QoS: Time-Based Thresholds for WRED and Queue Limit

The QoS: Time-Based Thresholds for WRED and Queue Limit feature allows you to specify the Weighted Random Early Detection (WRED) minimum and maximum thresholds or the queue limit threshold in milliseconds (ms). Previously, these thresholds could only be specified in packets or bytes. Now, all three units of measure are available. Once the threshold limits are configured in a policy map, the policy map can be used on multiple interfaces, including those with different amounts of bandwidth.

Feature History for QoS: Time-Based Thresholds for WRED and Queue Limit

Release	Modification
12.0(28)S	This feature was introduced.
12.2(27)SBA	This feature was integrated into Cisco IOS Release 12.2(27)SBA.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

CISCO SYSTEMS

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Prerequisites for QoS: Time-Based Thresholds for WRED and Queue Limit

Before configuring this feature, a traffic class must be configured and a policy map must exist. To create the traffic class (specifying the appropriate match criteria) and the policy map, use the modular quality of service (QoS) command-line interface (MQC).

Restrictions for QoS: Time-Based Thresholds for WRED and Queue Limit

This feature allows you to specify either the WRED thresholds or the queue limit threshold in packets (the default unit of measure), bytes, or milliseconds (ms). However, these units cannot be mixed. That is, the unit of measure in the *same* class, in the *same* policy map, cannot be mixed. For example, if you specify the minimum threshold for a particular class in milliseconds, the maximum threshold for that class must also be in milliseconds.

Information About QoS: Time-Based Thresholds for WRED and Queue Limit

To configure the QoS: Time-Based Thresholds for WRED and Queue Limit feature, you should understand the following concepts:

- Benefits, page 2
- Setting Thresholds by Using WRED, page 3
- Setting Thresholds by Using the queue-limit Command, page 3
- random-detect Commands with the Millisecond (ms) Keyword, page 3
- Mixing Threshold Units of Measure, page 4

Benefits

Queue Limit Thresholds Specified in Additional Units of Measure

Previously, the WRED thresholds and the queue limit thresholds could only be specified in packets or bytes. With this feature, the thresholds can be specified either in packets, bytes or milliseconds. These additional units of measure provide more flexibility and allow you to fine-tune your configuration.

Policy Maps Can be Reused as Needed on Multiple Interfaces

The WRED and queue limit thresholds are specified and configured in policy maps. Once the threshold limits are configured in a policy map, the policy map can be used on multiple interfaces, including those with different amounts of bandwidth. This is especially useful when the bandwidth for a class on given interface is being specified as a percentage of the total bandwidth available.

Setting Thresholds by Using WRED

WRED is a congestion avoidance mechanism. WRED combines the capabilities of the Random Early Detection (RED) algorithm with the IP precedence feature to provide for preferential traffic handling of higher priority packets. WRED can selectively discard lower priority traffic when the interface begins to get congested and provide differentiated performance characteristics for different classes of service.

WRED differs from other congestion avoidance techniques such as queueing strategies because it attempts to anticipate and avoid congestion rather than control congestion once it occurs.

WRED is enabled by using the **random-detect** command. Then the minimum threshold, maximum threshold, and mark probability denominator can be set to determine the treatment that packets receive by using the appropriate command. For example, the **random-detect precedence** command can be used to determine the thresholds for a specific IP precedence.

For more information about WRED, refer to the “Congestion Avoidance” section of the *Cisco IOS Quality of Service Solutions Configuration Guide*.

Setting Thresholds by Using the queue-limit Command

The **queue-limit** command allows you to specify or modify the maximum number of packets the queue can hold (that is, the threshold) for a class policy configured in a policy map. Packets belonging to a class are subject to the guaranteed bandwidth allocation and the queue limits that characterize the traffic class. With the **queue-limit** command, the threshold is the aggregate threshold for the entire class.

After a queue has reached its configured queue limit, enqueuing of additional packets to the traffic class causes tail drop or WRED (if configured) to take effect, depending on how the policy map is configured. (Tail drop is a means of avoiding congestion that treats all traffic equally and does not differentiate between classes of service.)

Queues fill during periods of congestion. When the output queue is full and tail drop is in effect, packets are dropped until the congestion is eliminated and the queue is no longer full).

Tail drop is used for distributed class-based weighted fair queueing (DCBWFQ) traffic classes unless you explicitly configure a service policy to use WRED to drop packets as a means of avoiding congestion. Note that if you use WRED instead of tail drop for one or more traffic classes making up a service policy, you must ensure that WRED is not configured for the interface to which you attach that service policy.

For more information about tail drop and DCBWFQ, refer to the “Congestion Management” section of the *Cisco IOS Quality of Service Solutions Configuration Guide*.

random-detect Commands with the Millisecond (ms) Keyword

This feature allows you to specify the WRED minimum and maximum thresholds in milliseconds (ms). You can specify the threshold in milliseconds by using the **ms** keyword available with the **random-detect** commands listed in Table 1.

Table 1 ***random-detect Commands with the Milliseconds (ms) Keyword***

Command	Description
random-detect clp	Configures the WRED parameters for a particular cell loss priority (CLP) value, or a particular CLP value for a class policy in a policy map.
random-detect cos	Configures the WRED parameters for a particular class of service (CoS) value, or a particular CoS value for a class policy in a policy map.
random-detect discard-class	Configures the WRED parameters for a particular discard-class, or a particular discard-class for a class policy in a policy map.
random-detect dscp	Configures the WRED parameters for a particular differentiated services code point (DSCP) value, or a particular DSCP value for a class policy in a policy map.
random-detect precedence	Configures WRED parameters for a particular IP precedence, or a particular IP precedence for a class policy in a policy map.

For more information about these commands, see the "Command Reference" section of this document.

Mixing Threshold Units of Measure

With this feature, the thresholds can be specified in packets (the default unit of measure), bytes, or milliseconds (ms). For instance, with WRED, you can specify the minimum threshold and the maximum threshold in packets, bytes, or milliseconds. However, the units cannot be mixed. For example, if you specify the minimum threshold in milliseconds, the maximum threshold must also be specified in milliseconds.

How to Configure QoS: Time-Based Thresholds for WRED and Queue Limit

This section contains the following procedures:

- Enabling WRED and Using WRED to Specify Thresholds, page 5 (required)
- Using the queue-limit Command to Specify the Thresholds, page 6 (required)
- Attaching the Policy Map to an Interface, page 8 (required)
- Verifying the Configuration, page 9 (optional)

Enabling WRED and Using WRED to Specify Thresholds

This procedure allows you to set the WRED thresholds for traffic with a specific value, such as the IP precedence, differentiated services code point (DSCP), Resource Reservation Protocol (RSVP), discard-class, class of service (CoS), or cell loss priority (CLP).

To enable WRED and use it to specify the thresholds for user-defined categories of traffic, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map** *policy-name*
4. **class** {*class-name* | **class-default**}
5. **bandwidth** {*bandwidth-kbps* | **remaining percent** *percentage* | **percent** *percentage*}

   or
6. **shape** [**average** | **peak**] *mean-rate* [[*burst-size*] [*excess-burst-size*]]
7. **random-detect**
8. **random-detect precedence** {*precedence* | **rsvp**} *min-threshold* {**bytes** | **ms** | **packets**} *max-threshold* {**bytes** | **ms** | **packets**} [*mark-probability-denominator*]
9. **exit**

DETAILED STEPS

	Command	Purpose

Step 1	**`enable`**
	
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		- Enter your password if prompted.

Step 2	**`configure terminal`**
	
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 3	**`policy-map`** *`policy-name`*
	
	Example:
	`Router(config)# policy-map policy1`
		Specifies the name of the policy map to be created. Enters policy-map configuration mode.
		- Enter policy map name.

Step 4	**`class`** {*`class-name`* | **`class-default`**}
	
	Example:
	`Router(config-pmap)# class class1`
		Specifies the class so that you can configure or modify its policy. Enters policy-map class configuration mode.
		- Enter the class name or specify the default class (class-default).

	To continue with the configuration, you must either specify a bandwidth (Step 5) or enable traffic shaping (Step 6). Choose one or the other.	

	Command	Purpose

Step 5	**bandwidth** {*bandwidth-kbps* | **remaining percent** *percentage* | **percent** *percentage*}
	Example:
	`Router(config-pmap-c)# bandwidth percent 40`
		(Optional) Specifies or modifies the bandwidth allocated for a class belonging to a policy map.
		• Enter the bandwidth to be set or modified.

	Or	
Step 6	**shape** [**average** | **peak**] *mean-rate* [[*burst-size*] [*excess-burst-size*]] **Example:** `Router(config-pmap-c)# shape average 51200`	(Optional) Enables either average or peak rate traffic shaping. • Specify either average or peak traffic shaping.
Step 7	**random-detect** **Example:** `Router(config-pmap-c)# random-detect`	Enables WRED or distributed WRED (DWRED).
Step 8	**random-detect precedence** {*precedence* | **rsvp**} *min-threshold* {**bytes**| **ms** | **packets**} *max-threshold* {**bytes** | **ms** | **packets**} [*mark-probability-denominator*] **Example:** `Router(config-pmap-c)# random-detect precedence 2 512 ms 1020 ms`	Configures WRED and DWRED parameters for a particular IP precedence. • Specify the IP precedence or RSVP value, and thresholds, as needed. **Note** In this example, the WRED parameters were specified for traffic with a specific IP precedence value. Other values can be specified with other **random-detect** commands. For a list of the other **random-detect** commands, see Table 1 on page 4.
Step 9	**exit** **Example:** `Router(config-pmap-c)# exit`	(Optional) Exits policy-map class configuration mode.

Using the queue-limit Command to Specify the Thresholds

The **queue-limit** command allows you to set the aggregate-level thresholds for an entire class. To specify the thresholds by using the **queue-limit** command, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map** *policy-name*
4. **class** {*class-name* | **class-default**}
5. **bandwidth** {*bandwidth-kbps* | **remaining percent** *percentage* | **percent** *percentage*}

   or

6. **shape** [**average** | **peak**] *mean-rate* [[*burst-size*] [*excess-burst-size*]]
7. **queue-limit** *number-of-packets* {**bytes** | **ms** | **packets**}
8. **exit**

DETAILED STEPS

	Command	Purpose

Step 1	**`enable`**
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	**`configure terminal`**
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 3	**`policy-map`** *`policy-name`*
	Example:
	`Router(config)# policy-map policy1`
		Specifies the name of the policy map to be created. Enters policy-map configuration mode.
		• Enter policy map name.

Step 4	**`class`** {*`class-name`* | **`class-default`**}
	Example:
	`Router(config-pmap)# class class1`
		Specifies the class so that you can configure or modify its policy. Enters policy-map class configuration mode.
		• Enter the class name or specify the default class (class-default).

	To continue with the configuration, you must either specify a bandwidth (Step 5) or enable traffic shaping (Step 6). Choose one or the other.	

Step 5	**`bandwidth`** {*`bandwidth-kbps`* | **`remaining percent`** *`percentage`* | **`percent`** *`percentage`*}
	Example:
	`Router(config-pmap-c)# bandwidth percent 40`
		(Optional) Specifies or modifies the bandwidth allocated for a class belonging to a policy map.
		• Enter the bandwidth to be set or modified.

	Or	
Step 6	**`shape`** [**`average`** | **`peak`**] *`mean-rate`* [[*`burst-size`*] [*`excess-burst-size`*]] **Example:** `Router(config-pmap-c)# shape average 51200`	(Optional) Enables either average or peak rate traffic shaping. • Specifies either average or peak traffic shaping.

	Command	Purpose
Step 7	**queue-limit** *number-of-packets* [**bytes** | **ms** | **packets**] **Example:** `Router(config-pmap-c)# queue-limit 200 ms`	Specifies or modifies the maximum number of packets the queue can hold (that is, the queue limit) for a class configured in a policy map. • Enter the queue limit. The unit of measure can be bytes, milliseconds, or packets.
Step 8	**exit** **Example:** `Router(config-pmap-c)# exit`	(Optional) Exits policy-map class configuration mode.

Attaching the Policy Map to an Interface

So far, you have specified the threshold in a policy map. The next step is to attach the policy map to an interface. Policy maps can be attached to either the input or output direction of the interface.

Note Depending on the needs of your network, you may need to attach the policy map to a subinterface, an ATM PVC, a Frame Relay DLCI, or other type of interface.

To attach the policy map to an interface, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **pvc** [*name*] *vpi/vci* [**ilmi** | **qsaal** | **smds**]
5. **service-policy** {**input** | **output**} *policy-map-name*
6. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose

Step 3	**`interface`** *`type number`*
	Example:
	`Router(config)# interface s4/0`
		Configures an interface (or subinterface) type and enters interface configuration mode.
		• Enter the interface type number.

Step 4	**`pvc`** `[`*`name`*`]` *`vpi`*`/`*`vci`* `[`**`ilmi`** `|` **`qsaal`** `|` **`smds`**`]`
	Example:
	`Router(config-if)# pvc cisco 0/16 ilmi`
		(Optional) Creates or assigns a name to an ATM PVC and specifies the encapsulation type on an ATM PVC. Enters ATM VC configuration mode.
		Note This step is required only if you are attaching the policy map to an ATM PVC. If you are not attaching the policy map to an ATM PVC, skip this step and proceed with Step 5.

Step 5	**`service-policy`** `{`**`input`** `|` **`output`**`}` *`policy-map-name`*
	Example:
	`Router(config-if)# service-policy output policy1`
		Specifies the name of the policy map to be attached to the input *or* output direction of the interface.
		Note Policy maps can be configured on ingress or egress routers. They can also be attached in the input or output direction of an interface. The direction (input or output) and the router (ingress or egress) to which the policy map should be attached varies according your network configuration. When using the **service-policy** command to attach the policy map to an interface, be sure to choose the router and the interface direction that are appropriate for your network configuration.
		• Enter the policy map name.

Step 6	**`exit`**
	Example:
	`Router(config-if)# exit`
		(Optional) Exits interface configuration mode.

Verifying the Configuration

To verify the configuration, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **show policy-map** [*policy-map*]

   or

   show policy-map interface *interface-name*
3. **exit**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**`enable`**
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	**`show policy-map`** `[`*`policy-map`*`]`
	Example:
	`Router# show class-map class1`
		Displays all information about a class map, including the match criterion.
		• Enter class map name.

	and/or	

	`show policy-map interface` *`interface-name`*
	Example:
	`Router# show policy-map interface s4/0`
		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.
		• Enter the interface name.

Step 3	**`exit`**
	Example:
	`Router# exit`
		(Optional) Exits EXEC mode.

Troubleshooting Tips

The commands in the "Verifying the Configuration" section allow you to verify that you achieved the intended configuration and that the feature is functioning correctly. If, after using the **show** commands listed above, you find that the configuration is not correct or the feature is not functioning as expected, perform these operations:

If the configuration is not the one you intended, complete the following steps:

1. Use the **show running-config** command and analyze the output of the command.
2. If the policy map does not appear in the output of the **show running-config** command, enable the **logging console** command.
3. Attach the policy map to the interface again.

If the packets are not being matched correctly (for example, the packet counters are not incrementing correctly), complete the following procedures:

1. Run the **show policy-map** command and analyze the output of the command.
2. Run the **show running-config** command and analyze the output of the command.
3. Use the **show policy-map interface** command and analyze the output of the command. Check the following findings:
    a. If a policy map applies queueing, and the packets are matching the correct class, but you see unexpected results, compare the number of the packets in the queue with the number of the packets matched.

b. If the interface is congested, and only a small number of the packets are being matched, check the tuning of the transmission (tx) ring, and evaluate whether the queueing is happening on the tx ring. To do this, use the **show controllers** command, and look at the value of the tx count in the output of the command.

Configuration Examples for QoS: Time-Based Thresholds for WRED and Queue Limit

This section provides the following configuration examples:

- Using WRED to Set Thresholds: Example, page 11
- Using the queue-limit Command to Set Thresholds: Example, page 11
- Verifying the Configuration: Example, page 12

Using WRED to Set Thresholds: Example

In the following example, WRED has been configured in the policy map called “policy1”. In this WRED configuration, the bandwidth has been specified as a percentage (80%), and the minimum and maximum thresholds for IP precedence 2 are set to 512 milliseconds and 1020 milliseconds, respectively.

```
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
Router(config-pmap-c)# random-detect precedence 2 512 ms 1020 ms
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface s4/0
Router(config-if)# service-policy output policy1
Router(config-if)# end
```

Using the queue-limit Command to Set Thresholds: Example

In the following example, a policy map called “policy2” has been configured. The policy2 policy map contains a class called “class1.” The bandwidth for this class has been specified as a percentage (80%) and the **queue-limit** command has been used to set the threshold to 200 milliseconds.

```
Router> enable
Router# configure terminal
Router(config)# policy-map policy2
Router(config-pmap)# class class1
Router(config-pmap-c)# bandwidth percent 80
Router(config-pmap-c)# queue-limit 200 ms
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface s4/0
Router(config-if)# service-policy output policy1
Router(config-if)# end
```

Verifying the Configuration: Example

To verify that this feature is configured correctly, use either the **show policy-map** command or the **show policy-map interface** command.

This section contains two sets of sample output from the **show policy-map interface** command and the **show policy-map** command—one set showing the output when WRED is used to configure the feature, one set showing the output when the **queue-limit** command is used to configure the feature.

WRED Threshold Configuration Sample Output

The following is sample output of the **show policy-map** command when WRED has been used to specify the thresholds. The words “time-based wred” indicates that the thresholds have been specified in milliseconds (ms).

```
Router# show policy-map
  Policy Map policy1
    Class class1
      bandwidth 80 (%)
       time-based wred, exponential weight 9

      class    min-threshold    max-threshold    mark-probability
      ----------------------------------------------------------
      0       -                -                1/10
      1       -                -                1/10
      2       512              1024             1/10
      3       -                -                1/10
      4       -                -                1/10
      5       -                -                1/10
      6       -                -                1/10
      7       -                -                1/10
```

The following is sample output of the **show policy-map interface** command when WRED has been used to specify the thresholds.

```
Router# show policy-map interface Ethernet2/0

 Ethernet2/0

  Service-policy output: policy1 (1100)

    Class-map: class1 (match-all) (1101/1)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: protocol ftp (1102)
      Queueing
      queue limit 16 ms/ 16000 bytes
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts queued/bytes queued) 0/0
      bandwidth 80.00% (%) (8000 kbps)
        Exp-weight-constant: 9 (1/512)
        Mean queue depth: 0 ms/ 0 bytes
        class    Transmitted  Random drop   Tail drop    Minimum       Maximum       Mark
                 pkts/bytes   pkts/bytes    pkts/bytes   thresh        thresh        prob
                                                         ms/bytes      ms/bytes
        0        0/0          0/0           0/0           4/4000        8/8000       1/10
        1        0/0          0/0           0/0           4/4500        8/8000       1/10
        2        0/0          0/0           0/0         512/512000   1024/1024000    1/10
        3        0/0          0/0           0/0           5/5500        8/8000       1/10
        4        0/0          0/0           0/0           6/6000        8/8000       1/10
        5        0/0          0/0           0/0           6/6500        8/8000       1/10
        6        0/0          0/0           0/0           7/7000        8/8000       1/10
        7        0/0          0/0           0/0           7/7500        8/8000       1/10

    Class-map: class-default (match-any) (1105/0)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any  (1106)
        0 packets, 0 bytes
        5 minute rate 0 bps

      queue limit 64 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts queued/bytes queued) 0/0
```

Formula for Converting the Threshold from Milliseconds to Bytes

When converting the threshold from milliseconds to bytes, the following formula is used:

milliseconds * (bandwidth configured for the class) / 8 = total number of bytes

For this example, the following numbers would be used in the formula:

512 ms * 8000 kbps / 8 = 512000 bytes

Note Class1 has a bandwidth of 8000 kbps.

queue-limit command Threshold Configuration Sample Output

The following is sample output of the **show policy-map** command when the **queue-limit** command has been used to specify the thresholds in milliseconds.

```
Router# show policy-map
  Policy Map policy1
    Class class1
      bandwidth 80 (%)
      queue-limit 200 ms
```

The following is sample output from the **show policy-map interface** command when the **queue-limit** command has been used to specify the thresholds.

```
Router# show policy-map interface

 Ethernet2/0

  Service-policy output: policy1 (1070)

    Class-map: class1 (match-all) (1071/1)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: protocol ftp (1072)
      Queueing
      queue limit 200 ms/ 200000 bytes
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts queued/bytes queued) 0/0
      bandwidth 80.00% (%) (8000 kbps)

    Class-map: class-default (match-any) (1075/0)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any  (1076)
        0 packets, 0 bytes
  5 minute rate 0 bps

queue limit 64 packets
(queue depth/total drops/no-buffer drops) 0/0/0
(pkts queued/bytes queued) 0/0
```

Formula for Converting the Threshold from Milliseconds to Bytes

When converting the threshold from milliseconds to bytes, the following formula is used:

milliseconds * (bandwidth configured for the class)/ 8 = total number of bytes

For this example, the following numbers would be used in the formula:

200 ms * 8000 kbps / 8 = 200000 bytes

Note Class1 has a bandwidth of 8000 kbps.

Additional References

The following sections provide references related to the QoS: Time-Based Thresholds for WRED and Queue Limit feature.

Related Documents

Related Topic	Document Title
Quality of service (QoS) commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	*Cisco IOS Quality of Service Solutions Command Reference*, Release 12.3 T.
Congestion avoidance mechanisms, including tail drop, RED and WRED	*Cisco IOS Quality of Service Solutions Configuration Guide*
Congestion management mechanisms, including CBWFQ, and DCBWFQ	*Cisco IOS Quality of Service Solutions Configuration Guide*
Byte-Based WRED	*Byte-Based Weight Random Early Detection* feature module, Cisco IOS Release 12.0(26)S

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	—

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml

Command Reference

This section documents new and modified commands. All other commands used with this feature are documented in the Cisco IOS Release 12.3 command reference publications.

New Commands

- **random-detect atm-clp-based**
- **random-detect clp**
- **random-detect cos**
- **random-detect cos-based**
- **random-detect dscp-based**
- **random-detect prec-based**

Modified Commands

- **queue-limit**
- **random-detect discard-class**
- **random-detect discard-class-based**
- **random-detect dscp**
- **random-detect precedence**
- **show policy-map**
- **show policy-map interface**

queue-limit

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

queue-limit *number-of-packets*

no queue-limit *number-of-packets*

Syntax Description

number-of-packets	A number in the range from 1 to 64 specifying the maximum number of packets that the queue for this class can accumulate.

Defaults

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

On all other platforms, the default is 64.

Command Modes

Policy-map class configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(5)XE	This command was integrated into Cisco IOS Release 12.0(5)XE. Support for VIP-enabled Cisco 7500 series routers was added.
12.1(5)T	This command was implemented on the VIP-enabled Cisco 7500 series routers.
12.2(27)SBA	This command was integrated into Cisco IOS Release 12.2(27)SBA.

Usage Guidelines

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

Overriding Queue Limits Set by the Bandwidth Command

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

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

Examples

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

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

Related Commands

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

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 *clp-value*

Syntax Description

clp-value	CLP value. Valid values are 0 or 1.

Defaults

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

Command History

Release	Modification
12.0(28)S	This command was introduced.
12.2(27)SBA	This command was integrated into Cisco IOS Release 12.2(27)SBA.

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)# exit
Router(config-pmap)# exit
Router(config)# exit
```

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 clp

To specify the ATM cell loss priority (CLP) value of a packet, the minimum and maximum thresholds, and the maximum probability denominator used for enabling weighted random early detection (WRED), use the **random-detect clp** command in policy-map class configuration mode. To reset the thresholds and maximum probability denominator to the default values for the specified ATM CLP, use the **no** form of this command.

random-detect clp *clp-value min-threshold max-threshold max-probability-denominator*

no random-detect clp *clp-value min-threshold max-threshold max-probability-denominator*

Syntax Description

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

Defaults

The default values for the *min-threshold* and *max-threshold* arguments are based on the output buffering capacity and the transmission speed for the interface.

The default for the *max-probability-denominator* argument is 10; 1 out of every 10 packets is dropped at the maximum threshold.

Command Modes

Policy-map class configuration

Command History

Release	Modification
12.0(28)S	This command was introduced.
12.2(27)SBA	This command was integrated into Cisco IOS Release 12.2(27)SBA.

Usage Guidelines

Note the following points when using the **random-detect clp** command:

- When the average queue length reaches the minimum threshold, WRED randomly drops some packets with the specified IP precedence.
- When the average queue length exceeds the maximum threshold, WRED drops all packets with the specified IP precedence.
- The *max-probability-denominator* argument is 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.

Examples

In the following example, WRED has been enabled using the **random-detect clp** command. With the **random-detect clp** command, the ATM CLP has been specified, along with the minimum and maximum thresholds, and the maximum probability denominator.

```
Router> enable
Router# configure terminal
Router(config)# policy-map policymap1
Router(config-pmap)# class class1
Router(config-pmap-c)# random-detect clp 1 12 25 1/10
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# exit
```

Related Commands

Command	Description
random-detect atm-clp-based	Enables WRED on the basis of the ATM CLP of a packet.
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

To specify the class of service (CoS) value of a packet, the minimum and maximum thresholds, and the maximum probability denominator used for enabling weighted random early detection (WRED), use the **random-detect cos** command in policy-map class configuration mode. To reset the thresholds and maximum probability denominator to the default values for the specified CoS, use the **no** form of this command.

random-detect cos *cos-value min-threshold max-threshold max-probability-denominator*

no random-detect cos *cos-value min-threshold max-threshold max-probability-denominator*

Syntax Description

cos-value	Specific IEEE 802.1Q CoS value from 0 to 7.
min-threshold	Minimum threshold in number of packets. Valid values are 1 to 4096.
max-threshold	Maximum threshold in number of packets. Valid values are 1 to 4096.
max-probability-denominator	Denominator for the fraction of packets dropped when the average queue depth is at the maximum threshold. Valid values are 1 to 65535.

Defaults

The default values for the *min-threshold* and *max-threshold* arguments are based on the output buffering capacity and the transmission speed for the interface.

The default value for the *max-probability-denominator* argument is 10; 1 out of every 10 packets is dropped at the maximum threshold.

Command Modes

Policy-map class configuration

Command History

Release	Modification
12.0(28)S	This command was introduced.
12.2(27)SBA	This command was integrated into Cisco IOS Release 12.2(27)SBA.

Usage Guidelines

Note the following points when using the **random-detect cos** command:

- When the average queue length reaches the minimum threshold, WRED randomly drops some packets with the specified IP precedence.
- When the average queue length exceeds the maximum threshold, WRED drops all packets with the specified IP precedence.
- The *max-probability-denominator* argument is 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.

Examples

In the following example, WRED has been enabled using the **random-detect cos** command. With the **random-detect cos** command, the CoS value has been specified, along with the minimum and maximum thresholds, and the maximum probability denominator.

```
Router> enable
Router# configure terminal
Router(config)# policy-map policymap1
Router(config-pmap)# class class1
Router(config-pmap-c)# random-detect cos 1 12 25 1/10
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# exit
```

Related Commands

Command	Description
random-detect atm-clp-based	Configures 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-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 *cos-value*

Syntax Description

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

Defaults

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

Command History

Release	Modification
12.0(28)S	This command was introduced.
12.2(27)SBA	This command was integrated into Cisco IOS Release 12.2(27)SBA.

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)# exit
Router(config-pmap)# exit
Router(config)# exit
```

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 policy-map configuration mode. To disable this feature, use the **no** form of this command.

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

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

Syntax Description

value	Discard class. Valid values are 0 to 7.
min-threshold	Minimum threshold in number of packets. Valid values are 1 to 4096. When the average queue length reaches the minimum threshold, WRED randomly drops some packets with the specified IP precedence.
max-threshold	Maximum threshold in number of packets. Valid values are 1 to 4096. When the average queue length exceeds the maximum threshold, WRED drops all packets with the specified IP precedence.
mark-prob-denominator	Denominator for the fraction of packets dropped when the average queue depth is at the maximum threshold. For example, if the denominator is 512, 1 out of every 512 packets is dropped when the average queue is at the maximum threshold. Valid values are 1 to 65535. The default is 10; 1 out of every 10 packets is dropped at the maximum threshold.

Defaults

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

Command Modes

Policy-map configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.2(27)SBA	This command was integrated into Cisco IOS Release 12.2(27)SBA.

Usage Guidelines

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

Examples

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

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

```
random-detect-discard-class 2 100 200 10
```

Related Commands

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

random-detect discard-class-based

To base weighted random early detection (WRED) on the discard class value of a packet, use the **random-detect discard-class-based** command in policy-map 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 configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.2(27)SBA	This command was integrated into Cisco IOS Release 12.2(27)SBA.

Usage Guidelines

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

Examples

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

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

Related Commands

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

random-detect dscp

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

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

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

Syntax Description

dscpvalue	Specifies the DSCP value. The DSCP value can be a number from 0 to 63, or it can be one of the following keywords: **ef**, **af11**, **af12**, **af13**, **af21**, **af22**, **af23**, **af31**, **af32**, **af33**, **af41**, **af42**, **af43**, **cs1**, **cs2**, **cs3**, **cs4**, **cs5**, or **cs7**.
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) 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 drops all packets with the specified DSCP value.
mark-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.

Defaults

If WRED is using the DSCP value to calculate the drop probability of a packet, all entries of the DSCP table are initialized with the default settings shown in Table 2 in the “Usage Guidelines” section of this command.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(5)T	This command was introduced.
12.2(27)SBA	This command was integrated into Cisco IOS Release 12.2(27)SBA.

Usage Guidelines

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

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

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

Table 2 lists the default settings used by the **random-detect dscp** command for the DSCP value specified. Table 2 lists the DSCP value, and its corresponding minimum threshold, maximum threshold, and mark probability. The last row of the table (the row labeled “default”) shows the default settings used for any DSCP value not specifically shown in the table.

Table 2 random-detect dscp Default Settings

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

Examples

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

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

Related Commands

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

random-detect dscp-based

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

random-detect dscp-based

no random-detect dscp-based

Syntax Description

This command has no arguments or keywords.

Defaults

The defaults are platform-dependent.

Command Modes

Policy-map class configuration

Command History

Release	Modification
12.0(28)S	This command was introduced.
12.2(27)SBA	This command was integrated into Cisco IOS Release 12.2(27)SBA.

Usage Guidelines

With the **random-detect dscp-based** command, WRED is based on the DSCP value of the packet.

Use the **random-detect dscp-based** command before configuring the **random-detect dscp** command.

Examples

The following example shows that random detect is based on the DSCP 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 dscp-based
Router(config-pmap-c)# random-detect dscp af22 512 ms 1020 ms
Router(config-pmap-c)# exit
```

Related Commands

Command	Description
random-detect	Enables WRED or DWRED.
random-detect dscp	Configures the WRED parameters for a particular DSCP value; configures the WRED parameters for a particular DSCP value for a class policy in a policy map.

random-detect prec-based

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.

Defaults

The defaults are platform-dependent.

Command Modes

Policy-map class configuration

Command History

Release	Modification
12.0(28)S	This command was introduced.
12.2(27)SBA	This command was integrated into Cisco IOS Release 12.2(27)SBA.

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.

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 prec-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

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

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

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

Syntax Description

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 3 in the “Usage Guidelines” section of this command.
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.
mark-prob-denominator	Denominator for the fraction of packets dropped when the average queue depth is at the maximum threshold. For example, if the denominator is 512, 1 out of every 512 packets is dropped when the average queue is at the maximum threshold. The value range is from 1 to 65536. The default is 10; 1 out of every 10 packets is dropped at the maximum threshold.

Defaults

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

The default *min-threshold* depends on the precedence. The *min-threshold* for IP Precedence 0 corresponds to half of the *max-threshold*. The values for the remaining precedences fall between half the *max-threshold* and the *max-threshold* at evenly spaced intervals. See Table 3 in the “Usage Guidelines” section of this command for a list of the default minimum threshold values for each IP Precedence.

Command Modes

Interface configuration when used on an interface

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

Command History

Release	Modification
11.1 CC	This command was introduced.
12.2(27)SBA	This command was integrated into Cisco IOS Release 12.2(27)SBA.

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

Table 3 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 Switching Services Configuration Guide* and the *Cisco IOS Switching Services Command Reference*.

Note The DWRED feature is not supported in a class policy.

Examples

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

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

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

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

Related Commands

Command	Description
bandwidth (policy-map class)	Specifies or modifies the bandwidth allocated for a class belonging to a policy map.
fair-queue (class-default)	Specifies the number of dynamic queues to be reserved for use by the class-default class as part of the default class policy.
random-detect dscp	Changes the minimum and maximum packet thresholds for the DSCP value.
random-detect (per VC)	Enables per-VC WRED or per-VC DWRED.
random-detect exponential-weighting-constant	Configures the WRED and DWRED exponential weight factor for the average queue size calculation.
random-detect flow count	Sets the flow count for flow-based WRED.
show policy-map interface	Displays the configuration of all classes configured for all service policies on the specified interface or displays the classes for the service policy for a specific PVC on the interface.
show queue	Displays the contents of packets inside a queue for a particular interface or VC.
show queueing	Lists all or selected configured queueing strategies.

show policy-map

To display the configuration of all classes for a specified service policy map or all classes for all existing policy maps, use the **show policy-map** command in EXEC mode.

show policy-map [*policy-map*]

Syntax Description

policy-map	(Optional) Name of the service policy map whose complete configuration is to be displayed.

Defaults

All existing policy map configurations are displayed.

Command Modes

EXEC

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.
12.0(7)S	This command was integrated into Cisco IOS Release 12.0(7)S.
12.1(1)E	This command was integrated into Cisco IOS Release 12.1(1)E.
12.2(13)T	The output of this command was modified for the Percentage-Based Policing and Shaping feature and includes the bandwidth percentage used when calculating traffic policing and shaping.
12.0(28)S	The output of this command was modified for the QoS: Percentage-Based Policing feature to display the committed (conform) burst (bc) and excess (peak) burst (be) sizes in milliseconds (ms).
12.2(27)SBA	This command was integrated into Cisco IOS Release 12.2(27)SBA.

Usage Guidelines

The **show policy-map** command displays the configuration of a service policy map created using the **policy-map** command. You can use the **show policy-map** command to display all class configurations comprising any existing service policy map, whether or not that service policy map has been attached to an interface.

Examples

The following is sample output from the **show policy-map** command. This sample output displays the contents of a policy map called “policy1.” In policy 1, traffic policing on the basis of a committed information rate (CIR) of 20 percent has been configured, and the bc and be have been specified in milliseconds. As part of the traffic policing configuration, optional conform, exceed, and violate actions have been specified.

```
Router# show policy-map policy1
  Policy Map policy1
    Class class1
     police cir percent 20 bc 300 ms pir percent 40 be 400 ms
```

```
conform-action transmit
exceed-action drop
violate-action drop
```

Table 4 describes the significant fields shown in the display.

Table 4 show policy-map Field Descriptions

Field	Description
Policy Map	Name of policy map displayed.
Class	Name of class configured in policy map displayed.
police	Indicates that traffic policing on the basis of specified percentage of bandwidth has been enabled. The committed burst (bc) and excess burst (be) sizes have been specified in milliseconds (ms), and optional conform, exceed, and violate actions have been specified.

Related Commands

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

show policy-map interface

To display the packet statistics of all classes that are configured for all service policies either on the specified interface or subinterface or on a specific permanent virtual circuit (PVC) on the interface, use the **show policy-map interface** command in EXEC mode.

show policy-map interface *interface-name* [**vc** [*vpi/*] *vci*][**dlci** *dlci*] [**input** | **output**]

Syntax Description

interface-name	Name of the interface or subinterface whose policy configuration is to be displayed.
vc	(Optional) For ATM interfaces only, shows the policy configuration for a specified PVC. The name can be up to 16 characters long.
vpi/	(Optional) ATM network virtual path identifier (VPI) for this PVC. On the Cisco 7200 and 7500 series routers, this value ranges from 0 to 255. The absence of both the forward slash (/) and a *vpi* value defaults the *vpi* value to 0. If this value is omitted, information for all virtual circuits (VCs) on the specified ATM interface or subinterface is displayed. The *vpi* and *vci* arguments cannot both be set to 0; if one is 0, the other cannot be 0.
vci	(Optional) ATM network virtual channel identifier (VCI) for this PVC. This value ranges from 0 to 1 less than the maximum value set for this interface by the **atm vc-per-vp** command. Typically, the lower values 0 to 31 are reserved for specific traffic (F4 Operation, Administration, and Maintenance (OAM), switched virtual circuit (SVC) signaling, Integrated Local Management Interface (ILMI), and so on) and should not be used. The VCI is a 16-bit field in the header of the ATM cell. The VCI value is unique only on a single link, not throughout the ATM network, because it has local significance only. The *vpi* and *vci* arguments cannot both be set to 0; if one is 0, the other cannot be 0.
dlci	(Optional) Indicates a specific PVC for which policy configuration will be displayed.
dlci	(Optional) Specific data-link connection identifier (DLCI) number used on the interface. Policy configuration for the corresponding PVC will be displayed when a DLCI is specified.
input	(Optional) Indicates that the statistics for the attached input policy will be displayed.
output	(Optional) Indicates that the statistics for the attached output policy will be displayed.

Defaults

No default behavior or values

Command Modes

EXEC

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.
12.0(7)S	This command was integrated into Cisco IOS Release 12.0(7)S.
12.1(1)E	This command was integrated into Cisco IOS Release 12.1(1)E.
12.1(2)T	This command was modified to display information about the policy for all Frame Relay PVCs on the interface, or, if a DLCI is specified, the policy for that specific PVC. This command was also modified to display the total number of packets marked by the QoS set action.
12.1(3)T	This command was modified to display per-class accounting statistics.
12.2(4)T	This command was modified to display burst parameters and associated actions.
12.2(8)T	This command was modified to display the multiple actions configured for packets conforming to, exceeding, or violating a specific rate.
12.0(28)S	The output of this command was modified for the QoS: Percentage-Based Policing feature to include milliseconds when calculating the committed (conform) burst (bc) and excess (peak) burst (be) sizes.
12.2(27)SBA	This command was integrated into Cisco IOS Release 12.2(27)SBA.

Usage Guidelines

The **show policy-map interface** command displays the configuration for classes on the specified interface or the specified PVC only if a service policy has been attached to the interface or the PVC.

Examples

The following is sample output from the **show policy-map interface** command. This sample displays the statistics for the serial 2/0 interface on which traffic policing has been enabled. The committed (conform) burst (bc) and excess (peak) burst (be) are specified in milliseconds (ms).

```
Router# show policy-map interface s2/0
 Serial2/0

  Service-policy output: policy1 (1050)

    Class-map: class1 (match-all) (1051/1)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: ip precedence 0  (1052)
      police:
          cir 20 % bc 300 ms
          cir 409500 bps, bc 15360 bytes
          pir 40 % be 400 ms
          pir 819000 bps, be 40960 bytes
        conformed 0 packets, 0 bytes; actions:
          transmit
        exceeded 0 packets, 0 bytes; actions:
          drop
        violated 0 packets, 0 bytes; actions:
          drop
        conformed 0 bps, exceed 0 bps, violate 0 bps

    Class-map: class-default (match-any) (1054/0)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any  (1055)
        0 packets, 0 bytes
        5 minute rate 0 bps
```

In this example, the CIR and PIR are displayed in bps, and both the committed burst (bc) and excess burst (be) are displayed in bits.

The CIR, PIR bc, and be are calculated on the basis of the formulas described below.

Formula for Calculating the CIR

When calculating the CIR, the following formula is used:

- CIR percentage specified (as shown in the output of the **show policy-map** command) * bandwidth (BW) of the interface (as shown in the output of the **show interfaces** command) = total bits per second

According to the output of the **show interfaces** command for the serial 2/0 interface, the interface has a bandwidth (BW) of 2048 kbps.

```
Router # show interfaces s2/0
Serial2/0 is administratively down, line protocol is down
  Hardware is M4T
  MTU 1500 bytes, BW 2048 Kbit, DLY 20000 usec, rely 255/255, load 1/255
```

The following values are used for calculating the CIR:

20 % * 2048 kbps = 409600 bps

Formula for Calculating the PIR

When calculating the PIR, the following formula is used:

- PIR percentage specified (as shown in the output of the **show policy-map** command) * bandwidth (BW) of the interface (as shown in the output of the **show interfaces** command) = total bits per second

According to the output of the **show interfaces** command for the serial 2/0 interface, the interface has a bandwidth (BW) of 2048 kbps.

```
Router # show interfaces s2/0
Serial2/0 is administratively down, line protocol is down
  Hardware is M4T
  MTU 1500 bytes, BW 2048 Kbit, DLY 20000 usec, rely 255/255, load 1/255
```

The following values are used for calculating the PIR:

40 % * 2048 kbps = 819200 bps

Note Discrepancies between this total and the total shown in the output of the **show policy-map interface** command can be attributed to a rounding calculation or to differences associated with the specific interface configuration.

Formula for Calculating the Committed Burst (bc)

When calculating the bc, the following formula is used:

- The bc in milliseconds (as shown in the **show policy-map** command) * the CIR in bits per seconds = total number bytes

The following values are used for calculating the bc:

300 ms * 409600 bps = 15360 bytes

Formula for Calculating the Excess Burst (be)

When calculating the bc and the be, the following formula is used:

- The be in milliseconds (as shown in the **show policy-map** command) * the PIR in bits per seconds = total number bytes

The following values are used for calculating the be:

400 ms * 819200 bps = 40960 bytes

Table 5 describes the significant fields shown in the display.

Table 5 show policy-map interface Field Descriptions[1]

Field	Description
Service-policy output	Name of the output service policy applied to the specified interface or VC.
Class-map	Class of traffic being displayed. Output is displayed for each configured class in the policy. The choice for implementing class matches (for example, match-all or match-any) can also appear next to the traffic class.
packets and bytes	Number of packets (also shown in bytes) identified as belonging to the class of traffic being displayed.
offered rate	Rate, in kbps, of packets coming in to the class.
drop rate	Rate, in kbps, at which packets are dropped from the class. The drop rate is calculated by subtracting the number of successfully transmitted packets from the offered rate.
Match	Match criteria specified for the class of traffic. Choices include criteria such as the Layer 3 packet length, IP precedence, IP differentiated services code point (DSCP) value, Multiprotocol Label Switching (MPLS) experimental value, access groups, and quality of service (QoS) groups. For more information about the variety of match criteria options that are available, refer to the "Configuring the Modular Quality of Service Command-Line Interface" chapter of the *Cisco IOS Quality of Service Solutions Configuration Guide*.
police	Indicates that traffic policing has been enabled. Display includes the CIR, PIR (in both a percentage of bandwidth and in bps) and the bc and be in bytes and milliseconds. Also displays the optional conform, exceed, and violate actions, if any, and the statistics associated with these optional actions.

[1] A number in parentheses may appear next to the service-policy output name, class-map name, and match criteria information. The number is for Cisco internal use only and can be disregarded.

Related Commands

Command	Description
police (percent)	Configures traffic policing on the basis of a percentage of bandwidth available on an interfaces.
shape (percent)	Specifies average or peak rate traffic shaping on the basis of a percentage of bandwidth available on an interface.
show frame-relay pvc	Displays statistics about PVCs for Frame Relay interfaces.
show interfaces	Displays statistics for all interfaces configured on the router or access server.
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 class	Displays the configuration for the specified class of the specified policy map.