IOS Release 12.1E or Release 12.0S. The **random-detect dscp** command is available only in policy-map class configuration mode in Cisco IOS Release 12.1E.

Defaults for VIP-Enabled Cisco 7500 Series Routers and Catalyst 6000 Family Switches with a FlexWAN Module

For all IP precedence values, the default *mark-probability-denominator* is 10, and the *max-threshold* value is based on the output buffering capacity and the transmission speed of the interface.

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

Unless the maximum and minimum threshold values for the DSCP values are configured by the user, all DSCP values have the same minimum threshold and maximum threshold values as the value specified for precedence 0.

Specifying the DSCP Value

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

On a particular traffic class, eight DSCP values can be configured per traffic class. Overall, 29 values can be configured on a traffic class: 8 precedence values, 12 AF code points, 1 EF code point, and 8 user-defined DSCP values.

Assured Forwarding Code Points

The AF code points provide a means for a domain to offer four different levels (four different AF classes). Forwarding assurances for IP packets received from other (such as customer) domains. Each one of the four AF classes is allocated a certain amount of forwarding services (buffer space and bandwidth).

Within each AF class, IP packets are marked with one of three possible drop precedence values (binary 2{010}, 4{100}, or 6{110}), which exist as the three lowest bits in the DSCP header. In congested network environments, the drop precedence value of the packet determines the importance of the packet within the AF class. Packets with higher drop precedence values are discarded before packets with lower drop precedence values.

The upper three bits of the DSCP value determine the AF class; the lower three values determine the drop probability.

Expedited Forwarding Code Points

The EF code point is usually used to mark high-priority, time-sensitive data. The EF code point marking is equal to the highest precedence value; therefore, the EF code point is always equal to precedence value 7.

Class Selector Values

The Class Selector (CS) values are equal to IP precedence values (for instance, cs1 is the same as IP precedence 1).

Default Values

Table 28 lists the default WRED minimum threshold value for each IP precedence value on the distributed platforms.

Table 28 Default WRED Minimum Threshold Values for the Distributed Platforms

IP (Precedence)	Class Selector (CS) Value	Minimum Threshold Value (Fraction of Maximum Threshold Value)	Important Notes About the Value
0	cs0	8/16	All DSCP values that are not configured by the user will have the same threshold values as IP precedence 0.
1	cs1	9/16	—
2	cs2	10/16	—
3	cs3	11/16	—
4	cs4	12/16	—
5	cs5	13/16	—
6	cs6	14/16	—
7	cs7	15/16	The EF code point will always be equal to IP precedence 7.

Defaults for Non-VIP-Enabled Cisco 7500 Series Routers and Catalyst 6000 Family Switches with a FlexWAN Module

All platforms except the VIP-enabled Cisco 7500 series router and the Catalyst 6000 have the default values shown in Table 29.

If WRED is using the DSCP value to calculate the drop probability of a packet, all 64 entries of the DSCP table are initialized with the default settings shown in Table 29.

Table 29 random-detect dscp Default Settings

DSCP (Precedence)	Minimum Threshold	Maximum Threshold	Mark Probability
0(0)	20	40	1/10
1	22	40	1/10
2	24	40	1/10
3	26	40	1/10
4	28	40	1/10
5	30	40	1/10
6	32	40	1/10
7	34	40	1/10
8(1)	22	40	1/10
9	22	40	1/10
10	24	40	1/10
11	26	40	1/10
12	28	40	1/10
13	30	40	1/10
14	32	40	1/10
15	34	40	1/10
16(2)	24	40	1/10
17	22	40	1/10
18	24	40	1/10
19	26	40	1/10
20	28	40	1/10
21	30	40	1/10
22	32	40	1/10
23	34	40	1/10
24(3)	26	40	1/10
25	22	40	1/10
26	24	40	1/10
27	26	40	1/10
28	28	40	1/10
29	30	40	1/10

Table 29 random-detect dscp Default Settings (continued)

DSCP (Precedence)	Minimum Threshold	Maximum Threshold	Mark Probability
30	32	40	1/10
31	34	40	1/10
32(4)	28	40	1/10
33	22	40	1/10
34	24	40	1/10
35	26	40	1/10
36	28	40	1/10
37	30	40	1/10
38	32	40	1/10
39	34	40	1/10
40(5)	30	40	1/10
41	22	40	1/10
42	24	40	1/10
43	26	40	1/10
44	28	40	1/10
45	30	40	1/10
46	36	40	1/10
47	34	40	1/10
48(6)	32	40	1/10
49	22	40	1/10
50	24	40	1/10
51	26	40	1/10
52	28	40	1/10
53	30	40	1/10
54	32	40	1/10
55	34	40	1/10
56(7)	34	40	1/10
57	22	40	1/10
58	24	40	1/10
59	26	40	1/10
60	28	40	1/10
61	30	40	1/10
62	32	40	1/10
63	34	40	1/10
rsvp	36	40	1/10

Examples

The following example enables WRED to use the DSCP value 8. The minimum threshold for the DSCP value 8 is 20, the maximum threshold is 40, and the mark probability is 1/10.

```
random-detect dscp 8 20 40 10
```

Related Commands

Command	Description
random-detect	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 dscp (aggregate)

To configure aggregate Weighted Random Early Detection (WRED) parameters for specific differentiated services code point (DSCP) value, use the **random-detect dscp values (aggregate)** command in QoS policy-map class configuration mode. To disable configuration of aggregate WRED DSCP values, use the **no** form of this command.

random-detect dscp *sub-class-val1 sub-class-val2 sub-class-val3 sub-class-val4 min-thresh max-thresh mark-prob*

no random-detect dscp *sub-class-val1 sub-class-val2 sub-class-val3 sub-class-val4 min-thresh max-thresh mark-prob*

Cisco 10000 Series Router (PRE3)

random-detect dscp values *sub-class-val1* [...[*sub-class-val8*]] **minimum-thresh** *min-thresh-value* **maximum-thresh** *max-thresh-value* **mark-prob** *mark-prob-value*

no random-detect dscp values *sub-class-val1* [...[*sub-class-val8*]] **minimum-thresh** *min-thresh-value* **maximum-thresh** *max-thresh-value* **mark-prob** *mark-prob-value*

Syntax Description

sub-class-val1 *sub-class-val2* *sub-class-val3* *sub-class-val4*	DSCP value(s) to which the following WRED profile parameter specifications are to apply. A maximum of eight subclasses (DSCP values) can be specified per command-line interface (CLI) entry. See the "Usage Guidelines" for a list of valid DSCP values.
min-thresh	The minimum number of packets allowed in the queue. When the average queue length reaches the minimum threshold, WRED randomly drops some packets with the specified DSCP value. Valid minimum threshold values are 1 to 16384.
max-thresh	The maximum number of packets allowed in the queue. When the average queue length exceeds the maximum threshold, WRED drops all packets with the specified DSCP value. Valid maximum threshold values are 1 to 16384.
mark-prob	The 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.
Cisco 10000 Series Router	
values *sub-class-val1* [...[*subclass-val8*]]	DSCP value(s) to which the following WRED profile parameter specifications are to apply. A maximum of 8 subclasses (DSCP values) can be specified per CLI entry. 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**.
minimum-thresh *min-thresh*	Specifies the minimum number of packets allowed in the queue. When the average queue length reaches the minimum threshold, WRED randomly drops some packets with the specified DSCP value. Valid minimum threshold values are 1 to 16384.

maximum-thresh *max-thresh*	Specifies the maximum number of packets allowed in the queue. When the average queue length exceeds the maximum threshold, WRED drops all packets with the specified DSCP value. Valid maximum threshold values are 1 to 16384.
mark-probability *mark-prob*	Specifies the 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.

Command Default

For all precedence levels, the *mark-prob* default value is 10 packets.

Command Modes

Policy-map class configuration

Command History

Release	Modification
12.2(18)SXE	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2 and implemented on the Cisco 10000 series router.

Usage Guidelines

For ATM interfaces, the Aggregate WRED feature requires that the ATM SPA cards are installed in a Cisco 7600 SIP-200 carrier card or a Cisco 7600 SIP-400 carrier card.

To configure WRED on an ATM interface, you must use the **random-detect aggregate** commands; the standard random-detect commands are no longer supported on ATM interfaces.

Use this command with a **random-detect aggregate** command within a policy map configuration.

Repeat this command for each set of DSCP values that share WRED parameters.

After the policy map is defined, the policy map must be attached at the virtual circuit (VC) level.

The set of subclass (DSCP precedence) values defined on a **random-detect dscp (aggregate)** CLI will be aggregated into a single hardware WRED resource. The statistics for these subclasses will also be aggregated.

Use the **show policy-map interface** command to display the statistics for aggregated subclasses.

Cisco 10000 Series Router

For the PRE2, the **random-detect** command specifies the default profile for the queue. For the PRE3, the aggregate **random-detect** command is used instead to configure aggregate parameters for WRED. The PRE3 accepts the PRE2 **random-detect** command as a hidden command.

On the PRE2, accounting for the default profile is per precedence. On the PRE3, accounting and configuration for the default profile is per class map.

On the PRE2, the default threshold is per precedence for a DSCP or precedence value without an explicit threshold configuration. On the PRE3, the default threshold is to have no WRED configured.

On the PRE2, the drop counter for each precedence belonging to the default profile only has a drop count that matches the specific precedence value. Because the PRE2 has a default threshold for the default profile, the CBQOSMIB displays default threshold values. On the PRE3, the drop counter for each precedence belonging to the default profile has the aggregate counter of the default profile and not the individual counter for a specific precedence. The default profile on the PRE3 does not display any default threshold values in the CBQOSMIB if you do not configure any threshold values for the default profile.

DSCP Values

You must enter one or more differentiated service code point (DSCP) values. The command may include any combination of the following:

- numbers (0 to 63) representing differentiated services code point values
- af numbers (for example, af11) identifying specific AF DSCPs
- cs numbers (for example, cs1) identifying specific CS DSCPs
- **default**—Matches packets with the default DSCP.
- **ef**—Matches packets with EF DSCP.

For example, if you wanted the DCSP values of 0, 1, 2, 3, 4, 5, 6, or 7 (note that only one of the IP DSCP values must be a successful match criterion, not all of the specified DSCP values), enter the **match dscp 0 1 2 3 4 5 6 7** command.

Examples

The following example shows how to create a class map named map1 and associate it with the policy map named map2. The configuration enables WRED to drop map1 packets based on DSCP 8 with a minimum threshold of 24 and a maximum threshold of 40. The map2 policy map is attached to the outbound ATM interface 1/0/0.

```
Router(config-if)# class-map map1
Router(config-cmap)# match access-group 10
Router(config-cmap)# exit
Router(config)# policy-map map2
Router(config-pmap)# class map1
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-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface atm 1/0/0
Router(config-if)# service-policy output map2
```

The following example shows a DSCP-based aggregate WRED configuration for an ATM interface. Note that first a policy map named dscp-aggr-wred is defined for the default class, then dscp-based aggregate WRED is enabled with the **random-detect dscp-based aggregate** command, then subclasses and WRED parameter values are assigned in a series of **random-detect dscp (aggregate)** commands, and, finally, the policy map is attached at the ATM VC level using the **interface** and **service-policy** commands.

```
Router(config)# policy-map dscp-aggr-wred
Router(config-pmap)# class class-default
Router(config-pmap-c)# random-detect dscp-based aggregate minimum-thresh 1 maximum-thresh
10 mark-prob 10
!
! Define an aggregate subclass for packets with DSCP values of 0-7 and assign the WRED
! profile parameter values for this subclass
```

```
Router(config-pmap-c)# random-detect dscp 0 1 2 3 4 5 6 7 minimum-thresh 10 maximum-thresh
20 mark-prob 10
Router(config-pmap-c)# random-detect dscp 8 9 10 11 minimum-thresh 10 maximum-thresh 40
mark-prob 10
Router(config)# interface ATM4/1/0.11 point-to-point
Router(config-subif)# ip address 10.0.0.2 255.255.255.0
Router(config-subif)# pvc 11/101
Router(config-subif)# service-policy output dscp-aggr-wred
```

Cisco 10000 Series Router

The following example shows how to create a class map named Gold and associate it with the policy map named Business. The configuration enables WRED to drop Gold packets based on DSCP 8 with a minimum threshold of 24 and a maximum threshold of 40. The Business policy map is attached to the outbound ATM interface 1/0/0.

```
Router(config-if)# class-map Gold
Router(config-cmap)# match access-group 10
Router(config-cmap)# exit
Router(config)# policy-map Business
Router(config-pmap)# class Gold
Router(config-pmap-c)# bandwidth 48
Router(config-pmap-c)# random-detect dscp-based
Router(config-pmap-c)# random-detect dscp values 8 minimum-thresh 24 maximum-thresh 40
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface atm 1/0/0
Router(config-if)# service-policy output Business
```

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.
interface	Configures an interface type and enters interface configuration mode.
policy-map	Creates a policy map that can be attached to one or more interfaces to specify a service policy.
random-detect aggregate	Enables aggregate WRED and optionally specifies default WRED parameter values for a default aggregate class. This default class will be used for all subclasses that have not been explicitly configured.
service-policy	Attaches a policy map to an input interface or VC, or an output interface or VC, to be used as the service policy for that interface or VC.
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 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.

Command Default

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 "pol1":

```
Router(config)# policy-map pol1
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

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

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

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

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

Command Default

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 (QoS) Command-Line Interface (CLI) (MQC)

Command History

Release	Modification
11.1CC	This command was introduced.
12.0(5)T	This command was made available as a QoS policy-map class configuration command.
12.0(5)XE	This command was integrated into Cisco IOS Release 12.0(5)XE and implemented on Versatile Interface Processor (VIP) enabled Cisco 7500 series routers.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T and implemented on VIP-enabled Cisco 7500 series routers.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB and implemented on the Cisco 10000 series router.

Release	Modification
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.0(1)S	This command was modified. This command was hidden in interface configuration mode.
15.1(3)T	This command was modified. This command was hidden in interface configuration mode.

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 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 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 IP Switching Configuration Guide* and the *Cisco IOS IP Switching 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

Note Effective with Cisco IOS Release 15.1(3)T, the **random-detect flow** command is hidden. Although this command is still available in Cisco IOS software, the CLI interactive Help does not display it if you attempt to view it by entering a question mark at the command line.

This command will be completely removed in a future release. For more information, see the *Legacy QoS Command Deprecation* feature document in the *Cisco IOS Quality of Service Solutions Configuration Guide*.

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.

Command Default

Flow-based WRED is disabled by default.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)T	This command was modified. This command was hidden.

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

Note Effective with Cisco IOS Release 15.1(3)T, the **random-detect flow average-depth-factor** command is hidden. Although this command is still available in Cisco IOS software, the CLI interactive Help does not display it if you attempt to view it by entering a question mark at the command line.

This command will be completely removed in a future release. For more information, see the *Legacy QoS Command Deprecation* feature document in the *Cisco IOS Quality of Service Solutions Configuration Guide*.

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.

Command Default

The default average depth factor is 4.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)T	This command was modified. This command was hidden.

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

Note Effective with Cisco IOS Release 15.1(3)T, the **random-detect flow count** command is hidden. Although this command is still available in Cisco IOS software, the CLI interactive Help does not display it if you attempt to view it by entering a question mark at the command line.

This command will be completely removed in a future release. For more information, see the *Legacy QoS Command Deprecation* feature document in the *Cisco IOS Quality of Service Solutions Configuration Guide*.

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

number	Specifies a value from 16 to 2^{15} (32768).

Command Default

256

Command Modes

Interface configuration

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)T	This command was modified. This command was hidden.

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 prec-based

Note Effective with Cisco IOS Release 12.4(20)T, the **random-detect prec-based** command is replaced by the **random-detect precedence-based** command. See the **random-detect precedence-based** command for more information.

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

random-detect prec-based

no random-detect prec-based

Syntax Description

This command has no arguments or keywords.

Command Default

WRED is disabled by default.

Command Modes

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

Command History

Release	Modification
12.0(28)S	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.4(20)T	This command was replaced by the **random-detect precedence-based** command within a policy map.

Usage Guidelines

With the **random-detect prec-based** command, WRED is based on the IP precedence value of the packet.

Use the **random-detect prec-based** command before configuring the **random-detect precedence** command.

Beginning with Cisco IOS Release 12.4(20)T, use the **random-detect precedence** command when you configure a policy map.

Examples

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

```
Router> enable
Router# configure terminal
Router(config)# policy-map policy1
Router(config-pmap)# class class1
Router(config-pmap-c)# bandwidth percent 80
Router(config-pmap-c)# random-detect precedence-based
Router(config-pmap-c)# random-detect precedence 2 500 ms 1000 ms
Router(config-pmap-c)# exit
```

Related Commands

Command	Description
random-detect	Enables WRED or DWRED.
random-detect precedence	Configures the WRED and DWRED parameters for a particular IP precedence; configures WRED parameters for a particular IP precedence for a class policy in a policy map.

random-detect precedence

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

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

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 max-probability-denominator*

no random-detect precedence

Syntax Description

precedence	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 30 in the "Usage Guidelines" section.
rsvp	Indicates Resource Reservation Protocol (RSVP) traffic.
min-threshold	Minimum threshold in number of packets. The value range of this argument is from 1 to 4096. When the average queue length reaches the minimum threshold, WRED randomly drops some packets with the specified IP Precedence.
max-threshold	Maximum threshold in number of packets. The value range of this argument is from the value of the *min-threshold* argument to 4096. When the average queue length exceeds the maximum threshold, WRED drops all packets with the specified IP Precedence.
max-probability-denominator	Denominator for the fraction of packets dropped when the average queue depth is at the maximum threshold. For example, if the denominator is 512, 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.

Command Default

For all precedences, the *max-probability-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 30 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 (config-if)
Policy-map class configuration when used to specify class policy in a policy map (config-pmap-c)

Command History

Release	Modification
11.1CC	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(20)T	Support was added for hierarchical queueing framework (HQF) using the Modular Quality of Service (QoS) Command-Line Interface (CLI) (MQC). **Note** This command replaces the **random-detect prec-based** command in policy-map configuration.
15.0(1)S	This command was modified. This command was hidden in interface configuration mode.
15.1(3)T	This command was modified. This command was hidden in interface configuration mode.

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 30 lists the default minimum threshold value for each IP Precedence.

Table 30 Default WRED and DWRED Minimum Threshold Values

	Minimum Threshold Value (Fraction of Maximum Threshold Value)	
IP Precedence	**WRED**	**DWRED**
0	9/18	8/16
1	10/18	9/16
2	11/18	10/16
3	12/18	11/16
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 IP Switching Configuration Guide* and the *Cisco IOS IP Switching 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.

random-detect precedence (aggregate)

To configure aggregate Weighted Random Early Detection (WRED) parameters for specific IP precedence value(s), use the **random-detect precedence** (aggregate) command in policy-map class configuration mode. To disable configuration of aggregate WRED precedence values, use the **no** form of this command.

random-detect precedence s*ub-class-val1* [*sub-class-val2* **s***ub-class-val3* **s***ub-class-val4*] ***min-thresh max-thresh mark-prob***

no random-detect precedence s*ub-class-val1* [*sub-class-val2* **s***ub-class-val3* **s***ub-class-val4*]

Cisco 10000 Series Router (PRE3)

random-detect precedence s*ub-class-val1* [...[*sub-class-val8*]] **minimum-thresh** *min-thresh* **maximum-thresh** *max-thresh* **mark-probability** *mark-prob*

no random-detect precedence s*ub-class-val1* [...[*sub-class-val8*]]

Syntax Description

s*ub-class-val1* *sub-class-val2* **s***ub-class-val3* **s***ub-class-val4*	IP precedence value to which the following WRED profile parameter specifications are to apply. Up to four subclasses (IP precedence values) can be specified per command line interface (CLI) entry. The value range is from 0 to 7.
min-thresh	Minimum threshold (in number of packets) for the subclass(es). Valid values are from 1 to 12288.
max-thresh	Specifies the maximum threshold (in number of packets) for the subclass(es). Valid values are from the minimum threshold argument to 12288.
mark-prob	Specifies the denominator for the fraction of packets dropped when the average queue depth is at the maximum threshold for the subclass(es). Valid values are from 1 to 255.
Cisco 10000 Series Router	
s*ub-class-val1* [...[*subclass-val8*]]	IP precedence value(s) to which the following WRED profile parameter specifications are to apply. A maximum of 8 subclasses (IP precedence values) can be specified per CLI entry. The value range is from 0 to 7.
minimum-thresh *min-thresh*	Specifies the minimum number of packets allowed in the queue. When the average queue length reaches the minimum threshold, WRED randomly drops some packets with the specified IP precedence value. Valid minimum threshold values are 1 to 16384.
maximum-thresh *max-thresh*	Specifies the maximum number of packets allowed in the queue. When the average queue length exceeds the maximum threshold, WRED drops all packets with the specified IP precedence value. Valid maximum threshold values are 1 to 16384.
mark-probability *mark-prob*	Specifies the 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.

Command Default

Cisco 10000 Series Router

For all precedence levels, the *mark-prob* default is 10 packets.

Command Modes

Policy-map class configuration

Command History

Release	Modification
12.0(17)SL	This command was introduced on the Cisco 10000 series router.
12.2(18)SXE	This command was introduced.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB and implemented on the Cisco 10000 series router for the PRE3.

Usage Guidelines

For ATM interfaces, the Aggregate WRED feature requires that the ATM SPA cards are installed in a Cisco 7600 SIP-200 carrier card or a Cisco 7600 SIP-400 carrier card.

To configure WRED on an ATM interface, you must use the random-detect aggregate commands; the standard random-detect commands are no longer supported on ATM interfaces

Use this command with a **random-detect aggregate** command within a policy map configuration.

Repeat this command for each set of IP precedence values that share WRED parameters.

After the policy map is defined, the policy map must be attached at the VC level.

The set of subclass (IP precedence) values defined on a **random-detect precedence** (aggregate) CLI will be aggregated into a single hardware WRED resource. The statistics for these subclasses will also be aggregated.

Use the **show policy-map interface** command to display the statistics for aggregated subclasses.

Cisco 10000 Series Router

Table 31 lists the default drop thresholds for WRED based on DSCP, IP precedence, and discard-class. The drop probability indicates that the router drops one packet for every 10 packets.

Table 31 WRED Default Drop Thresholds

DSCP, Precedence, and Discard-Class Values	Minimum Threshold (times the queue size)	Maximum Threshold (times the queue size)	Drop Probability
All DSCPs	1/4	1/2	1/10
0	1/4	1/2	1/10
1	9/32	1/2	1/10
2	5/16	1/2	1/10
3	11/32	1/2	1/10
4	3/8	1/2	1/10
5	13/32	1/2	1/10
6	7/16	1/2	1/10
7	15/32	1/2	1/10

For the PRE2, the **random-detect** command specifies the default profile for the queue. For the PRE3, the aggregate **random-detect** command is used instead to configure aggregate parameters for WRED. The PRE3 accepts the PRE2 **random-detect** command as a hidden CLI.

On the PRE2, accounting for the default profile is per precedence. On the PRE3, accounting and configuration for the default profile is per class map.

On the PRE2, the default threshold is per precedence for a DSCP or precedence value without an explicit threshold configuration. On the PRE3, the default threshold is to have no WRED configured.

On the PRE2, the drop counter for each precedence belonging to the default profile only has a drop count that matches the specific precedence value. Because the PRE2 has a default threshold for the default profile, the CBQOSMIB displays default threshold values. On the PRE3, the drop counter for each precedence belonging to the default profile has the aggregate counter of the default profile and not the individual counter for a specific precedence. The default profile on the PRE3 does not display any default threshold values in the CBQOSMIB if you do not configure any threshold values for the default profile.

Examples

Cisco 10000 Series Router

The following example shows how to enable IP precedence-based WRED on the Cisco 10000 series router. In this example, the configuration of the class map named Class1 indicates to classify traffic based on IP precedence 3, 4, and 5. Traffic that matches IP precedence 3, 4, or 5 is assigned to the class named Class1 in the policy map named Policy1. WRED-based packet dropping is configured for Class1 and is based on IP precedence 3 with a minimum threshold of 500, maximum threshold of 1500, and a mark-probability-denominator of 200. The QoS policy is applied to PVC 1/32 on the point-to-point ATM subinterface 1/0/0.1.

```
Router(config)# class-map Class1
Router(config-cmap)# match ip precedence 3 4 5
Router(config-cmap)# exit
Router(config)# policy-map Policy1
Router(config-pmap)# class Class1
Router(config-pmap-c)# bandwidth 1000
Router(config-pmap-c)# random-detect prec-based
Router(config-pmap-c)# random-detect precedence 3 500 1500 200
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface atm 1/0/0
Router(config-if)# atm pxf queuing
Router(config-if)# interface atm 1/0/0.1 point-to-point
Router(config-subif)# pvc 1/32
Router(config-subif-atm-vc)# ubr 10000
Router(config-subif-atm-vc)# service-policy output policy1
```

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.
interface	Configures an interface type and enters interface configuration mode.
policy-map	Creates a policy map that can be attached to one or more interfaces to specify a service policy.

Command	Description
random-detect aggregate	Enables aggregate WRED and optionally specifies default WRED parameter values for a default aggregate class. This default class will be used for all subclasses that have not been explicitly configured.
service-policy	Attaches a policy map to an input interface or VC, or an output interface or VC, to be used as the service policy for that interface or VC.
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-group

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

This command will be completely removed in a future release. For more information, see the *Legacy QoS Command Deprecation* feature document in the *Cisco IOS Quality of Service Solutions Configuration Guide*.

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

group-name	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.

Command Default

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).
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.0(1)S	This command was modified. This command was hidden.
15.1(3)T	This command was modified. This command was hidden.

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 (per VC)	Enables per-VC WRED or per-VC VIP-distributed WRED.
show queueing	Lists all or selected configured queueing strategies.
show queueing interface	Displays the queueing statistics of an interface or VC.

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.
bps	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.
acl-index	(Optional) Access list number. Values are numbers from 1 to 2699.
rate-limit	(Optional) The access list is a rate-limit access list.
rate-limit-acl-index	(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).
dscp-value	(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.
qos-group-number	(Optional) The qos-group number. Values are numbers from 0 to 99.
burst-normal	Normal burst size, in bytes. The minimum value is bps divided by 2000. The value is a number from 1000 to 512000,000.
burst-max	Excess burst size, in bytes. The value is a number from 2000 to 1024000000.

conform-action *conform-action*	Action to take on packets that conform to the specified rate limit. Specify one of the following keywords: • **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 *exceed-action*	Action to take on packets that exceed the specified rate limit. Specify one of the following keywords: • **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.

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

Usage Guidelines Use this command to 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 (in bytes) = configured rate (in bits per second) * (1 byte)/(8 bits) * 1.5 seconds

17.000.000 * (1 byte)/(8 bits) * 1.5 seconds = 3.187.500 bytes

extended burst = 2 * normal burst

2 * 3.187.500 = 6.375.000 bytes

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 Solutions Configuration Guide*.

Examples In the following example, the recommended burst parameters for CAR are used:

```
Router(config)# interface serial6/1/0
Router(config-if)# rate-limit input access-group 1 17000000 3187500 6375000 conform-action
transmit exceed-action drop
```

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 1,500,000 bytes and an excess burst size of 3,000,000 bytes. Traffic that conforms is sent with an MPLS experimental field of 5. Traffic that does not conform is dropped. See the following command in the example:

```
rate-limit input 8000000 1500000 3000000 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 3750000 7500000
conform-action set-mpls-exp-transmit 5 exceed-action set-mpls-exp-transmit 0
Router(config-if)# rate-limit input access-group 102 10000000 1875000 3750000
conform-action set-mpls-exp-transmit 5 exceed-action drop
Router(config-if)# rate-limit input 8000000 1500000 3000000 conform-action
set-mpls-exp-transmit 5 exceed-action drop
Router(config-if)# ip address 10.1.1.1 255.255.255.252
!
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 1500 3000 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 1500 3000 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.

rcv-queue bandwidth

To define the bandwidths for ingress (receive) WRR queues through scheduling weights in interface configuration command mode, use the **rcv-queue bandwidth** command. To return to the default settings, use the **no** form of this command.

rcv-queue bandwidth *weight-1 ... weight-n*

no rcv-queue bandwidth

Syntax Description

weight-1 ... weight-n	WRR weights; valid values are from 0 to 255.

Command Default

The defaults are as follows:

- QoS enabled—4:255
- QoS disabled—255:1

Command Modes

Interface configuration

Command History

Release	Modification
12.2(17a)SX	This command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

This command is supported on 2q8t and 8q8t ports only.

You can configure up to seven queue weights.

Examples

This example shows how to allocate a three-to-one bandwidth ratio:

```
Router(config-if)# rcv-queue bandwidth 3 1
Router(config-if)#
```

Related Commands

Command	Description
rcv-queue queue-limit	Sets the size ratio between the strict-priority and standard receive queues.
show queueing interface	Displays queueing information.

rcv-queue cos-map

To map the class of service (CoS) values to the standard receive-queue drop thresholds, use the **rcv-queue cos-map** command in interface configuration mode. To remove the mapping, use the **no** form of this command.

rcv-queue cos-map *queue-id threshold-id cos-1 ... cos-n*

no rcv-queue cos-map *queue-id threshold-id*

Syntax Description

queue-id	Queue ID; the valid value is 1.
threshold-id	Threshold ID; valid values are from 1 to 4.
cos-1 ... cos-n	CoS values; valid values are from 0 to 7.

Command Default

The defaults are listed in Table 32.

Table 32 CoS-to-Standard Receive Queue Map Defaults

queue	threshold	cos-map	queue	threshold	cos-map
With QoS Disabled			**With QoS Enabled**		
1	1	0,1, 2,3,4,5,6,7	1	1	0,1
1	2		1	2	2,3
1	3		1	3	4
1	4		1	4	6,7
2	1	5	2	1	5

Command Modes

Interface configuration

Command History

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

Usage Guidelines

The *cos-n* value is defined by the module and port type. When you enter the *cos-n* value, note that the higher values indicate higher priorities.

Use this command on trusted ports only.

Examples

This example shows how to map the CoS values 0 and 1 to threshold 1 in the standard receive queue:

```
Router (config-if)# rcv-queue cos-map 1 1 0 1
  cos-map configured on:  Gi1/1 Gi1/2
```

Related Commands

Command	Description
show queueing interface	Displays queueing information.

rcv-queue queue-limit

To set the size ratio between the strict-priority and standard receive queues, use the **rcv-queue queue-limit** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

rcv-queue queue-limit *q-limit-1 q-limit-2*

no rcv-queue queue-limit

Syntax Description

q-limit-1	Standard queue weight; valid values are from 1 and 100 percent.
q-limit-2	Strict-priority queue weight; see the "Usage Guidelines" section for valid values.

Command Default

The defaults are as follows:

- 80 percent is for low priority.
- 20 percent is for strict priority.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

Valid strict-priority weight values are from 1 to 100 percent, except on 1p1q8t ingress LAN ports, where valid values for the strict-priority queue are from 3 to 100 percent.

The **rcv-queue queue-limit** command configures ports on a per-ASIC basis.

Estimate the mix of strict-priority-to-standard traffic on your network (for example, 80-percent standard traffic and 20-percent strict-priority traffic) and use the estimated percentages as queue weights.

Examples

This example shows how to set the receive-queue size ratio for Gigabit Ethernet interface 1/2:

```
Router# configure terminal
Router(config)# interface gigabitethernet 1/2
Router(config-if)# rcv-queue queue-limit 75 15
Router(config-if)# end
```

Related Commands

Command	Description
show queueuing interface	Displays queueing information.

rcv-queue random-detect

To specify the minimum and maximum threshold for the specified receive queues, use the **rcv-queue random-detect** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

rcv-queue random-detect {**max-threshold** | **min-threshold**} *queue-id threshold-percent-1 ... threshold-percent-n*

no rcv-queue random-detect {**max-threshold** | **min-threshold**} *queue-id*

Syntax Description

max-threshold	Specifies the maximum threshold.
min-threshold	Specifies the minimum threshold.
queue-id	Queue ID; the valid value is 1.
threshold-percent-1 threshold-percent-n	Threshold weights; valid values are from 1 to 100 percent.

Command Default

The defaults are as follows:

- **min-threshold**—80 percent
- **max-threshold**—20 percent

Command Modes

Interface configuration

Command History

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

Usage Guidelines

This command is supported on 1p1q8t and 8q8t ports only.

The 1p1q8t interface indicates one strict queue and one standard queue with eight thresholds. The 8q8t interface indicates eight standard queues with eight thresholds. The threshold in the strict-priority queue is not configurable.

Each threshold has a low- and a high-threshold value. The threshold values are a percentage of the receive-queue capacity.

For additional information on configuring receive-queue thresholds, refer to the QoS chapter in the *Cisco 7600 Series Router Cisco IOS Software Configuration Guide*.

Examples

This example shows how to configure the low-priority receive-queue thresholds:

```
Router (config-if)# rcv-queue random-detect max-threshold 1 60 100
```

Related Commands

Command	Description
show queueing interface	Displays queueing information.

rcv-queue threshold

To configure the drop-threshold percentages for the standard receive queues on 1p1q4t and 1p1q0t interfaces, use the **rcv-queue threshold** command in interface configuration mode. To return the thresholds to the default settings, use the **no** form of this command.

rcv-queue threshold *queue-id threshold-percent-1 ... threshold-percent-n*

no rcv-queue threshold

Syntax Description

queue-id	Queue ID; the valid value is 1.
threshold- percent-1 ... threshold- percent-n	Threshold ID; valid values are from 1 to 100 percent.

Command Default

The defaults for the 1p1q4t and 1p1q0t configurations are as follows:

- Quality of service (QoS) assigns all traffic with class of service (CoS) 5 to the strict-priority queue.
- QoS assigns all other traffic to the standard queue.

The default for the 1q4t configuration is that QoS assigns all traffic to the standard queue.

If you enable QoS, the following default thresholds apply:

- 1p1q4t interfaces have this default drop-threshold configuration:
  - Frames with CoS 0, 1, 2, 3, 4, 6, or 7 go to the standard receive queue.
  - Using standard receive-queue drop threshold 1, the Cisco 7600 series router drops incoming frames with CoS 0 or 1 when the receive-queue buffer is 50 percent or more full.
  - Using standard receive-queue drop threshold 2, the Cisco 7600 series router drops incoming frames with CoS 2 or 3 when the receive-queue buffer is 60 percent or more full.
  - Using standard receive-queue drop threshold 3, the Cisco 7600 series router drops incoming frames with CoS 4 when the receive-queue buffer is 80 percent or more full.
  - Using standard receive-queue drop threshold 4, the Cisco 7600 series router drops incoming frames with CoS 6 or 7 when the receive-queue buffer is 100 percent full.
  - Frames with CoS 5 go to the strict-priority receive queue (queue 2), where the Cisco 7600 series router drops incoming frames only when the strict-priority receive-queue buffer is 100 percent full.
- 1p1q0t interfaces have this default drop-threshold configuration:
  - Frames with CoS 0, 1, 2, 3, 4, 6, or 7 go to the standard receive queue. The Cisco 7600 series router drops incoming frames when the receive-queue buffer is 100 percent full.
  - Frames with CoS 5 go to the strict-priority receive queue (queue 2), where the Cisco 7600 series router drops incoming frames only when the strict-priority receive-queue buffer is 100 percent full.

Note The 100-percent threshold may be actually changed by the module to 98 percent to allow Bridge Protocol Data Unite (BPDU) traffic to proceed. The BPDU threshold is factory set at 100 percent.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

The *queue-id* value is always 1.

A value of 10 indicates a threshold when the buffer is 10 percent full.

Always set threshold 4 to 100 percent.

Receive thresholds take effect only on ports whose trust state is trust cos.

Configure the 1q4t receive-queue tail-drop threshold percentages with the **wrr-queue threshold** command.

Examples

This example shows how to configure the receive-queue drop thresholds for Gigabit Ethernet interface 1/1:

```
Router(config-if)# rcv-queue threshold 1 60 75 85 100
```

Related Commands

Command	Description
show queueing interface	Displays queueing information.
wrr-queue threshold	Configures the drop-threshold percentages for the standard receive and transmit queues on 1q4t and 2q2t interfaces.

recoverable-loss

To enable Enhanced Compressed Real-Time Transport Protocol (ECRTP), use the **recoverable-loss** command in IPHC-profile configuration mode. To disable ECRTP, use the **no** form of this command.

recoverable-loss {**dynamic** | *packet-drops*}

no recoverable-loss

Syntax Description

dynamic	Indicates that the dynamic recoverable loss calculation is used.
packet-drops	Maximum number of consecutive packet drops. Range is from 1 to 8.

Command Default

ECRTP is disabled.

Command Modes

IPHC-profile configuration (config-iphcp)

Command History

Release	Modification
12.4(9)T	This command was introduced.
12.4(11)T	Support was added for Frame Relay encapsulation.

Usage Guidelines

The **recoverable-loss** command is part of the ECRTP feature.

ECRPT Functionality

ECRTP reduces corruption by managing the way the compressor updates the context information at the decompressor. The compressor sends updated context information periodically to keep the compressor and decompressor synchronized. By repeating the updates, the probability of context corruption because of packet loss is minimized.

The synchronization of context information between the compressor and the decompressor can be performed dynamically (by specifying the **dynamic** keyword) or whenever a specific number of packets are dropped (by using the *packet-drops* argument).

The number of packet drops represents the quality of the link between the hosts. The lower the number of packet drops, the higher the quality of the link between the hosts.

The packet drops value is maintained independently for each context and does not have to be the same for all contexts.

Note If you specify the number of packet drops with the *packet-drops* argument, the **recoverable-loss** command automatically enables ECRTP.

Intended for Use with IPHC Profiles

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

Examples

The following example shows how to configure an IPHC profile called profile2. In this example, ECRTP is enabled with a maximum number of five consecutive packet drops.

```
Router> enable
Router# configure terminal
Router(config)# iphc-profile profile2 ietf
Router(config-iphcp)# recoverable-loss 5
Router(config-iphcp)# end
```

Related Commands

Command	Description
iphc-profile	Creates an IPHC profile.

redirect interface

To configure a traffic class to redirect packets belonging to a specific class to the interface that is specified in the command, use the **redirect interface** command in policy-map class configuration mode. To prevent the packets from getting redirected, use the **no** form of this command

redirect interface *interface type number*

no redirect interface *interface type number*

Syntax Description

interface type number	The type and number of the interface to which the packets need to be redirected.

Command Default

If this command is not specified, the packets are not redirected to an interface

Command Modes

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

Command History

Release	Modification
12.2(18)ZYA1	This command was introduced.

Usage Guidelines

Use this command to redirect packets to a predefined interface. You can also configure the **redirect interface** command with the **log** command but not with a **drop** or **copy interface** command. This command cannot be configured with a service policy for a stack class. The packets can be redirected only to the following interfaces:

- Ethernet
- Fast Ethernet
- Gigabit Ethernet
- Ten Gigabit Ethernet

Examples

In the following example, a traffic class called cmtest has been created and configured for use in a policy map called pmtest. The policy map (service policy) is attached to Fast Ethernet interface 4/15. All packets in the cmtest are redirected to FastEthernet interface 4/18.

```
Router(config)# policy-map type access-control pmtest
Router(config-pmap)# class cmtest
Router(config-pmap-c)# redirect interface FastEthernet 4/18
Router(config-pmap-c)# log
Router(config-pmap-c)# exit
Router(config)# interface FastEthernet 4/18
Router(config-if)# service-policy input pmtest
```

Related Commands

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

refresh max-period

To set the number of packets sent between full-header refresh occurrences, use the **refresh max-period** command in IPHC-profile configuration mode. To use the default number of packets, use the **no** form of this command.

refresh max-period {*number-of-packets* | **infinite**}

no refresh max-period

Syntax Description

number-of-packets	Number of packets sent between full-header refresh occurrences. Range is from 0 to 65535. Default is 256.
infinite	Indicates no limitation on the number of packets sent between full-header refresh occurrences.

Command Default

The number of packets sent between full-header refresh occurrences is 256.

Command Modes

IPHC-profile configuration

Command History

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

Usage Guidelines

Use the **refresh max-period** command to set the number of non-TCP packets sent between full-header refresh occurrences. The **refresh max-period** command also allows you to specify no limitation on the number of packets sent between full-header refresh occurrences. To specify no limitation on the number of packets sent, use the **infinite** keyword.

Prerequisite

Before you use the **refresh max-period** command, you must enable non-TCP header compression by using the **non-tcp** command.

Intended for Use with IPHC Profiles

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

Examples

The following is an example of an IPHC profile called profile2. In this example, the number of packets sent before a full-header refresh occurrence is 700 packets.

```
Router> enable
Router# configure terminal
Router(config)# iphc-profile profile2 ietf
Router(config-iphcp)# non-tcp
Router(config-iphcp)# refresh max-period 700
Router(config-iphcp)# end
```

Related Commands

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

refresh max-time

To set the amount of time to wait before a full-header refresh occurrence, use the **refresh max-time** command in IPHC-profile configuration mode. To use the default time, use the **no** form of this command.

refresh max-time {*seconds* | **infinite**}

no refresh max-time

Syntax Description

seconds	Length of time, in seconds, to wait before a full-header refresh occurrence. Range is from 0 to 65535. Default is 5.
infinite	Indicates no limitation on the time between full-header refreshes.

Command Default

The amount of time to wait before a full-header refresh occurrence is set to 5 seconds.

Command Modes

IPHC-profile configuration

Command History

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

Usage Guidelines

Use the **refresh max-time** command to set the maximum amount of time to wait before a full-header refresh occurs. The **refresh max-time** command also allows you to indicate no limitation on the time between full-header refresh occurrences. To specify no limitation on the time between full-header refresh occurrences, use the **infinite** keyword.

Prerequisite

Before you use the **refresh max-time** command, you must enable non-TCP header compression by using the **non-tcp** command.

Intended for Use with IPHC Profiles

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

Examples

The following is an example of an IPHC profile called profile2. In this example, the maximum amount of time to wait before a full-header refresh occurs is 500 seconds.

```
Router> enable
Router# configure terminal
Router(config)# iphc-profile profile2 ietf
Router(config-iphcp)# non-tcp
Router(config-iphcp)# refresh max-time 500
Router(config-iphcp)# end
```

Related Commands

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

refresh rtp

To enable a context refresh occurrence for Real-Time Transport Protocol (RTP) header compression, use the **refresh rtp** command in IPHC-profile configuration mode. To disable a context refresh occurrence for RTP header compression, use the **no** form of this command.

refresh rtp

no refresh rtp

Syntax Description

This command has no arguments or keywords.

Command Default

Context refresh occurrences for RTP header compression are disabled.

Command Modes

IPHC-profile configuration

Command History

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

Usage Guidelines

Use the **refresh rtp** command to enable a context refresh occurrence for RTP header compression. A context is the state that the compressor uses to compress a header and that the decompressor uses to decompress a header. The context is the uncompressed version of the last header sent and includes information used to compress and decompress the packet.

Prerequisite

Before you use the **refresh rtp** command, you must enable RTP header compression by using the **rtp** command.

Intended for Use with IPHC Profiles

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

Examples

The following is an example of an IPHC profile called profile2. In this example, the **refresh rtp** command is used to enable a context refresh occurrence for RTP header compression.

```
Router> enable
Router# configure terminal
Router(config)# iphc-profile profile2 ietf
Router(config-iphcp)# rtp
Router(config-iphcp)# refresh rtp
Router(config-iphcp)# end
```

Related Commands

Command	Description
iphc-profile	Creates an IPHC profile.
rtp	Enables RTP header compression within an IPHC profile.

rtp

To enable Real-Time Transport Protocol (RTP) header compression within an IP Header Compression (IPHC) profile, use the **rtp** command in IPHC-profile configuration mode. To disable RTP header compression within an IPHC profile, use the **no** form of this command.

rtp

no rtp

Syntax Description

This command has no arguments or keywords.

Command Default

RTP header compression is enabled.

Command Modes

IPHC-profile configuration

Command History

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

Usage Guidelines

The **rtp** command enables RTP header compression and automatically enables non-TCP header compression (the equivalent of using the **non-tcp** command).

Intended for Use with IPHC Profiles

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

Examples

The following example shows how to configure an IPHC profile called profile2. In this example, RTP header compression is configured.

```
Router> enable
Router# configure terminal
Router(config)# iphc-profile profile2 ietf
Router(config-iphcp)# rtp
Router(config-iphcp)# end
```

Related Commands

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