# QoS: Congestion Avoidance Configuration Guide, Cisco IOS XE Gibraltar 16.10.x


**Americas Headquarters**
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com go trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2018 Cisco Systems, Inc. All rights reserved.

# CONTENTS


CHAPTER 1 **Read Me First** 1

Read Me First 1

CHAPTER 2 **Congestion Avoidance Overview** 3

Congestion Avoidance Overview 3

Finding Feature Information 3

Weighted Random Early Detection 3

About Random Early Detection 3

About WRED 6

CHAPTER 3 **IPv6 QoS: MQC WRED-Based Drop** 9

IPv6 QoS: MQC WRED-Based Drop 9

Finding Feature Information 9

Information About IPv6 QoS: MQC WRED-Based Drop 9

Implementation Strategy for QoS for IPv6 9

Congestion Avoidance for IPv6 Traffic 10

Additional References 10

Feature Information for IPv6 QoS: MQC WRED-Based Drop 11

CHAPTER 4 **Configuring Weighted Random Early Detection** 13

Configuring Weighted Random Early Detection 13

Finding Feature Information 13

About Weighted Random Early Detection 13

How to Configure WRED 14

Enabling WRED 14

Changing WRED Parameters 14

Monitoring WRED 15
WRED Configuration Examples 15
Example WRED Configuration 15
Example Parameter-Setting WRED 16
Feature Information for Configuring Weighted Random Early Detection 17

CHAPTER 5 **Byte-Based Weighted Random Early Detection 19**
Byte-Based Weighted Random Early Detection 19
Finding Feature Information 19
Restrictions for Byte-Based Weighted Random Early Detection 19
Information About Byte-Based Weighted Random Early Detection 19
Changes in functionality of WRED 19
Changes in Queue Limit and WRED Thresholds 20
How to Configure Byte-Based Weighted Random Early Detection 20
Configuring Byte-Based WRED 20
Configuring the Queue Depth and WRED Thresholds 21
Changing the Queue Depth and WRED Threshold Unit Modes 24
Verifying the Configuration for Byte-Based WRED 27
Configuration Examples for Byte-Based Weighted Random Early Detection 28
Example Configuring Byte-Based WRED 28
Additional References 29
Feature Information for Byte-Based Weighted Random Early Detection 30

CHAPTER 6 **WRED Explicit Congestion Notification 31**
WRED Explicit Congestion Notification 31
Finding Feature Information 31
Prerequisites for WRED-Explicit Congestion Notification 31
Information About WRED-Explicit Congestion Notification 31
WRED-Explicit Congestion Notification Feature Overview 31
How WRED Works 32
ECN Extends WRED Functionality 32
Benefits of WRED Explicit Congestion Notification 33
How to Configure WRED-Explicit Congestion Notification 33
Configuring Explicit Congestion Notification 33

Verifying the Explicit Congestion Notification Configuration 35
Configuration Examples for WRED-Explicit Congestion Notification 36
Example Enabling ECN 36
Example Verifying the ECN Configuration 36
Additional References 37
Feature Information for WRED Explicit Congestion Notification 38

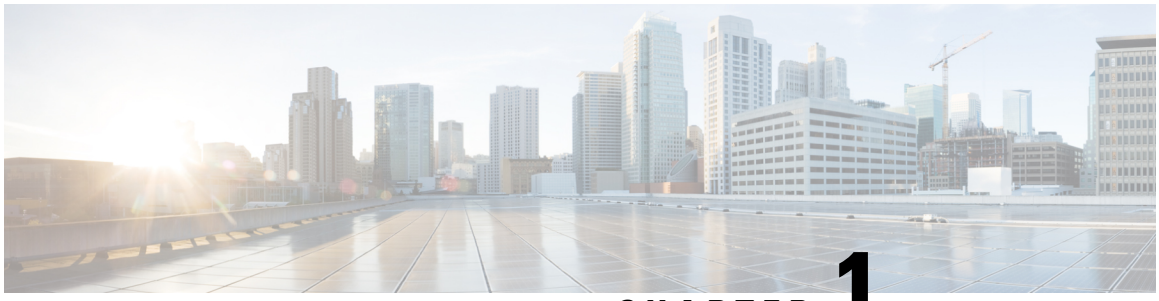
CHAPTER 7 **QoS Time-Based Thresholds for WRED and Queue Limit 41**
QoS Time-Based Thresholds for WRED and Queue Limit 41
Finding Feature Information 41
Prerequisites for QoS Time-Based Thresholds for WRED and Queue Limit 41
Restrictions for QoS Time-Based Thresholds for WRED and Queue Limit 41
Information About QoS Time-Based Thresholds for WRED and Queue Limit 42
Benefits of QoS Time-Based Thresholds for WRED and Queue Limit 42
Setting Thresholds by Using WRED 42
Setting Thresholds by Using the queue-limit Command 42
random-detect Commands with the Milliseconds Keyword 43
Mixing Threshold Units of Measure 43
How to Configure QoS Time-Based Thresholds for WRED and Queue Limit 43
Enabling WRED and Using WRED to Specify Thresholds 43
Using the queue-limit Command to Specify the Thresholds 45
Attaching the Policy Map to an Interface in a QoS Time-Based Threshold for WRED Configuration 46
Verifying the QoS Time-Based Thresholds for WRED and Queue Limit Configuration 48
Configuration Examples for QoS Time-Based Thresholds for WRED and Queue Limit 49
Example Using WRED to Set Thresholds 49
Example Using the queue-limit Command to Set Thresholds 50
Example Verifying the Configuration 50
Example WRED Threshold Configuration Sample Output 50
Example queue-limit command Threshold Configuration Sample Output 51
Additional References 52
Feature Information for QoS Time-Based Thresholds for WRED and Queue Limit 53

CHAPTER 8 **DiffServ Compliant WRED 55**

DiffServ Compliant WRED 55
Finding Feature Information 55
Information About DiffServ Compliant WRED 55
Differentiated Services for WRED 55
Usage Guidelines for DiffServ Compliant WRED 56
How to Configure DiffServ Compliant WRED 56
Configuring DiffServ Compliant WRED 56
Configuration Examples for DiffServ Compliant WRED 59
Example: DiffServ compliant WRED 59
Additional References 59
Feature Information for DiffServ Compliant WRED 60

CHAPTER 9 **Shaping on Dialer Interfaces 63**
Shaping on Dialer Interfaces 63
Finding Feature Information 63
Restrictions for Shaping on Dialer Interfaces 63
Information About Shaping on Dialer Interfaces 63
QoS on PPP Session on Dialer Interfaces 63
QoS Dialer Interface Topology 64
How to Configure Shaping on Dialer Interfaces 64
Configuring an Output Queueing Policy for Dialer Interfaces 64
Configuring QoS for PPPoEoA for Dialer Interfaces 67
Configuring QoS for PPPoE for Dialer Interfaces 70
Configuring QoS for PPPoA for Dialer Interfaces 72
Configuring QoS for Multiple Sessions on Dialer Interfaces 75
Applying CoS Values to a Dialer Interface 78
Configuration Examples for Shaping on Dialer Interfaces 80
Example: Configuring Output Queuing Policy for a Dialer Interface 80
Example: Configuring QoS for PPPoEoA for a Dialer Interface 80
Example: Configuring QoS for a PPPoE on a Dialer Interface 81
Example: Configuring QoS for PPPoA on a Dialer Interface 81
Example: Configuring QoS for Multiple Sessions on a Dialer Interface 82
Example: Applying CoS Values to a Dialer Interface 82
Additional References for Shaping on Dialer Interfaces 82

Feature Information for Shaping on Dialer Interfaces 83



CHAPTER 1

# Read Me First


- Read Me First, on page 1


# Read Me First

### Important Information about Cisco IOS XE 16

Effective Cisco IOS XE Release 3.7.0E (for Catalyst Switching) and Cisco IOS XE Release 3.17S (for Access and Edge Routing) the two releases evolve (merge) into a single version of converged release—the Cisco IOS XE 16—providing one release covering the extensive range of access and edge products in the Switching and Routing portfolio.

### Feature Information

Use Cisco Feature Navigator to find information about feature support, platform support, and Cisco software image support. An account on Cisco.com is not required.

### Related References

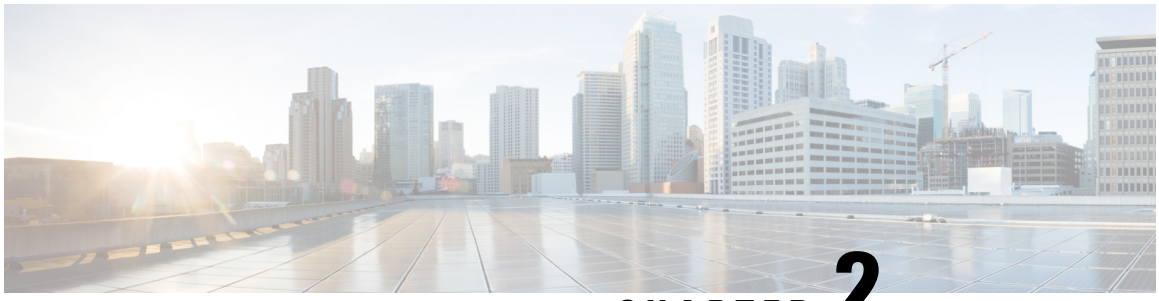
- Cisco IOS Command References, All Releases

### Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see What's New in Cisco Product Documentation.

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the What's New in Cisco Product Documentation RSS feed. RSS feeds are a free service.

Read Me First



CHAPTER 2

# Congestion Avoidance Overview


• Congestion Avoidance Overview, on page 3


# Congestion Avoidance Overview

Congestion avoidance techniques monitor network traffic loads in an effort to anticipate and avoid congestion at common network bottlenecks. Congestion avoidance is achieved through packet dropping. Among the more commonly used congestion avoidance mechanisms is Random Early Detection (RED), which is optimum for high-speed transit networks. Cisco IOS XE Software includes an implementation of RED, called Weighted RED (WRED), that combines the capabilities of the RED algorithm with the IP Precedence feature. WRED, when configured, controls when the router drops packets.

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

## Weighted Random Early Detection

WRED helps avoid the globalization problems that can occur. Global synchronization occurs as waves of congestion crest only to be followed by troughs during which the transmission link is not fully utilized. Global synchronization of TCP hosts, for example, can occur because packets are dropped all at once. Global synchronization manifests when multiple TCP hosts reduce their transmission rates in response to packet dropping and then increase their transmission rates once again when the congestion is reduced.

### About Random Early Detection

The RED mechanism was proposed by Sally Floyd and Van Jacobson in the early 1990s to address network congestion in a responsive rather than reactive manner. Underlying the RED mechanism is the premise that most traffic runs on data transport implementations that are sensitive to loss and will temporarily slow down when some of their traffic is dropped. TCP, which responds appropriately--even robustly--to traffic drop by

slowing down its traffic transmission, effectively allows the traffic-drop behavior of RED to work as a congestion-avoidance signalling mechanism.

TCP constitutes the most heavily used network transport. Given the ubiquitous presence of TCP, RED offers a widespread, effective congestion-avoidance mechanism.

In considering the usefulness of RED when robust transports such as TCP are pervasive, it is important to consider also the seriously negative implications of employing RED when a significant percentage of the traffic is not robust in response to packet loss. Neither Novell NetWare nor AppleTalk is appropriately robust in response to packet loss, therefore you should not use RED for them.

## How It Works

The DiffServ Compliant WRED feature enables WRED to use the DSCP value when it calculates the drop probability for a packet. The DSCP value is the first six bits of the IP type of service (ToS) byte.

This feature adds two new commands, **random-detect dscp** and **dscp**. It also adds two new arguments, *dscp-based* and *prec-based* **,** to two existing WRED-related commands--the **random-detect**(interface) command and the **random-detect-group** command.

The *dscp-based* argument enables WRED to use the DSCP value of a packet when it calculates the drop probability for the packet. The *prec-based* argument enables WRED to use the IP Precedence value of a packet when it calculates the drop probability for the packet.

These arguments are optional (you need not use any of them to use the commands) but they are also mutually exclusive. That is, if you use the *dscp-based* argument, you cannot use the *prec-based* argument with the same command.

After enabling WRED to use the DSCP value, you can then use the new **random-detect dscp** command to change the minimum and maximum packet thresholds for that DSCP value.

Three scenarios for using these arguments are provided.

## Packet Drop Probability

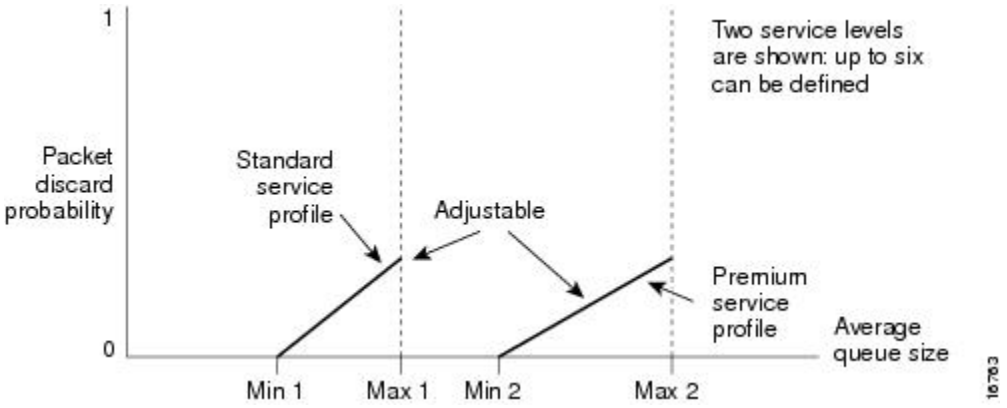
The packet drop probability is based on the minimum threshold, maximum threshold, and mark probability denominator.

When the average queue depth is above the minimum threshold, RED starts dropping packets. The rate of packet drop increases linearly as the average queue size increases until the average queue size reaches the maximum threshold.

The mark probability denominator is the fraction of packets dropped when the average queue depth is at the maximum threshold. For example, if the denominator is 512, one out of every 512 packets is dropped when the average queue is at the maximum threshold.

When the average queue size is above the maximum threshold, all packets are dropped. The figure below summarizes the packet drop probability.

*Figure 1: RED Packet Drop Probability*




The minimum threshold value should be set high enough to maximize the link utilization. If the minimum threshold is too low, packets may be dropped unnecessarily, and the transmission link will not be fully used.

The difference between the maximum threshold and the minimum threshold should be large enough to avoid global synchronization of TCP hosts (global synchronization of TCP hosts can occur as multiple TCP hosts reduce their transmission rates). If the difference between the maximum and minimum thresholds is too small, many packets may be dropped at once, resulting in global synchronization.

## How TCP Handles Traffic Loss

**Note** Both this section and How the Router Interacts with TCP, on page 6 contain detailed information that you need not read in order to use WRED or to have a general sense of the capabilities of RED. If you want to understand why problems of global synchronization occur in response to congestion and how RED addresses them, read these sections.

When the recipient of TCP traffic--called the receiver--receives a data segment, it checks the four octet (32-bit) sequence number of that segment against the number the receiver expected, which would indicate that the data segment was received in order. If the numbers match, the receiver delivers all of the data that it holds to the target application, then it updates the sequence number to reflect the next number in order, and finally it either immediately sends an acknowledgment (ACK) packet to the sender or it schedules an ACK to be sent to the sender after a short delay. The ACK notifies the sender that the receiver received all data segments up to but not including the one marked with the new sequence number.

Receivers usually try to send an ACK in response to alternating data segments they receive; they send the ACK because for many applications, if the receiver waits out a small delay, it can efficiently include its reply acknowledgment on a normal response to the sender. However, when the receiver receives a data segment out of order, it immediately responds with an ACK to direct the sender to resend the lost data segment.

When the sender receives an ACK, it makes this determination: It determines if any data is outstanding. If no data is outstanding, the sender determines that the ACK is a keepalive, meant to keep the line active, and it does nothing. If data is outstanding, the sender determines whether the ACK indicates that the receiver has received some or none of the data. If the ACK indicates receipt of some data sent, the sender determines if new credit has been granted to allow it to send more data. When the ACK indicates receipt of none of the data sent and there is outstanding data, the sender interprets the ACK to be a repeatedly sent ACK. This condition indicates that some data was received out of order, forcing the receiver to remit the first ACK, and that a

second data segment was received out of order, forcing the receiver to remit the second ACK. In most cases, the receiver would receive two segments out of order because one of the data segments had been dropped.

When a TCP sender detects a dropped data segment, it resends the segment. Then it adjusts its transmission rate to half of what is was before the drop was detected. This is the TCP back-off or slow-down behavior. Although this behavior is appropriately responsive to congestion, problems can arise when multiple TCP sessions are carried on concurrently with the same router and all TCP senders slow down transmission of packets at the same time.

### How the Router Interacts with TCP

**Note** The sections How TCP Handles Traffic Loss, on page 5 and How TCP Handles Traffic Loss, on page 5 contain detailed information that you need not read in order to use WRED or to have a general sense of the capabilities of RED. If you want to understand why problems of global synchronization occur in response to congestion and how RED addresses them, read these sections.

To see how the router interacts with TCP, we will look at an example. In this example, on average, the router receives traffic from one particular TCP stream every other, every 10th, and every 100th or 200th message in the interface in MAE-EAST or FIX-WEST. A router can handle multiple concurrent TCP sessions. Because network flows are additive, there is a high probability that when traffic exceeds the Transmit Queue Limit (TQL) at all, it will vastly exceed the limit. However, there is also a high probability that the excessive traffic depth is temporary and that traffic will not stay excessively deep except at points where traffic flows merge or at edge routers.

If the router drops all traffic that exceeds the TQL, many TCP sessions will simultaneously go into slow start. Consequently, traffic temporarily slows down to the extreme and then all flows slow-start again; this activity creates a condition of global synchronization.

However, if the router drops no traffic, as is the case when queueing features such as fair queueing or priority queueing (PQ) are used, then the data is likely to be stored in main memory, drastically degrading router performance.

By directing one TCP session at a time to slow down, RED solves the problems described, allowing for full utilization of the bandwidth rather than utilization manifesting as crests and troughs of traffic.

## About WRED

WRED combines the capabilities of the 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.

You can configure WRED to ignore IP precedence when making drop decisions so that nonweighted RED behavior is achieved.

For interfaces configured to use the Resource Reservation Protocol (RSVP) feature, WRED chooses packets from other flows to drop rather than the RSVP flows. Also, IP Precedence governs which packets are dropped--traffic that is at a lower precedence has a higher drop rate and therefore is more likely to be throttled back.

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.

## Why Use WRED

WRED makes early detection of congestion possible and provides for multiple classes of traffic. It also protects against global synchronization. For these reasons, WRED is useful on any output interface where you expect congestion to occur.

However, WRED is usually used in the core routers of a network, rather than at the edge of the network. Edge routers assign IP precedences to packets as they enter the network. WRED uses these precedences to determine how to treat different types of traffic.

WRED provides separate thresholds and weights for different IP precedences, allowing you to provide different qualities of service in regard to packet dropping for different traffic types. Standard traffic may be dropped more frequently than premium traffic during periods of congestion.

WRED is also RSVP-aware, and it can provide the controlled-load QoS service of integrated service.

## How It Works

By randomly dropping packets prior to periods of high congestion, WRED tells the packet source to decrease its transmission rate. If the packet source is using TCP, it will decrease its transmission rate until all the packets reach their destination, which indicates that the congestion is cleared.

WRED generally drops packets selectively based on IP precedence. Packets with a higher IP precedence are less likely to be dropped than packets with a lower precedence. Thus, the higher the priority of a packet, the higher the probability that the packet will be delivered.

WRED selectively drops packets when the output interface begins to show signs of congestion. By dropping some packets early rather than waiting until the queue is full, WRED avoids dropping large numbers of packets at once and minimizes the chances of global synchronization. Thus, WRED allows the transmission line to be used fully at all times.

In addition, WRED statistically drops more packets from large users than small. Therefore, traffic sources that generate the most traffic are more likely to be slowed down than traffic sources that generate little traffic.

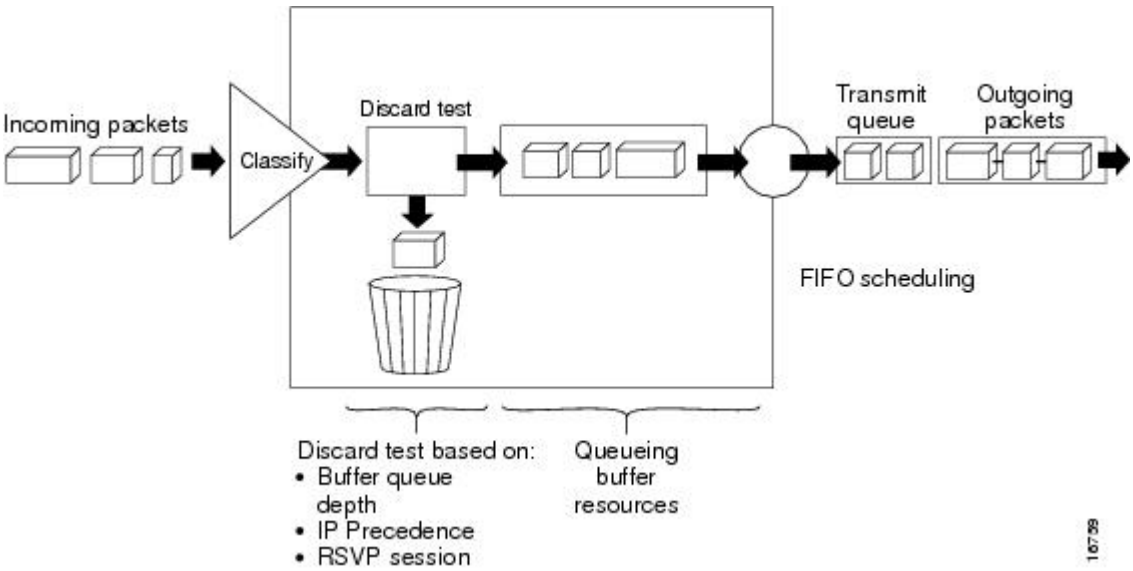
WRED helps to avoid the globalization problems. Global synchronization manifests when multiple TCP hosts reduce their transmission rates in response to packet dropping and then increase their transmission rates once again when the congestion is reduced.

WRED is only useful when the bulk of the traffic is TCP/IP traffic. With TCP, dropped packets indicate congestion, so the packet source will reduce its transmission rate. With other protocols, packet sources may not respond or may resend dropped packets at the same rate. Thus, dropping packets does not decrease congestion.

WRED treats non-IP traffic as precedence 0, the lowest precedence. Therefore, non-IP traffic, in general, is more likely to be dropped than IP traffic.

The figure below illustrates how WRED works.

*Figure 2: Weighted Random Early Detection*




## Average Queue Size

The average queue size is based on the previous average and the current size of the queue. The formula is:

```
average = (old_average * (1-1/2^n)) + (current_queue_size * 1/2^n)
```

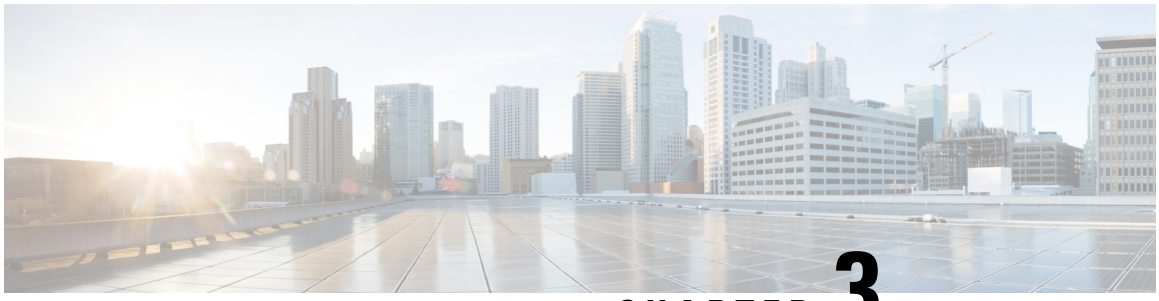
where *n* is the exponential weight factor, a user-configurable value.

For high values of *n*, the previous average queue size becomes more important. A large factor smooths out the peaks and lows in queue length. The average queue size is unlikely to change very quickly, avoiding drastic swings in size. The WRED process will be slow to start dropping packets, but it may continue dropping packets for a time after the actual queue size has fallen below the minimum threshold. The slow-moving average will accommodate temporary bursts in traffic.

**Note** If the value of *n* gets too high, WRED will not react to congestion. Packets will be sent or dropped as if WRED were not in effect.

For low values of *n*, the average queue size closely tracks the current queue size. The resulting average may fluctuate with changes in the traffic levels. In this case, the WRED process responds quickly to long queues. Once the queue falls below the minimum threshold, the process stops dropping packets.

If the value of *n* gets too low, WRED will overreact to temporary traffic bursts and drop traffic unnecessarily.



CHAPTER 3

# IPv6 QoS: MQC WRED-Based Drop


- IPv6 QoS: MQC WRED-Based Drop, on page 9


# IPv6 QoS: MQC WRED-Based Drop

WRED implements the RED-based drop policy on the packets that are likely to overflow the limits of CBWFQ.

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

## Information About IPv6 QoS: MQC WRED-Based Drop

### Implementation Strategy for QoS for IPv6

IPv6 packets are forwarded by paths that are different from those for IPv4. QoS features supported for IPv6 environments include packet classification, queuing, traffic shaping, weighted random early detection (WRED), class-based packet marking, and policing of IPv6 packets. These features are available at both the process switching and Cisco Express Forwarding switching paths of IPv6.

All of the QoS features available for IPv6 environments are managed from the modular QoS command-line interface (MQC). The MQC allows you to define traffic classes, create and configure traffic policies (policy maps), and then attach those traffic policies to interfaces.

To implement QoS in networks that are running IPv6, follow the same steps that you would follow to implement QoS in networks running only IPv4. At a very high level, the basic steps for implementing QoS are as follows:

- Know which applications in your network need QoS.
- Understand the characteristics of the applications so that you can make decisions about which QoS features would be appropriate.

- Know your network topology so that you know how link layer header sizes are affected by changes and forwarding.
- Create classes based on the criteria that you establish for your network. In particular, if the same network is also carrying IPv4 traffic along with IPv6 traffic, decide if you want to treat both of them the same way or treat them separately and specify match criteria accordingly. If you want to treat them the same, use match statements such as **match precedence**, **match dscp**, **set precedence**, and **set dscp**. If you want to treat them separately, add match criteria such as **match protocol ip** and **match protocol ipv6** in a match-all class map.
- Create a policy to mark each class.
- Work from the edge toward the core in applying QoS features.
- Build the policy to treat the traffic.
- Apply the policy.

## Congestion Avoidance for IPv6 Traffic

WRED implements the RED-based drop policy on the packets that are likely to overflow the limits of class-based weighted fair queueing (CBWFQ). WRED supports class-based and flow-based queueing (using DSCP or precedence values).

# Additional References

### Related Documents

| Related Topic | Document Title |
|---|---|
| Cisco IOS commands | *Cisco IOS Master Command List, All Releases* |
| IPv6 addressing and connectivity | *IPv6 Configuration Guide* |
| IPv6 commands | *Cisco IOS IPv6 Command Reference* |
| Cisco IOS IPv6 features | *Cisco IOS IPv6 Feature Mapping* |

### Technical Assistance

| Description | Link |
|---|---|
| The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password. | http://www.cisco.com/cisco/web/support/index.html |

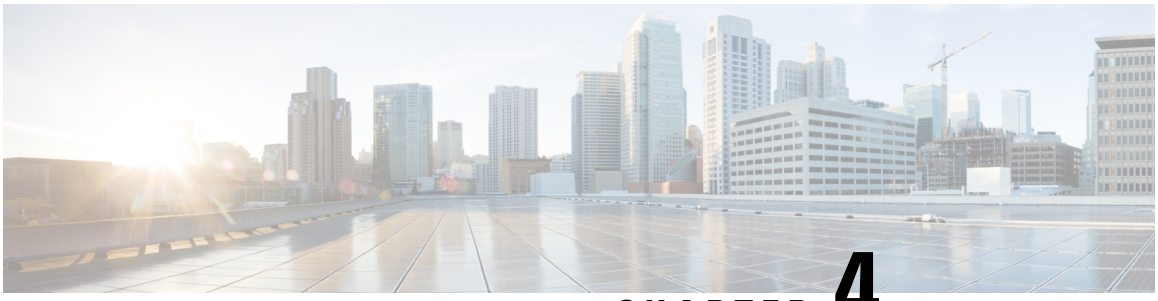
# Feature Information for IPv6 QoS: MQC WRED-Based Drop

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

***Table 1: Feature Information for IPv6 QoS: MQC WRED-Based Drop***

| Feature Name | Releases | Feature Information |
|---|---|---|
| IPv6 QoS: MQC WRED-Based Drop | Cisco IOS XE Release 2.1 | WRED implements the RED-based drop policy on the packets that are likely to overflow the limits of CBWFQ. |



CHAPTER 4

# Configuring Weighted Random Early Detection


• Configuring Weighted Random Early Detection, on page 13


# Configuring Weighted Random Early Detection

This module describes the tasks for configuring Weighted Random Early Detection (WRED) on a router.

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

## About Weighted Random Early Detection

Random Early Detection (RED) is a congestion avoidance mechanism that takes advantage of the congestion control mechanism of TCP. By randomly dropping packets prior to periods of high congestion, RED tells the packet source to decrease its transmission rate. WRED drops packets selectively based on IP precedence. Edge routers assign IP precedences to packets as they enter the network. (WRED is useful on any output interface where you expect to have congestion. However, WRED is usually used in the core routers of a network, rather than at the edge.) WRED uses these precedences to determine how it treats different types of traffic.

When a packet arrives, the following events occur:

1. The average queue size is calculated.
2. If the average is less than the minimum queue threshold, the arriving packet is queued.
3. If the average is between the minimum queue threshold for that type of traffic and the maximum threshold for the interface, the packet is either dropped or queued, depending on the packet drop probability for that type of traffic.
4. If the average queue size is greater than the maximum threshold, the packet is dropped.

**Note** WRED is useful with adaptive traffic such as TCP/IP. With TCP, dropped packets indicate congestion, so the packet source will reduce its transmission rate. With other protocols, packet sources may not respond or may resend dropped packets at the same rate. Thus, dropping packets does not decrease congestion. WRED treats non-IP traffic as precedence 0, the lowest precedence. Therefore, non-IP traffic is more likely to be dropped than IP traffic.

When you enable WRED with the **random-detect** interface configuration command, the parameters are set to their default values. The weight factor is 9. For all precedences, the mark probability denominator is 10, and maximum threshold is based on the output buffering capacity and the transmission speed for the interface.

The default minimum threshold depends on the precedence. The minimum threshold for IP Precedence 0 corresponds to half of the maximum threshold. The values for the remaining precedences fall between half the maximum threshold and the maximum threshold at evenly spaced intervals.

**Note** The default WRED 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 will benefit from the changed values.

# How to Configure WRED

## Enabling WRED

| Command | Purpose |
|---|---|
| `Router(config-if)# random-detect` | Enables WRED. |

## Changing WRED Parameters

| Command | Purpose |
|---|---|
| `Router(config-if)# random-detect exponential-weighting-constant` *exponent* | Configures the weight factor used in calculating the average queue length. |
| `Router(config-if)# random-detect precedence` *precedence min-threshold max-threshold mark-prob-denominator* | Configures parameters for packets with a specific IP Precedence. The minimum threshold for IP Precedence 0 corresponds to half the maximum threshold for the interface. Repeat this command for each precedence. To configure RED, rather than WRED, use the same parameters for each precedence. |

## Monitoring WRED

| Command | Purpose |
|---|---|
| `Router# show queue interface-type interface-number` | Displays the header information of the packets inside a queue. |
| `Router# show queueing interface interface-number [vc [[vpi/] vci]]` | Displays the WRED statistics of a specific virtual circuit (VC) on an interface. |
| `Router# show queueing random-detect` | Displays the queueing configuration for WRED. |
| `Router# show interfaces [type slot \| port-adapter \| port]` | Displays WRED configuration on an interface. |

# WRED Configuration Examples

## Example WRED Configuration

The following example enables WRED with default parameter values:

```
interface Serial5/0
 description to qos1-75a
 ip address 200.200.14.250 255.255.255.252
 random-detect
```

Use the **show interfaces** command output to verify the configuration. Notice that the "Queueing strategy" report lists "random early detection (RED)."

```
Router# show interfaces serial 5/0
Serial5/0 is up, line protocol is up
  Hardware is M4T
  Description: to qos1-75a
  Internet address is 200.200.14.250/30
  MTU 1500 bytes, BW 128 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 237/255
  Encapsulation HDLC, crc 16, loopback not set
  Keepalive not set
  Last input 00:00:15, output 00:00:00, output hang never
  Last clearing of "show interface" counters 00:05:08
  Input queue: 0/75/0 (size/max/drops); Total output drops: 1036
  Queueing strategy: random early detection(RED)
  5 minutes input rate 0 bits/sec, 2 packets/sec
  5 minutes output rate 119000 bits/sec, 126 packets/sec
     594 packets input, 37115 bytes, 0 no buffer
     Received 5 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     37525 packets output, 4428684 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions     DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
```

Use the **show queue** command output to view the current contents of the interface queue. Notice that there is only a single queue into which packets from all IP precedences are placed after dropping has taken place. The output has been truncated to show only three of the five packets.

```
Router# show queue serial 5/0

Output queue for Serial5/0 is 5/0
Packet 1, linktype: ip, length: 118, flags: 0x288
  source: 190.1.3.4, destination: 190.1.2.2, id: 0x0001, ttl: 254,
  TOS: 128 prot: 17, source port 11111, destination port 22222
    data: 0x2B67 0x56CE 0x005E 0xE89A 0xCBA9 0x8765 0x4321
          0x0FED 0xCBA9 0x8765 0x4321 0x0FED 0xCBA9 0x8765
Packet 2, linktype: ip, length: 118, flags: 0x288
  source: 190.1.3.5, destination: 190.1.2.2, id: 0x0001, ttl: 254,
  TOS: 160 prot: 17, source port 11111, destination port 22222
    data: 0x2B67 0x56CE 0x005E 0xE89A 0xCBA9 0x8765 0x4321
          0x0FED 0xCBA9 0x8765 0x4321 0x0FED 0xCBA9 0x8765
Packet 3, linktype: ip, length: 118, flags: 0x280
  source: 190.1.3.6, destination: 190.1.2.2, id: 0x0001, ttl: 254,
  TOS: 192 prot: 17, source port 11111, destination port 22222
    data: 0x2B67 0x56CE 0x005E 0xE89A 0xCBA9 0x8765 0x4321
          0x0FED 0xCBA9 0x8765 0x4321 0x0FED 0xCBA9 0x8765
```

Use the **show queueing** command output to view the current settings for each of the precedences. Also notice that the default minimum thresholds are spaced evenly between half and the entire maximum threshold. Thresholds are specified in terms of packet count.

```
Router# show queueing
Current random-detect configuration:
     Serial5/0
       Queueing strategy:random early detection (WRED)
       Exp-weight-constant:9 (1/512)
       Mean queue depth:28

       Class   Random       Tail    Minimum    Maximum     Mark
                 drop       drop  threshold  threshold  probability
         0        330          0         20         40     1/10
         1        267          0         22         40     1/10
         2        217          0         24         40     1/10
         3        156          0         26         40     1/10
         4         61          0         28         40     1/10
         5          6          0         31         40     1/10
         6          0          0         33         40     1/10
         7          0          0         35         40     1/10
        rsvp        0          0         37         40     1/10
```

## Example Parameter-Setting WRED

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
```

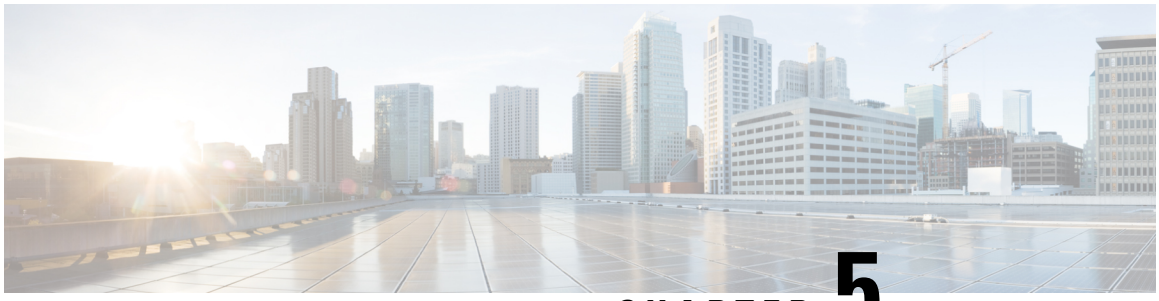
# Feature Information for Configuring Weighted Random Early Detection

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

***Table 2: Feature Information for Configuring Weighted Random Early Detection***

| Feature Name | Releases | Feature Information |
|---|---|---|
| Class-Based Weighted Fair Queueing (CBWFQ) and Weighted Random Early Detection (WRED) | Cisco IOS XE Release 2.1 | This feature was introduced on Cisco ASR 1000 Series Routers.<br>**Note** For information about CBWFQ, see the "Configuring Weighted Fair Queueing" module. |
| Random Early Detection (RED) | Cisco IOS XE Release 2.1 | This feature was introduced on Cisco ASR 1000 Series Routers. |
| Weighted Random Early Detection | Cisco IOS XE Release 2.1 | This feature was introduced on Cisco ASR 1000 Series Routers. |
| Weighted RED (WRED) | Cisco IOS XE Release 2.1 | This feature was introduced on Cisco ASR 1000 Series Routers. |



CHAPTER 5

# Byte-Based Weighted Random Early Detection


• Byte-Based Weighted Random Early Detection, on page 19


# Byte-Based Weighted Random Early Detection

This module explains how to enable byte-based Weighted Random Early Detection (WRED), and set byte-based queue limits and WRED thresholds.

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

## Restrictions for Byte-Based Weighted Random Early Detection

- WRED is only useful when the bulk of the traffic is TCP/IP traffic. With TCP, dropped packets indicate congestion, so the packet source will reduce its transmission rate. With other protocols, packet sources may not respond or may resend dropped packets at the same rate. Thus, dropping packets does not decrease congestion.
- You cannot configure byte-based WRED on a class in which the queue-limit is configured in milliseconds or packets.

## Information About Byte-Based Weighted Random Early Detection

### Changes in functionality of WRED

This feature extends the functionality of WRED. In previous releases, you specified the WRED actions based on the number of packets. With the byte-based WRED, you can specify WRED actions based on the number of bytes.

## Changes in Queue Limit and WRED Thresholds

In Cisco IOS XE Release 2.4, the Cisco ASR 1000 Series Aggregation Services Routers support the addition of bytes as a unit of configuration for both queue limits and WRED thresholds. Therefore, as of this release, packet-based and byte-based limits are configurable, with some restrictions.

# How to Configure Byte-Based Weighted Random Early Detection

## Configuring Byte-Based WRED

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **class-map** *class-map-name*
4. **match ip precedence** ip-precedence-value
5. exit
6. **policy-map** *policy-name*
7. **class** *class-name*
8. **random-detect**
9. **random-detect precedence** *precedence min-threshold* **bytes** *max-threshold* **bytes** *mark-prob-denominator*

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **class-map** *class-map-name*<br>**Example:**<br>`Router(config)# class-map c1` | Specifies the user-defined name of the traffic class. |
| **Step 4** | **match ip precedence** ip-precedence-value<br>**Example:**<br>`Router(config-cmap)# match ip precedence 1` | Specifies up to eight IP Precedence values used as match criteria. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 5** | exit<br>**Example:**<br>`Router(config-cmap)# exit` | Exits from class-map configuration mode. |
| **Step 6** | **policy-map** *policy-name*<br>**Example:**<br>`Router(config)# policy-map p1` | Specifies the name of the traffic policy to configure. |
| **Step 7** | **class** *class-name*<br>**Example:**<br>`Router(config-pmap)# class c1` | Specifies the name of a predefined traffic class, which was configured with the **class-map** command, used to classify traffic to the traffic policy. |
| **Step 8** | **random-detect**<br>**Example:**<br>`Router(config-pmap-c)# random-detect` | Enables WRED. |
| **Step 9** | **random-detect precedence** *precedence min-threshold* **bytes** *max-threshold* **bytes** *mark-prob-denominator*<br>**Example:**<br>**Example:**<br>`Router(config-pmap-c)# random-detect precedence 1 2000 bytes 3000 bytes 200` | Configures the parameters for bytes with a specific IP precedence. |

## Configuring the Queue Depth and WRED Thresholds

### Before you begin

Be sure that your configuration satisfies the following conditions when configuring the queue depth and WRED thresholds:

- When configuring byte-based mode, the queue limit must be configured prior to the WRED threshold and before the service policy is applied.
- When setting the queue depth and WRED thresholds in an enhanced QoS policies aggregation configuration, the limits are supported only for the default class at a subinterface policy map and for any classes at the main interface policy map.

**Note** Consider the following restrictions when you configure the queue depth and WRED thresholds:

- Do not configure the queue limit unit before you configure a queueing feature for a traffic class.
- If you do not configure a queue limit, then the default mode is packets.
- When you configure WRED thresholds, the following restrictions apply:
  - The WRED threshold must use the same unit as the queue limit. For example, if the queue limit is in packets, then the WRED thresholds also must be in packets.
  - If you do not configure a queue limit in bytes, then the default mode is packets and you must also configure the WRED threshold in packets.
  - The queue limit size must be greater than the WRED threshold.
- The unit modes for either the queue limit or WRED thresholds cannot be changed dynamically after a service policy is applied.

>

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map** *policy-map-name*
4. **class** *class-name*
5. *qos-queueing-feature*
6. **queue-limit** *queue-limit-size* [**bytes** | **packets**]
7. **random-detect** [**dscp-based** | **prec-based**]
8. Do one of the following:
   - **random-detect dscp** dscp-value {*min-threshold max-threshold* | *min-threshold* **bytes** *max-threshold* **bytes**} [*max-probability-denominator*]
   -
   -
   - **random-detect precedence** precedence {*min-threshold max-threshold* | *min-threshold* **bytes** *max-threshold* **bytes**} max-probability-denominator

## DETAILED STEPS

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

| | Command or Action | Purpose |
|---|---|---|
| | `Router# configure terminal` | |
| **Step 3** | **policy-map** *policy-map-name*<br>**Example:**<br>`Router(config)# policy-map main-interface` | Specifies the name of the traffic policy that you want to configure or modify and enters policy-map configuration mode. |
| **Step 4** | **class** *class-name*<br>**Example:**<br>`Router(config-pmap)# class AF1` | Specifies the name of the traffic class and enters policy-map class configuration mode. |
| **Step 5** | *qos-queueing-feature*<br>**Example:**<br>`Router(config-pmap-c)# bandwidth remaining ratio 90` | Enters a QoS configuration command. Some of the queueing features that are currently supported are **bandwidth**, **priority**, and **shape**.<br>**Note** Multiple QoS queueing commands can be entered at this step. However, due to dependencies between the queue limit and WRED thresholds, you should configure WRED after you configure the queue limit. |
| **Step 6** | **queue-limit** *queue-limit-size* [**bytes** \| **packets**]<br>**Example:**<br>`Router(config-pmap-c)# queue-limit 547500 bytes` | Specifies the maximum number (from 1 to 8192000) of bytes or packets that the queue can hold for this class. |
| **Step 7** | **random-detect** [**dscp-based** \| **prec-based**]<br>**Example:**<br>`Router(config-pmap-c)# random-detect dscp-based` | Enables WRED in either DSCP-based mode or precedence-based mode. |
| **Step 8** | Do one of the following:<br>• **random-detect dscp** dscp-value {*min-threshold max-threshold* \| *min-threshold* **bytes** *max-threshold* **bytes**} [*max-probability-denominator*]<br>•<br>•<br>• **random-detect precedence** precedence {*min-threshold max-threshold* \| *min-threshold* **bytes** *max-threshold* **bytes**} max-probability-denominator<br>**Example:**<br>`Router(config-pmap-c)# random-detect precedence 8 750000 bytes 750000 bytes` | Configures WRED parameters for a particular DSCP value or IP precedence.<br>**Note** Use the *min-threshold max-threshold* arguments without the **bytes** keyword to configure packet-based thresholds, when the **queue-limit** unit is also packets (the default). Alternatively, use these arguments with the **bytes** keyword when the **queue-limit** unit is configured in bytes. |

#### Examples

#### Correct Configuration

#### Invalid Configuration

#### Correct Configuration

#### Invalid Configuration

The following examples show both correct and invalid configurations to demonstrate some of the restrictions.

The following example shows the correct usage of setting the queue limit in bytes mode after the **bandwidth remaining ratio** queueing feature has been configured for a traffic class:

```
class AF1
 bandwidth remaining ratio 90
  queue-limit 750000 bytes
```

The following example shows an invalid configuration for the queue limit in bytes mode before the **bandwidth remaining ratio** queueing feature has been configured for a traffic class:

```
class AF1
 queue-limit 750000 bytes
  bandwidth remaining ratio 90
```

The following example shows the correct usage of setting the queue limit in bytes mode after the **bandwidth remaining ratio** queueing feature has been configured for a traffic class, followed by the setting of the thresholds for WRED in compatible byte mode:

```
class AF1
 bandwidth remaining ratio 90
  queue-limit 750000 bytes
   random-detect dscp-based
    random-detect dscp 8 750000 bytes 750000 bytes
```

This example shows an invalid configuration of the WRED threshold in bytes without any queue limit configuration, which therefore defaults to a packet-based queue depth. Therefore, the WRED threshold must also be in packets:

```
class AF1
 bandwidth remaining ratio 90
 random-detect dscp-based
 random-detect dscp 8 750000 bytes 750000 bytes
```

## Changing the Queue Depth and WRED Threshold Unit Modes

### SUMMARY STEPS

1. **enable**
2. **configure terminal**

3. **interface** *type number*
4. **no service-policy output** *policy-map-name*
5. **exit**
6. **policy-map** *policy-map-name*
7. **class** *class-name*
8. **queue-limit** *queue-limit-size* [**bytes** | **packets**]
9. Do one of the following:
   - **no random-detect dscp** *dscp-value* {*min-threshold max-threshold* | *min-threshold* **bytes** *max-threshold* **bytes**} [*max-probability-denominator*]
   -
   -
   - **no random-detect precedence** *precedence* {*min-threshold max-threshold* | *min-threshold* **bytes** *max-threshold* **bytes**} *max-probability-denominator*
10. Do one of the following:
    - **random-detect dscp** *dscp-value* {*min-threshold max-threshold* | *min-threshold* **bytes** *max-threshold* **bytes**} [*max-probability-denominator*]
    -
    -
    - **random-detect precedence** *precedence* {*min-threshold max-threshold*| *min-threshold* **bytes** *max-threshold* **bytes**} *max-probability-denominator*

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **interface** *type number*<br>**Example:**<br>`Router(config)# policy-map main-interface` | Specifies the interface where you want to remove a service policy, and enters interface configuration mode. |
| **Step 4** | **no service-policy output** *policy-map-name*<br>**Example:**<br>`Router(config-if)# no service-policy output main-interface-policy` | Removes a service policy applied to the specified interface. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 5** | **exit**<br>**Example:**<br>`Router(config-if)# exit` | Exits interface configuration mode and returns you to global configuration mode. |
| **Step 6** | **policy-map** *policy-map-name*<br>**Example:**<br>`Router(config)# policy-map main-interface-policy` | Specifies the name of the Traffic policy that you want to modify and enters policy-map configuration mode. |
| **Step 7** | **class** *class-name*<br>**Example:**<br>`Router(config-pmap)# class AF1` | Specifies the name of the traffic class and enters policy-map class configuration mode. |
| **Step 8** | **queue-limit** *queue-limit-size* [**bytes** \| **packets**]<br>**Example:**<br>`Router(config-pmap-c)# queue-limit 5000 packets` | Specifies the maximum number (from 1 to 8192000) of bytes or packets that the queue can hold for this class. |
| **Step 9** | Do one of the following:<br>• **no random-detect dscp** *dscp-value* {*min-threshold max-threshold* \| *min-threshold* **bytes** *max-threshold* **bytes**} [*max-probability-denominator*]<br>•<br>•<br>• **no random-detect precedence** *precedence* {*min-threshold max-threshold* \| *min-threshold* **bytes** *max-threshold* **bytes**} *max-probability-denominator*<br>**Example:**<br>`Router(config-pmap-c)# no random-detect dscp 8 750000 bytes 750000 bytes` | Removes the previously configured WRED parameters for a particular DSCP value or IP precedence. |
| **Step 10** | Do one of the following:<br>• **random-detect dscp** *dscp-value* {*min-threshold max-threshold* \| *min-threshold* **bytes** *max-threshold* **bytes**} [*max-probability-denominator*]<br>•<br>•<br>• **random-detect precedence** *precedence* {*min-threshold max-threshold*\| *min-threshold* **bytes** *max-threshold* **bytes**} *max-probability-denominator*<br>**Example:** | Configures WRED parameters for a particular DSCP value or IP precedence.<br>**Note** Use the *min-threshold max-threshold* arguments without the **bytes** keyword to configure packet-based thresholds, when the queue-limit unit is also packets (the default). Alternatively, use these arguments with the **bytes** keyword when the queue-limit unit is configured in bytes. |

| | Command or Action | Purpose |
|---|---|---|
| | `Router(config-pmap-c)# random-detect dscp 8 4000 4000` | |

### Examples

The following example shows how to change the queue depth and WRED thresholds to packet-based values once a service policy has been applied to an interface:

```
interface GigabitEthernet1/2/0
no service-policy output main-interface-policy
end
policy-map main-interface-policy
class AF1
 queue-limit 5000 packets
 no random-detect dscp 8 750000 bytes 750000 bytes
 random-detect dscp 8 4000 4000
```

## Verifying the Configuration for Byte-Based WRED

### SUMMARY STEPS

1. **show policy-map**
2. The **show policy-map interface** command shows output for an interface that is configured for byte-based WRED.

### DETAILED STEPS

**Step 1** **show policy-map**

The **show policy-map** command shows the output for a service policy called pol1 that is configured for byte-based WRED.

**Example:**

```
Router# show policy-map
Policy Map pol1
  Class class c1
Bandwidth 10 (%)
exponential weight 9
        class   min-threshold(bytes)   max-threshold(bytes)  mark-probability
        ----------------------------------------------------------------------

        0       -                     -                     1/10
        1       20000                 30000                 1/10
        2       -                     -                     1/10
        3       -                     -                     1/10
        4       -                     -                     1/10
        5       -                     -                     1/10
        6       -                     -                     1/10
        7       -                     -                     1/10
        rsvp    -                     -                     1/10
```

**Step 2** The **show policy-map interface** command shows output for an interface that is configured for byte-based WRED.

**Example:**

```
Router# show policy-map interface
serial3/1
Service-policy output: pol
Class-map: silver (match-all)
366 packets, 87840 bytes
30 second offered rate 15000 bps, drop rate 300 bps
Match: ip precedence 1
Queueing
Output Queue: Conversation 266
Bandwidth 10 (%)
(pkts matched/bytes matched) 363/87120
depth/total drops/no-buffer drops) 147/38/0
exponential weight: 9
mean queue depth: 25920
class     Transmitted       Random drop      Tail drop     Minimum Maximum Mark
          pkts/bytes        pkts/bytes       pkts/bytes    thresh  thresh  prob
                                                           (bytes)  (bytes)
0             0/0               0/0              0/0       20000    40000  1/10
1           328/78720         38/9120            0/0       22000    40000  1/10
2             0/0               0/0              0/0       24000    40000  1/10
3             0/0               0/0              0/0       26000    40000  1/10
4             0/0               0/0              0/0       28000    40000  1/10
```

# Configuration Examples for Byte-Based Weighted Random Early Detection

## Example Configuring Byte-Based WRED

The following example shows a service policy called wred-policy that sets up byte-based WRED for a class called prec2 and for the default class. The policy is then applied to Fast Ethernet interface 0/0/1.

```
policy wred-policy
 class prec2
   bandwidth 1000
   random-detect
   random-detect precedence 2 100 bytes 200 bytes 10
class class-default
   random-detect
   random-detect precedence 4 150 bytes 300 bytes 15
   random-detect precedence 6 200 bytes 400 bytes 5
interface fastethernet0/0/1
  service-policy output wred-policy
```

The following example shows the byte-based WRED results for the service policy attached to Ethernet interface 0/0/1.

```
Router# show policy-map interface
 Ethernet0/0/1
Service-policy output: wred-policy (1177)
Class-map: prec2 (match-all) (1178/10)
0 packets, 0 bytes
5 minute offered rate 0 bps, drop rate 0 bps
Match: ip precedence 2  (1179)
Queueing
```

```
queue limit 62500 bytes
(queue depth/total drops/no-buffer drops) 0/0/0
(pkts queued/bytes queued) 0/0
bandwidth 1000 (kbps)
Exp-weight-constant: 9 (1/512)
Mean queue depth: 0 bytes
class     Transmitted       Random drop      Tail drop Minimum        Maximum     Mark
          pkts/bytes        pkts/bytes       pkts/bytes thresh         thresh     prob
                                                        bytes         bytes
0             0/0               0/0              0/0     15625         31250     1/10
1             0/0               0/0              0/0     17578         31250     1/10
2             0/0               0/0              0/0       100           200     1/10
3             0/0               0/0              0/0     21484         31250     1/10
4             0/0               0/0              0/0     23437         31250     1/10
5             0/0               0/0              0/0     25390         31250     1/10
6             0/0               0/0              0/0     27343         31250     1/10
7             0/0               0/0              0/0     29296         31250     1/10
Class-map: class-default (match-any) (1182/0)
0 packets, 0 bytes
5 minute offered rate 0 bps, drop rate 0 bps
Match: any  (1183)
0 packets, 0 bytes
5 minute rate 0 bps
queue limit 562500 bytes
(queue depth/total drops/no-buffer drops) 0/0/0
(pkts queued/bytes queued) 0/0
Exp-weight-constant: 9 (1/512)
Mean queue depth: 0 bytes
class     Transmitted       Random drop      Tail drop Minimum        Maximum     Mark
          pkts/bytes        pkts/bytes       pkts/bytes thresh         thresh     prob
                                                        bytes         bytes
0             0/0               0/0              0/0    140625        281250     1/10
1             0/0               0/0              0/0    158203        281250     1/10
2             0/0               0/0              0/0    175781        281250     1/10
3             0/0               0/0              0/0    193359        281250     1/10
4             0/0               0/0              0/0       150           300     1/15
5             0/0               0/0              0/0    228515        281250     1/10
6             0/0               0/0              0/0       200           400     1/5
7             0/0               0/0              0/0    263671        281250     1/10
```

# Additional References

### Related Documents

| Related Topic | Document Title |
|---|---|
| QoS Commands | *Cisco IOS Quality of Service Solutions Command Reference* |
| Modular QoS CLI | Modular Quality of Service Command-Line Interface module |

### Standards

| Standard | Title |
|---|---|
| No new or modified standards are supported, and support for existing standards has not been modified. | -- |

### MIBs

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

### RFCs

| RFC | Title |
|---|---|
| No new or modified RFCs are supported, and support for existing RFCs has not been modified. | -- |

### Technical Assistance

| Description | Link |
|---|---|
| The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password. | http://www.cisco.com/cisco/web/support/index.html |

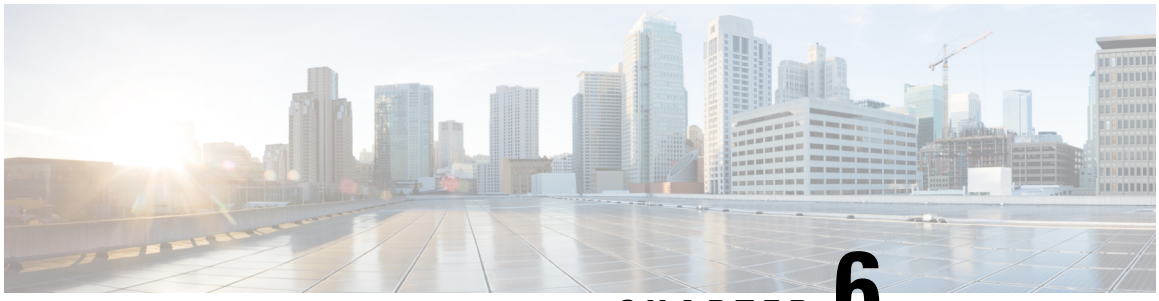
# Feature Information for Byte-Based Weighted Random Early Detection

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

***Table 3: Feature Information for Byte-Based Weighted Random Early Detection***

| Feature Name | Releases | Feature Information |
|---|---|---|
| Byte-Based Weighted Random Early Detection | Cisco IOS XE Release 2.4 | The Byte-Based Weighted Random Early Detection feature extends the functionality of WRED. In previous releases, you specified the WRED actions based on the number of packets. With the byte-based WRED, you can specify WRED actions based on the number of bytes.<br>This feature was introduced on Cisco ASR 1000 Series Routers.<br>The following commands were introduced or modified: **random-detect**, **random-detect precedence**, **show policy-map**, **show policy-map interface**. |



CHAPTER 6

# WRED Explicit Congestion Notification


- WRED Explicit Congestion Notification, on page 31


# WRED Explicit Congestion Notification

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

## Prerequisites for WRED-Explicit Congestion Notification

ECN must be configured through the Modular Quality of Service Command-Line Interface (MQC). For more information about the MQC, see the "Applying QoS Features Using the MQC" module.

## Information About WRED-Explicit Congestion Notification

### WRED-Explicit Congestion Notification Feature Overview

Currently, the congestion control and avoidance algorithms for Transmission Control Protocol (TCP) are based on the idea that packet loss is an appropriate indication of congestion on networks transmitting data using the best-effort service model. When a network uses the best-effort service model, the network delivers data if it can, without any assurance of reliability, delay bounds, or throughput. However, these algorithms and the best-effort service model are not suited to applications that are sensitive to delay or packet loss (for instance, interactive traffic including Telnet, web-browsing, and transfer of audio and video data). Weighted Random Early Detection (WRED), and by extension, Explicit Congestion Notification (ECN), helps to solve this problem.

RFC 3168, *The Addition of Explicit Congestion Notification (ECN) to IP*, states that with the addition of active queue management (for example, WRED) to the Internet infrastructure, routers are no longer limited to packet loss as an indication of congestion.

## How WRED Works

WRED makes early detection of congestion possible and provides a means for handling multiple classes of traffic. WRED can selectively discard lower priority traffic when the router begins to experience congestion and provide differentiated performance characteristics for different classes of service. It also protects against global synchronization. Global synchronization occurs as waves of congestion crest, only to be followed by periods of time during which the transmission link is not used to capacity. For these reasons, WRED is useful on any output interface or router where congestion is expected to occur.

WRED is implemented at the core routers of a network. Edge routers assign IP precedences to packets as the packets enter the network. With WRED, core routers then use these precedences to determine how to treat different types of traffic. WRED provides separate thresholds and weights for different IP precedences, enabling the network to provide different qualities of service, in regard to packet dropping, for different types of traffic. Standard traffic may be dropped more frequently than premium traffic during periods of congestion.

For more information about WRED, refer to the "Congestion Avoidance Overview" module.

## ECN Extends WRED Functionality

WRED drops packets, based on the average queue length exceeding a specific threshold value, to indicate congestion. ECN is an extension to WRED in that ECN marks packets instead of dropping them when the average queue length exceeds a specific threshold value. When configured with the WRED -- Explicit Congestion Notification feature, routers and end hosts would use this marking as a signal that the network is congested and slow down sending packets.

As stated in RFC 3168, *The Addition of Explicit Congestion Notification (ECN) to IP,* implementing ECN requires an ECN-specific field that has two bits--the ECN-capable Transport (ECT) bit and the CE (Congestion Experienced) bit--in the IP header. The ECT bit and the CE bit can be used to make four ECN field combinations of 00 to 11. The first number is the ECT bit and the second number is the CE bit. The table below lists each of the ECT and CE bit combination settings in the ECN field and what the combinations indicate.

***Table 4: ECN Bit Setting***

| ECT Bit | CE Bit | Combination Indicates |
|---|---|---|
| 0 | 0 | Not ECN-capable |
| 0 | 1 | Endpoints of the transport protocol are ECN-capable |
| 1 | 0 | Endpoints of the transport protocol are ECN-capable |
| 1 | 1 | Congestion experienced |

The ECN field combination 00 indicates that a packet is not using ECN.

The ECN field combinations 01 and 10--called ECT(1) and ECT(0), respectively--are set by the data sender to indicate that the endpoints of the transport protocol are ECN-capable. Routers treat these two field combinations identically. Data senders can use either one or both of these two combinations. For more information about these two field combinations, and the implications of using one over the other, refer to RFC 3168, *The Addition of Explicit Congestion Notification (ECN) to IP.*

The ECN field combination 11 indicates congestion to the endpoints. Packets arriving a full queue of a router will be dropped.

### How Packets Are Treated When ECN Is Enabled

If the number of packets in the queue is below the minimum threshold, packets are transmitted. This happens whether or not ECN is enabled, and this treatment is identical to the treatment a packet receives when WRED only is being used on the network.

If the number of packets in the queue is between the minimum threshold and the maximum threshold, one of the following three scenarios can occur:

- If the ECN field on the packet indicates that the endpoints are ECN-capable (that is, the ECT bit is set to 1 and the CE bit is set to 0, or the ECT bit is set to 0 and the CE bit is set to 1)--and the WRED algorithm determines that the packet should have been dropped based on the drop probability--the ECT and CE bits for the packet are changed to 1, and the packet is transmitted. This happens because ECN is enabled and the packet gets marked instead of dropped.
- If the ECN field on the packet indicates that neither endpoint is ECN-capable (that is, the ECT bit is set to 0 and the CE bit is set to 0), the packet may be dropped based on the WRED drop probability. This is the identical treatment that a packet receives when WRED is enabled without ECN configured on the router.
- If the ECN field on the packet indicates that the network is experiencing congestion (that is, both the ECT bit and the CE bit are set to 1), the packet is transmitted. No further marking is required.

If the number of packets in the queue is above the maximum threshold, packets are dropped based on the drop probability. This is the identical treatment a packet receives when WRED is enabled without ECN configured on the router.

## Benefits of WRED Explicit Congestion Notification

### Improved Method for Congestion Avoidance

This feature provides an improved method for congestion avoidance by allowing the network to mark packets for transmission later, rather than dropping them from the queue. Marking the packets for transmission later accommodates applications that are sensitive to delay or packet loss and provides improved throughput and application performance.

### Enhanced Queue Management

Currently, dropped packets indicate that a queue is full and that the network is experiencing congestion. When a network experiences congestion, this feature allows networks to mark the IP header of a packet with a CE bit. This marking, in turn, triggers the appropriate congestion avoidance mechanism and allows the network to better manage the data queues. With this feature, ECN-capable routers and end hosts can respond to congestion before a queue overflows and packets are dropped, providing enhanced queue management.

# How to Configure WRED-Explicit Congestion Notification

## Configuring Explicit Congestion Notification

To configure ECN, complete the following steps.

### SUMMARY STEPS

1. **enable**

2. **configure terminal**
3. **policy-map** *policy-map-name*
4. **class** {*class-name*| **class-default**}
5. **bandwidth** {*bandwidth-kbps* | **percent** *percent*
6. **random-detect**
7. **random-detect ecn**
8. **end**

**DETAILED STEPS**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **policy-map** *policy-map-name*<br>**Example:**<br>`Router(config)# policy-map policy1` | Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy. Enters QoS policy-map configuration mode.<br>• Enter the name of the policy map. |
| **Step 4** | **class** {*class-name*| **class-default**}<br>**Example:**<br>`Router(config-pmap)# class class-default` | Specifies the name of the class whose policy you want to create or change or specifies the default class (commonly known as the class-default class) before you configure its policy. Enters policy-map-class configuration mode.<br>• Enter the name of the class or enter the **class-default**keyword. |
| **Step 5** | **bandwidth** {*bandwidth-kbps* | **percent** *percent*<br>**Example:**<br>`Router(config-pmap-c)#`<br>`bandwidth percent 35` | Specifies or modifies the bandwidth (either in kbps or a percentage) allocated for a class belonging to a policy map.<br>• Enter the bandwidth in kilobytes per second or enter the bandwidth percentage. |
| **Step 6** | **random-detect**<br>**Example:**<br>`Router(config-pmap-c)#`<br>`random-detect` | Enables WRED or distributed WRED (dWRED). |

| | Command or Action | Purpose |
|---|---|---|
| **Step 7** | **random-detect ecn**<br>**Example:**<br>`Router(config-pmap-c)#`<br>`random-detect ecn` | Enables ECN. |
| **Step 8** | **end**<br>**Example:**<br>`Router(config-pmap-c)#`<br>`end` | (Optional) Exits policy-map class configuration mode. |

## Verifying the Explicit Congestion Notification Configuration

To verify the ECN configuration, complete the following steps.

### SUMMARY STEPS

1. **enable**
2. **show policy-map**
3. **show policy-map interface**
4. **end**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **show policy-map**<br>**Example:**<br>`Router# show policy-map` | If ECN is enabled, displays ECN marking information for a specified policy map. |
| **Step 3** | **show policy-map interface**<br>**Example:**<br>`Router# show policy-map interface` | If ECN is enabled, displays ECN marking information for a specified interface. |
| **Step 4** | **end**<br>**Example:**<br>`Router#` | (Optional) Exits privileged EXEC mode. |

| | Command or Action | Purpose |
|---|---|---|
| | end | |

# Configuration Examples for WRED-Explicit Congestion Notification

## Example Enabling ECN

The following example enables ECN in the policy map called pol1:

```
Router(config)# policy-map pol1
 Router(config-pmap)# class class-default
 Router(config-pmap-c)# bandwidth per 70
 Router(config-pmap-c)# random-detect
 Router(config-pmap-c)# random-detect ecn
```

## Example Verifying the ECN Configuration

The following is sample output from the **show policy-map** command. The words "explicit congestion notification" (along with the ECN marking information) included in the output indicate that ECN has been enabled.

```
Router# show policy-map
   Policy Map pol1
     Class class-default
       Weighted Fair Queueing
             Bandwidth 70 (%)
             exponential weight 9
             explicit congestion notification
             class    min-threshold    max-threshold    mark-probability
             ------------------------------------------------------------
             ------------------------------------------------------------

             0        -                -                1/10
             1        -                -                1/10
             2        -                -                1/10
             3        -                -                1/10
             4        -                -                1/10
             5        -                -                1/10
             6        -                -                1/10
             7        -                -                1/10
             rsvp     -                -                1/10
```

The following is sample output from the **show policy-map interface**command. The words "explicit congestion notification" included in the output indicate that ECN has been enabled.

```
Router# show policy-map interface
 Serial4/1
 Serial4/1
  Service-policy output:policy_ecn
        Class-map:prec1 (match-all)
          1000 packets, 125000 bytes
          30 second offered rate 14000 bps, drop rate 5000 bps
          Match:ip precedence 1
          Weighted Fair Queueing
            Output Queue:Conversation 42
```

```
        Bandwidth 20 (%)
        Bandwidth 100 (kbps)
        (pkts matched/bytes matched) 989/123625
    (depth/total drops/no-buffer drops) 0/455/0
         exponential weight:9
         explicit congestion notification
         mean queue depth:0
class    Transmitted  Random drop  Tail drop   Minimum     Maximum     Mark
         pkts/bytes   pkts/bytes    pkts/bytes threshold   threshold   probability
  0        0/0          0/0          0/0          20          40         1/10
  1      545/68125      0/0          0/0          22          40         1/10
  2        0/0          0/0          0/0          24          40         1/10
  3        0/0          0/0          0/0          26          40         1/10
  4        0/0          0/0          0/0          28          40         1/10
  5        0/0          0/0          0/0          30          40         1/10
  6        0/0          0/0          0/0          32          40         1/10
  7        0/0          0/0          0/0          34          40         1/10
rsvp       0/0          0/0          0/0          36          40         1/10
class    ECN Mark
        pkts/bytes
  0      0/0
  1     43/5375
  2      0/0
  3      0/0
  4      0/0
  5      0/0
  6      0/0
  7      0/0
rsvp     0/0
```

# Additional References

### Related Documents

| Related Topic | Document Title |
|---|---|
| QoS commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples | *Cisco IOS Quality of Service Solutions Command Reference* |
| MQC | "Applying QoS Features Using the MQC" module |
| Congestion avoidance concepts | "Congestion Avoidance Overview" module |

### Standards

| Standard | Title |
|---|---|
| No new or modified standards are supported, and support for existing standards has not been modified. | -- |

### MIBs

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

### RFCs

| RFC | Title |
|---|---|
| RFC 2309 | *Internet Performance Recommendation* |
| RFC 2884 | *Performance Evaluation of Explicit Congestion Notification (ECN) in IP Networks* |
| RFC 3168 | *The Addition of Explicit Congestion Notification (ECN) to IP* |

### Technical Assistance

| Description | Link |
|---|---|
| The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password. | http://www.cisco.com/cisco/web/support/index.html |

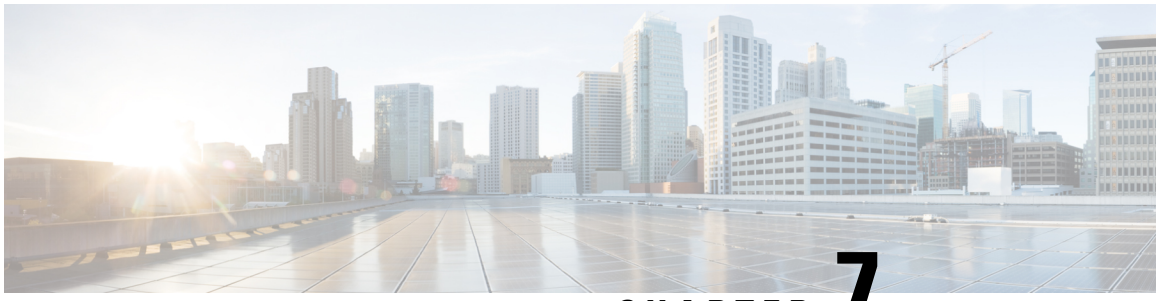
# Feature Information for WRED Explicit Congestion Notification

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

*Table 5: Feature Information for WRED Explicit Congestion Notification*

| Feature Name | Software Releases | Feature Configuration Information |
|---|---|---|
| WRED Explicit Congestion Notification | Cisco IOS XE Release 2.1 | Currently, the congestion control and avoidance algorithms for Transmission Control Protocol (TCP) are based on the idea that packet loss is an appropriate indication of congestion on networks transmitting data using the best-effort service model. When a network uses the best-effort service model, the network delivers data if it can, without any assurance of reliability, delay bounds, or throughput. However, these algorithms and the best-effort service model are not suited to applications that are sensitive to delay or packet loss (for instance, interactive traffic including Telnet, web-browsing, and transfer of audio and video data). Weighted Random Early Detection (WRED), and by extension, Explicit Congestion Notification (ECN), helps to solve this problem.<br><br>The following commands were introduced or modified: **random-detect ecn**, **show policy-map**, **show policy-map interface**. |



CHAPTER 7

# QoS Time-Based Thresholds for WRED and Queue Limit


• QoS Time-Based Thresholds for WRED and Queue Limit, on page 41


# 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.

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

## 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

## Benefits of QoS Time-Based Thresholds for WRED and Queue Limit

### 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.

## 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.

## random-detect Commands with the Milliseconds 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 the table below.

***Table 6: 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. |

## 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

## Enabling WRED and Using WRED to Specify Thresholds

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map** *policy-name*
4. **class** {*class-name***class-default**}
5. To continue with the configuration, you must either specify a bandwidth or enable traffic shaping. Choose one or the other.
6. **bandwidth** {*bandwidth-kbps* | **remaining percent** *percentage* | **percent** *percentage*}
7. **shape** [**average** | **peak**] *mean-rate* [*burst-size*] [*excess-burst-size*]
8. **random-detect**
9. **random-detect precedence** {*precedence* | **rsvp**} *min-threshold* {**bytes**| **ms**| **packets**} *max-threshold*{**bytes** | **ms**| **packets**} [*mark-probability-denominator*]

10. **exit**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **policy-map** *policy-name*<br>**Example:**<br>`Router(config)# policy-map policy1` | Specifies the name of the policy map to be created. Enters policy-map configuration mode.<br>• Enter policy map name. |
| **Step 4** | **class** {*class-name***class-default**}<br>**Example:**<br>`Router(config-pmap)# class class1` | Specifies the class so that you can configure or modify its policy. Enters policy-map class configuration mode.<br>• Enter the class name or specify the default class (class-default). |
| **Step 5** | To continue with the configuration, you must either specify a bandwidth or enable traffic shaping. Choose one or the other. | |
| **Step 6** | **bandwidth** {*bandwidth-kbps* \| **remaining percent** *percentage* \| **percent** *percentage*}<br>**Example:**<br>`Router(config-pmap-c)# bandwidth percent 40` | (Optional) Specifies or modifies the bandwidth allocated for a class belonging to a policy map.<br>• Enter the bandwidth to be set or modified. |
| **Step 7** | **shape** [**average** \| **peak**] *mean-rate* [*burst-size*] [*excess-burst-size*]<br>**Example:**<br>`Router(config-pmap-c)# shape average 51200` | (Optional) Enables either average or peak rate traffic shaping.<br>• Specify either average or peak traffic shaping. |
| **Step 8** | **random-detect**<br>**Example:**<br>`Router(config-pmap-c)# random-detect` | Enables WRED or distributed WRED (DWRED). |
| **Step 9** | **random-detect precedence** {*precedence* \| **rsvp**} *min-threshold* {**bytes**\| **ms**\| **packets**} *max-threshold*{**bytes** \| **ms**\| **packets**} [*mark-probability-denominator*] | Configures WRED and DWRED parameters for a particular IP precedence. |

| | Command or Action | Purpose |
|---|---|---|
| | **Example:**<br>`Router(config-pmap-c)# random-detect precedence 2 512 ms 1020 ms` | • Specify the IP precedence or RSVP value, and thresholds, as needed.<br>**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. |
| **Step 10** | **exit**<br>**Example:**<br>`Router(config-pmap-c)# exit` | (Optional) Exits policy-map class configuration mode. |

## Using the queue-limit Command to Specify the Thresholds

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map** *policy-name*
4. **class** {*class-name* **class-default**}
5. To continue with the configuration, you must either specify a bandwidth or enable traffic shaping. Choose one or the other.
6. **bandwidth** {*bandwidth-kbps* | **remaining percent** *percentage* | **percent** *percentage*}
7. **shape** [**average** | **peak**] *mean-rate* [[*burst-size*] [*excess-burst-size*]]
8. **queue-limit** *number-of-packets* [**bytes** | **ms** | **packets**]
9. **exit**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **policy-map** *policy-name*<br>**Example:**<br>`Router(config)#` | Specifies the name of the policy map to be created. Enters policy-map configuration mode.<br>• Enter policy map name. |

| | Command or Action | Purpose |
|---|---|---|
| | `policy-map`<br><br>`policy1` | |
| **Step 4** | **class** {*class-name* **class-default**}<br>**Example:**<br><br>`Router(config-pmap)# class class1` | Specifies the class so that you can configure or modify its policy. Enters policy-map class configuration mode.<br>• Enter the class name or specify the default class (class-default). |
| **Step 5** | To continue with the configuration, you must either specify a bandwidth or enable traffic shaping. Choose one or the other. | |
| **Step 6** | **bandwidth** {*bandwidth-kbps* \| **remaining percent** *percentage* \| **percent** *percentage*}<br>**Example:**<br><br>`Router(config-pmap-c)# bandwidth percent 40` | (Optional) Specifies or modifies the bandwidth allocated for a class belonging to a policy map.<br>• Enter the bandwidth to be set or modified. |
| **Step 7** | **shape** [**average** \| **peak**] *mean-rate* [[*burst-size*] [*excess-burst-size*]]<br>**Example:**<br><br>`Router(config-pmap-c)# shape average 51200` | (Optional) Enables either average or peak rate traffic shaping.<br>• Specifies either average or peak traffic shaping. |
| **Step 8** | **queue-limit** *number-of-packets* [**bytes** \| **ms** \| **packets**]<br>**Example:**<br><br>`Router(config-pmap-c)# queue-limit 200 ms` | (Optional) 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.<br>• Enter the queue limit. The unit of measure can be bytes, milliseconds, or packets. |
| **Step 9** | **exit**<br>**Example:**<br><br>`Router(config-pmap-c)# exit` | (Optional) Exits policy-map class configuration mode. |

## Attaching the Policy Map to an Interface in a QoS Time-Based Threshold for WRED Configuration

**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.

### 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**<br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **interface** *type number*<br>**Example:**<br>`Router(config)#`<br>`interface serial4/0` | Configures an interface (or subinterface) type and enters interface configuration mode.<br>• Enter the interface type number. |
| **Step 4** | **pvc** [*name*] *vpi* / *vci* [**ilmi** | **qsaal** | **smds**]<br>**Example:**<br>`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.<br>**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*<br>**Example:**<br>`Router(config-if)#`<br>`service-policy output policy1`<br>**Example:** | Specifies the name of the policy map to be attached to the input *or* output direction of the interface.<br>**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.<br>• Enter the policy map name. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 6** | **exit**<br>**Example:**<br>`Router(config-if)# exit` | (Optional) Exits interface configuration mode. |

## Verifying the QoS Time-Based Thresholds for WRED and Queue Limit Configuration

### SUMMARY STEPS

1. **enable**
2. **show policy-map** [*policy-map*]
3. and/or
4. **show policy-map interface** *interface-name*
5. **exit**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **show policy-map** [*policy-map*]<br>**Example:**<br>`Router# show policy-map policy1` | Displays all information about a class map, including the match criterion.<br>• Enter class map name. |
| **Step 3** | and/or | |
| **Step 4** | **show policy-map interface** *interface-name*<br>**Example:**<br>`Router#`<br>`show policy-map interface serial4/0` | 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.<br>• Enter the interface name. |
| **Step 5** | **exit**<br>**Example:**<br>`Router# exit` | (Optional) Exits privileged 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 the following findings:
    1. 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.

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

## Example Using WRED to Set Thresholds

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
```

## Example Using the queue-limit Command to Set Thresholds

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
```

## Example Verifying the Configuration

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.

## Example 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.

## Example 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

### Related Documents

| Related Topic | Document Title |
|---|---|
| Cisco IOS commands | Cisco IOS Master Commands List, All Releases |
| 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* |
| Congestion avoidance mechanisms, including tail drop, RED and WRED | *Cisco IOS Quality of Service Solutions Configuration Guide* |

| Related Topic | Document Title |
|---|---|
| Congestion management mechanisms, including CBWFQ, and DCBWFQ | *Cisco IOS Quality of Service Solutions Configuration Guide* |
| Byte-Based WRED | Byte-Based Weight Random Early Detection module |

### Standards

| Standard | Title |
|---|---|
| No new or modified standards are supported, and support for existing standards has not been modified. | -- |

### MIBs

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

### RFCs

| RFC | Title |
|---|---|
| No new or modified RFCs are supported, and support for existing RFCs has not been modified. | -- |

### Technical Assistance

| Description | Link |
|---|---|
| The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password. | http://www.cisco.com/cisco/web/support/index.html |

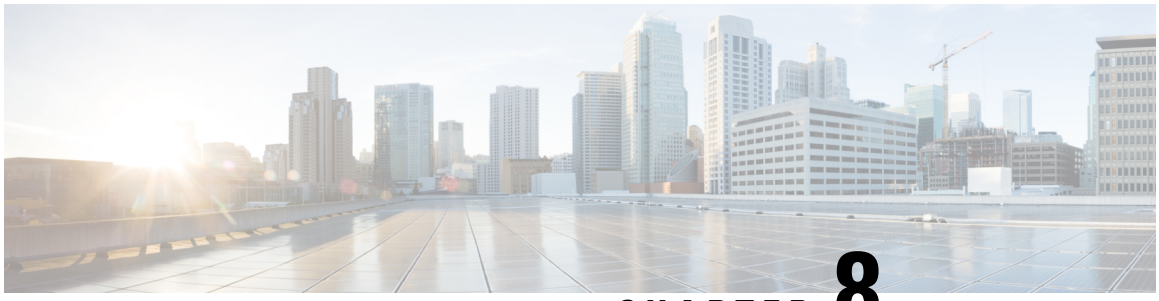
# Feature Information for QoS Time-Based Thresholds for WRED and Queue Limit

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

*Table 7: Feature Information for QoS Time-Based Thresholds for WRED and Queue Limit*

| Feature Name | Releases | Feature Information |
|---|---|---|
| QoS Time-Based Thresholds for WRED and Queue Limit | Cisco IOS XE Release 3.2S | 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).<br><br>The following commands are introduced or modified: **queue-limit, random-detect precedence, show policy-map, show policy-map interface.** |



CHAPTER 8

# DiffServ Compliant WRED


• DiffServ Compliant WRED, on page 55



# DiffServ Compliant WRED


DiffServ Compliant WRED extends the functionality of Weighted Random Early Detection to enable support for DiffServ and Assured Forwarding (AF) per hop behavior (PHB). This feature enables customers to implement AF PHB by coloring packets according to Differentiated Services Code Point (DSCP) values and then assigning preferential drop probabilities to those packets.

**Note** This feature can be used with IP packets only. It is not intended for use with Multiprotocol Label Switching (MPLS)-encapsulated packets.

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

## Information About DiffServ Compliant WRED

### Differentiated Services for WRED

Differentiated Services is a multiple service model that can satisfy differing Quality of Service (QoS) requirements. With Differentiated Services, the network tries to deliver a particular kind of service based on the QoS specified by each packet. This specification can occur in different ways. The DiffServ Compliant WRED feature enables WRED to use either the 6-bit differentiated services code point (DSCP) or the IP Precedence setting in IP packets when it calculates the drop probability for a packet. The DSCP value is the first six bits of the IP type of service (ToS) byte.

## Usage Guidelines for DiffServ Compliant WRED

To configure the DiffServ Compliant WRED feature, first specify the policy map, add the class, and configure the bandwidth or shape for the class. If you want WRED to use the DSCP value when it calculates the drop probability, use the *dscp-based* argument with the **random-detect** command to specify the DSCP value and then use the **random-detect dscp** command to modify the default minimum and maximum thresholds for the DSCP value. If you want WRED to use the IP Precedence value when it calculates the drop probability, use the *precedence-based* argument with the **random-detect** command to specify the IP Precedence value. This configuration can then be applied wherever policy maps are attached (for example, at the interface level, the per-VC level, or the shaper level).

Remember the following points when using the commands included with this feature:

- If you use the *dscp-based* argument, WRED will use the DSCP value to calculate the drop probability.
- If you use the *precedence-based* argument, WRED will use the IP Precedence value to calculate the drop probability.
- The *dscp-based* and *precedence-based* arguments are mutually exclusive.
- If you do not specify either argument, WRED will use the IP Precedence value to calculate the drop probability (the default method).

# How to Configure DiffServ Compliant WRED

## Configuring DiffServ Compliant WRED

This example configures DiffServ Compliant WRED to use the DSCP value to calculate the drop probability for a packet.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number* [**name-tag**]
4. **class-map** *class-map-name*
5. **match** *match-criterion*
6. **policy-map** *policy-map-name*
7. **class** {*class-name* | **class-default**}
8. **bandwidth** {*kbps* | **remaining** *percentage* | **percent** *percentage*}
9. **random-detect** [**dscp-based** | **precedence-based**]
10. **random-detect dscp** *dscp-value min-threshold max-threshold* [ *mark-probability-denominator*]
11. **exit**
12. **exit**
13. **interface** *type number* [**name-tag**]
14. **service-policy output** *policy-map-name*
15. **end**
16. **show policy-map interface** *type number*
17. **exit**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **interface** *type number* [**name-tag**]<br>**Example:**<br>`Device(config)# interface GigabitEthernet 0/0/0` | Configures an interface type and enters interface configuration mode.<br>• Enter the interface type and number. |
| **Step 4** | **class-map** *class-map-name*<br>**Example:**<br>`Device(config-if)# class-map diffservclass` | Specifies the name of the class map to be created and enters QoS class-map configuration mode. |
| **Step 5** | **match** *match-criterion*<br>**Example:**<br>`Device(config-cmap)# match any` | Configures the match criteria for a class map. |
| **Step 6** | **policy-map** *policy-map-name*<br>**Example:**<br>`Device(config-cmap)# policy-map diffservpm` | Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy, and enters QoS policy-map configuration mode. |
| **Step 7** | **class** {*class-name* \| **class-default**}<br>**Example:**<br>`Device(config-pmap)# class diffservclass` | Specifies the name of the class whose policy you want to create or change or specifies the default class (commonly known as the class-default class) before you configure its policy.<br>• Enters QoS policy-map class configuration mode. |
| **Step 8** | **bandwidth** {*kbps* \| **remaining** *percentage* \| **percent** *percentage*}<br>**Example:**<br>`Device(config-pmap-c)# bandwidth percent 30` | Specifies the bandwidth allocated for a class belonging to a policy map. |
| **Step 9** | **random-detect** [**dscp-based** \| **precedence-based**]<br>**Example:** | Configures WRED for a class in a policy map. |

| | Command or Action | Purpose |
|---|---|---|
| | `Device(config-pmap-c)# random-detect dscp-based` | |
| **Step 10** | **random-detect dscp** *dscp-value min-threshold max-threshold* [ *mark-probability-denominator*]<br>**Example:**<br>`Device(config-pmap-c)# random-detect dscp af11 10000 30000 25` | Changes the minimum and maximum packet thresholds for the differentiated services code point (DSCP) value. |
| **Step 11** | **exit**<br>**Example:**<br>`Device(config-pmap-c)# exit` | Exits QoS policy-map class configuration mode. |
| **Step 12** | **exit**<br>**Example:**<br>`Device(config-pmap)# exit` | Exits QoS policy-map configuration mode. |
| **Step 13** | **interface** *type number* [**name-tag**]<br>**Example:**<br>`Device(config)# interface GigabitEthernet 0/0/0` | Configures an interface type and enters interface configuration mode.<br>• Enter the interface type and number. |
| **Step 14** | **service-policy output** *policy-map-name*<br>**Example:**<br>`Device(config-if)# service-policy output policy1` | Attaches a policy map to an output interface.<br>• Enter the policy map name.<br>**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. |
| **Step 15** | **end**<br>**Example:**<br>`Device(config-if)# end` | Returns to privileged EXEC mode. |
| **Step 16** | **show policy-map interface** *type number*<br>**Example:** | (Optional) Displays the traffic 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. |

| | Command or Action | Purpose |
|---|---|---|
| | `Device# show policy-map interface GigabitEthernet 0/0/0` | • Enter the interface type and number. |
| **Step 17** | **exit**<br>**Example:**<br>`Device# exit` | (Optional) Exits privileged EXEC mode. |

# Configuration Examples for DiffServ Compliant WRED

## Example: DiffServ compliant WRED

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

```
Device(config)# class-map c1
Device(config-cmap)# match ip precedence 1
Device(config-cmap)# policy-map p1
Device(config-pmap)# class c1
Device(config-pmap-c)# bandwidth 48
Device(config-pmap-c)# random-detect dscp-based
Device(config-pmap-c)# random-detect dscp 8 24 40 (bytes/ms)
Device(config-if)# service-policy output p1
```

# Additional References

### Related Documents

| Related Topic | Document Title |
|---|---|
| Cisco IOS commands | Cisco IOS Master Commands List, All Releases |
| QoS commands | *Cisco IOS Quality of Service Solutions Command Reference* |
| MQC | *QoS: Modular QoS: Command-Line Interface Configuration Guide* |

### Standards and RFCs

| Standard/RFC | Title |
|---|---|
| RFC 2474 | *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers* |
| RFC 2475 | *An Architecture for Differentiated Services Framework* |

| Standard/RFC | Title |
|---|---|
| RFC 2597 | *Assured Forwarding PHB* |
| RFC 2598 | *An Expedited Forwarding PHB* |

### MIBs

| MIB | MIBs Link |
|---|---|
| CISCO-CLASS-BASED-QOS-MIB<br>CISCO-CLASS-BASED-QOS-CAPABILITY-MIB | To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL:<br>http://www.cisco.com/go/mibs |

### Technical Assistance

| Description | Link |
|---|---|
| The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password. | http://www.cisco.com/cisco/web/support/index.html |

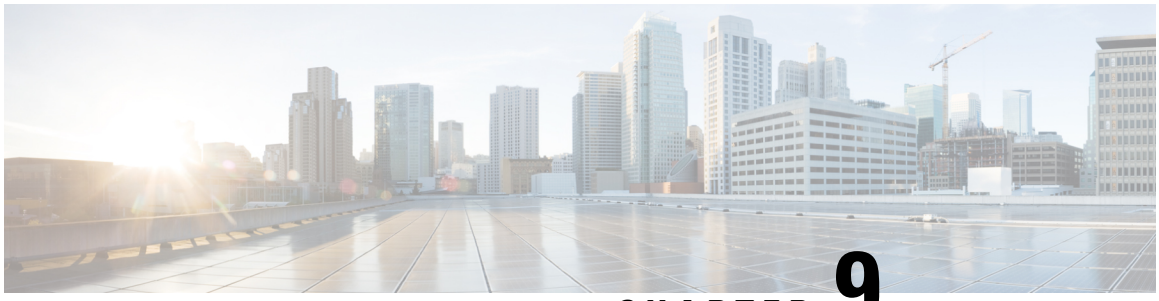
# Feature Information for DiffServ Compliant WRED

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

*Table 8: Feature Information for DiffServ Compliant WRED*

| Feature Name | Releases | Feature Information |
|---|---|---|
| DiffServ Compliant WRED | Cisco IOS XE Release 3.6S | DiffServ Compliant WRED extends the functionality of WRED to enable support for DiffServ and AF per-hop behavior.<br><br>In Cisco IOS XE Release 3.6S, support was added for the Cisco ASR 903 Router.<br><br>The following commands were introduced or modified: **random-detect**, **random-detect dscp**, **random-detect precedence**. |



CHAPTER 9

# Shaping on Dialer Interfaces


- Shaping on Dialer Interfaces, on page 63


# Shaping on Dialer Interfaces

The Shaping on Dialer Interfaces feature provides support for Point-to-Point Protocol over Ethernet (PPPoE) and Point-to-Point Protocol over Asynchronous Transfer Mode (PPPoA) configurations on dialer interfaces. The feature provides support for Modular QoS CLI (MQC)-based queuing and shaping that supports per-customer quality of service (QoS). Parent policies are attached to an Ethernet in the First Mile (EFM) interface, and child policies are attached to individual dialer interfaces. Class of service (CoS) values are set by applying a policy to the dialer interface. The feature also enables the collection of queuing statistics on the dialer interface and the polling of traffic counters for dialer interfaces.

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

## Restrictions for Shaping on Dialer Interfaces

- The output queueing policy must have a parent class-default shaper, and any other queueing actions must be configured in a child policy.

## Information About Shaping on Dialer Interfaces

### QoS on PPP Session on Dialer Interfaces

The Shaping on Dialer Interfaces feature consolidates the output queueing and classification on the egress interface (where all the queueing features are run). The police and set features (such as CoS marking) also work in the output path.

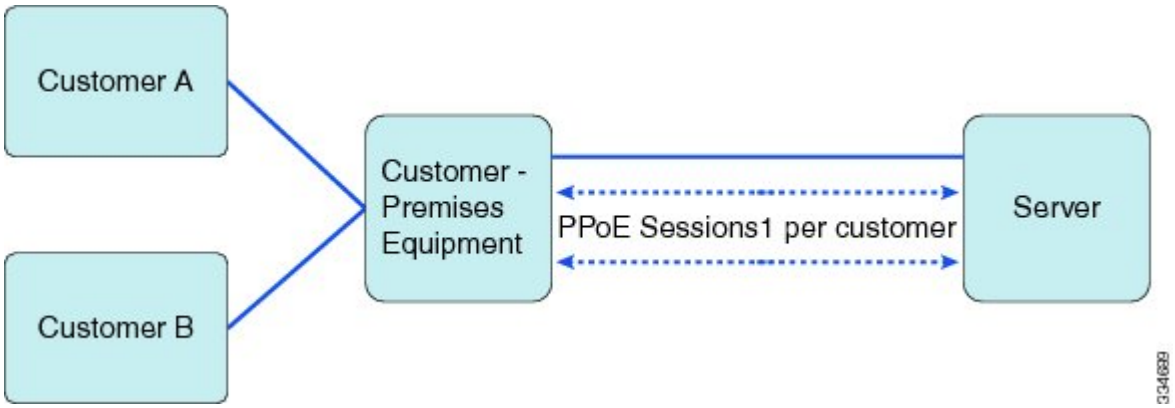
MQC-based QoS queuing and shaping features can be used to attach flat class-default shaped policies to the EFM and attach HQoS parent-shaped policies to the dialer interface.

Policies are applied to the dialer interface using the **service-policy** command. In addition the related show and debug commands display policy and queueing statistics associated with the dialer target.

## QoS Dialer Interface Topology

The following figure shows the supported topology for the Shaping on Dialer Interfaces feature:

***Figure 3: Shaping on Dialer Interfaces Topology***




The Customer Premises Equipment (CPE) is shared between several customers. Each customer connects to the CPE through a VLAN on a Gigabit Ethernet port. The CPE connects to the service over a DSL using an EFM interface (this looks like an Ethernet connection but uses DSL) over which all the incoming VLANs will be forwarded. The traffic for each VLAN (customer) is transmitted in a separate PPP session. Each session is set up using a dialer interface.

# How to Configure Shaping on Dialer Interfaces

## Configuring an Output Queueing Policy for Dialer Interfaces

### Before you begin

Because the dialer target is added to the dynamic target API, the output queueing policy must have a parent class-default shaper with any other queueing actions configured in a child policy.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map** *policy-map-name*
4. **class** *class-name*
5. **priority percent** *percentage*
6. **exit**
7. **class** *class-name*
8. **bandwidth percent** *percentage*

9. **exit**
10. **class** {*class-name* | **class-default**}
11. **fair-queue**
12. **exit**
13. **exit**
14. **policy-map** *policy-map-name*
15. **class class-default**
16. **shape average** *target-bit-rate*
17. **service-policy** *policy-map-name*
18. **exit**
19. **exit**
20. **interface** *type number*
21. **service-policy output** *policy-name*
22. **exit**

**DETAILED STEPS**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **policy-map** *policy-map-name*<br>**Example:**<br>`Device(config)# policy-map child` | Specifies the name of the policy map created earlier and enters policy-map configuration mode.<br>• Enter the policy map name. |
| **Step 4** | **class** *class-name*<br>**Example:**<br>`Device(config-pmap)# class voice` | Specifies the name of the class whose policy you want to create and enters policy-map class configuration mode. This class is associated with the class map created earlier.<br>• Enter the name of the class or enter the **class-default** keyword. |
| **Step 5** | **priority percent** *percentage*<br>**Example:**<br>`Device(config-pmap-c)# priority percent 30` | Specifies that the amount of guaranteed bandwidth will be specified by the percent of available bandwidth. |
| **Step 6** | **exit**<br>**Example:** | Returns to policy-map configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| | `Device(config-pmap-c)# exit` | |
| **Step 7** | **class** *class-name*<br>**Example:**<br>`Device(config-pmap)# class video` | Specifies the name of the class whose policy you want to create and enters policy-map class configuration mode. This class is associated with the class map created earlier.<br>• Enter the name of the class or enter the **class-default** keyword. |
| **Step 8** | **bandwidth percent** *percentage*<br>**Example:**<br>`Device(config-pmap-c)# bandwidth percent 50` | Specifies that the amount of guaranteed bandwidth will be specified by the percent of total bandwidth. |
| **Step 9** | **exit**<br>**Example:**<br>`Device(config-pmap-c)# exit` | Returns to policy-map configuration mode. |
| **Step 10** | **class** {*class-name* \| **class-default**}<br>**Example:**<br>`Device(config-pmap)# class class-default` | Specifies the name of the class whose policy you want to create and enters policy-map class configuration mode. This class is associated with the class map created earlier.<br>• Enter the name of the class or enter the **class-default** keyword. |
| **Step 11** | **fair-queue**<br>**Example:**<br>`Device(config-pmap-c)# fair-queue` | Enables flow-based fair queueing in this class. |
| **Step 12** | **exit**<br>**Example:**<br>`Device(config-pmap-c) exit` | Returns to policy-map configuration mode. |
| **Step 13** | **exit**<br>**Example:**<br>`Device(config-pmap) exit` | Returns to global configuration mode. |
| **Step 14** | **policy-map** *policy-map-name*<br>**Example:**<br>`Device(config)# policy-map parent` | Specifies the name of a policy map and enters policy-map configuration mode.<br>• Enter the policy map name. |
| **Step 15** | **class class-default**<br>**Example:** | Creates the class-default class. |

| | Command or Action | Purpose |
|---|---|---|
| | `Device(config-pmap)# class class-default` | |
| **Step 16** | **shape average** *target-bit-rate*<br>**Example:**<br>`Device(config-pmap-c)# shape average 1000000` | Specifies average rate traffic shaping as bits-per-second on an interface. |
| **Step 17** | **service-policy** *policy-map-name*<br>**Example:**<br>`Device(config-pmap-c)# service policy child` | Configures a service policy policy map. |
| **Step 18** | **exit**<br>**Example:**<br>`Device(config-pmap-c) exit` | Returns to policy-map configuration mode. |
| **Step 19** | **exit**<br>**Example:**<br>`Device(config-pmap) exit` | Returns to global configuration mode. |
| **Step 20** | **interface** *type number*<br>**Example:**<br>`Device(config)# interface Dialer 0` | Configures an interface type and enters interface configuration mode.<br>• Enter the interface type and number. |
| **Step 21** | **service-policy output** *policy-name*<br>**Example:**<br>`Device(config-if)# service-policy output parent` | Attaches a policy map to an output interface that will be used as the service policy for the interface. |
| **Step 22** | **exit**<br>**Example:**<br>`Device(config-if) exit` | Returns to global configuration mode. |

## Configuring QoS for PPPoEoA for Dialer Interfaces

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number* [**name-tag**]
4. **no ip address**
5. **no atm ilmi-keepalive**
6. **exit**
7. **interface** *type number* [**name-tag**]

8. **pvc** *vpi/vci*
9. **vbr-nrt** *output-pcr output-scr*
10. **pppoe-client dial-pool-number** *number*
11. **exit**
12. **exit**
13. **interface** *type number* [**name-tag**]
14. **mtu** *ip-address*
15. **ip address** *ip-address mask*
16. **encapsulation** *encapsulation-type*
17. **dialer pool** *number*
18. **dialer-group** *number*
19. **service-policy output** *name*
20. **exit**
21. **dialer-list** *dialer-group* **protocol** *protocol-name* **permit**

**DETAILED STEPS**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **interface** *type number* [**name-tag**]<br>**Example:**<br>`Device(config)# interface ATM 0` | Configures an interface type and enters interface configuration mode.<br>• Enter the interface type and number. |
| **Step 4** | **no ip address**<br>**Example:**<br>`Device(config-if)# no ip address` | Disables IP processing on the interface. |
| **Step 5** | **no atm ilmi-keepalive**<br>**Example:**<br>`Device(config-if)# no atm ilmi-keepalive` | Disables Interim Local Management Interface (ILMI) keepalives on the interface. |
| **Step 6** | **exit**<br>**Example:**<br>`Device(config-if)# exit` | Exits interface configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 7** | **interface** *type number* [**name-tag**]<br>**Example:**<br>`Device(config)# interface ATM 0.1 point-to-point` | Configures an interface type and enters interface configuration mode.<br>• Enter the interface type, number, and name. |
| **Step 8** | **pvc** *vpi/vci*<br>**Example:**<br>`Device(config-if)# pvc 4/46` | Creates an ATM permanent virtual circuit (PVC), and enters ATM virtual circuit configuration mode.<br>• Enter the ATM network virtual path identifier (VPI) and ATM network virtual channel identifier (VCI) for this PVC. |
| **Step 9** | **vbr-nrt** *output-pcr output-scr*<br>**Example:**<br>`Device(config-if-atm-vc)# vbr-nrt 738 738` | Configures the variable bit rate-nonreal time (VBR-NRT) quality of service (QoS) and specifies the output peak cell rate (PCR), and output sustainable cell rate (SCR) for an ATM permanent virtual circuit (PVC). |
| **Step 10** | **pppoe-client dial-pool-number** *number*<br>**Example:**<br>`Device(config-if-atm-vc)# pppoe-client dial-pool-number 1` | Configures a PPP over Ethernet (PPPoE) client and specifies the dial-on-demand routing (DDR) functionality. |
| **Step 11** | **exit**<br>**Example:**<br>`Device(config-if-atm-vc)# exit` | Exits ATM virtual circuit configuration mode. |
| **Step 12** | **exit**<br>**Example:**<br>`Device(config-if)# exit` | Exits interface configuration mode. |
| **Step 13** | **interface** *type number* [**name-tag**]<br>**Example:**<br>`Device(config)# interface Dialer 0` | Configures an interface type and enters interface configuration mode.<br>• Enter the interface type and number. |
| **Step 14** | **mtu** *ip-address*<br>**Example:**<br>`Device(config-if)# mtu 1200` | Adjusts the maximum packet size or maximum transmission unit (MTU) size. |
| **Step 15** | **ip address** *ip-address mask*<br>**Example:**<br>`Device(config-if)# ip address 172.16.0.0 255.0.0.0` | Sets the primary IP address for the interface.<br>• Enter the IP address and the IP address mask. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 16** | **encapsulation** *encapsulation-type*<br>**Example:**<br>`Device(config-if)# encapsulation ppp` | Sets the encapsulation method used by the interface. |
| **Step 17** | **dialer pool** *number*<br>**Example:**<br>`Device(config-if)# dialer pool 1` | Specifies the dialing pool that the dialer interface uses to connect to a specific destination subnetwork. |
| **Step 18** | **dialer-group** *number*<br>**Example:**<br>`Device(config-if)# dialer-group 1` | Controls access by configuring the interface to belong to a specific dialing group. |
| **Step 19** | **service-policy output** *name*<br>**Example:**<br>`Device(config-if)# service-policy output dialer-output-sp` | Attaches a policy map to an output interface that will be used as the service policy for the interface. |
| **Step 20** | **exit**<br>**Example:**<br>`Device(config-if)# exit` | Exits interface configuration mode. |
| **Step 21** | **dialer-list** *dialer-group* **protocol** *protocol-name* **permit**<br>**Example:**<br>`Device(config)# dialer-list 1 protocol ip permit` | Defines a dial-on-demand routing (DDR) dialer list for dialing by protocol or by a combination of a protocol and a previously defined access list. |

# Configuring QoS for PPPoE for Dialer Interfaces

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number* [**name-tag**]
4. **ppp enable group** *group-name*
5. **pppoe-client dial-pool-number** *number*
6. **exit**
7. **interface** *type number* [**name-tag**]
8. **mtu** *ip-address*
9. **ip address** *ip-address mask*
10. **encapsulation** *encapsulation-type*
11. **dialer pool** *number*

12. **dialer-group** *number*
13. **service-policy output** *name*
14. **exit**
15. **dialer-list** *dialer-group* **protocol** *protocol-name* **permit**

**DETAILED STEPS**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **interface** *type number* [**name-tag**]<br>**Example:**<br>`Device(config)# interface Ethernet 0/0` | Configures an interface type and enters interface configuration mode.<br>• Enter the interface type, number, and name. |
| **Step 4** | **ppp enable group** *group-name*<br>**Example:**<br>`Device(config-if)# ppp enable group global` | Enables PPPoE sessions on an Ethernet interface or subinterface. |
| **Step 5** | **pppoe-client dial-pool-number** *number*<br>**Example:**<br>`Device(config-if)# pppoe-client dial-pool-number 1` | Configures a PPPoE client and to specify the dial-on-demand routing (DDR) functionality. |
| **Step 6** | **exit**<br>**Example:**<br>`Device(config-if)# exit` | Exits interface configuration mode. |
| **Step 7** | **interface** *type number* [**name-tag**]<br>**Example:**<br>`Device(config)# interface Dialer 0` | Configures an interface type and enters interface configuration mode.<br>• Enter the interface type and number. |
| **Step 8** | **mtu** *ip-address*<br>**Example:**<br>`Device(config-if)# mtu 1200` | Adjusts the maximum packet size or maximum transmission unit (MTU) size. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 9** | **ip address** *ip-address mask*<br>**Example:**<br>`Device(config-if)# ip address 172.16.0.0 255.0.0.0` | Sets the primary IP address for the interface.<br>• Enter the IP address and the IP address mask. |
| **Step 10** | **encapsulation** *encapsulation-type*<br>**Example:**<br>`Device(config-if)# encapsulation ppp` | Sets the encapsulation method used by the interface. |
| **Step 11** | **dialer pool** *number*<br>**Example:**<br>`Device(config-if)# dialer pool 1` | Specifies the dialing pool that the dialer interface uses to connect to a specific destination subnetwork. |
| **Step 12** | **dialer-group** *number*<br>**Example:**<br>`Device(config-if)# dialer-group 1` | Controls access by configuring the interface to belong to a specific dialing group. |
| **Step 13** | **service-policy output** *name*<br>**Example:**<br>`Device(config-if)# service-policy output dialer-output-sp` | Attaches a policy map to an output interface that will be used as the service policy for the interface. |
| **Step 14** | **exit**<br>**Example:**<br>`Device(config-if)# exit` | Exits interface configuration mode. |
| **Step 15** | **dialer-list** *dialer-group* **protocol** *protocol-name* **permit**<br>**Example:**<br>`Device(config)# dialer-list 1 protocol ip permit` | Defines a dial-on-demand routing (DDR) dialer list for dialing by protocol or by a combination of a protocol and a previously defined access list. |

## Configuring QoS for PPPoA for Dialer Interfaces

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number* [**name-tag**]
4. **pvc** *vpi/vci*
5. **vbr-nrt** *output-pcr output-scr output-maxburstsize*

6. **dialer pool-member** *number*
7. **protocol** *protocol*
8. **exit**
9. **exit**
10. **interface** *type number* [**name-tag**]
11. **mtu** *ip-address*
12. **ip address** *ip-address mask*
13. **encapsulation** *encapsulation-type*
14. **dialer pool** *number*
15. **dialer-group** *number*
16. **service-policy output** *name*
17. **exit**
18. **dialer-list** *dialer-group* **protocol** *protocol-name* **permit**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **interface** *type number* [**name-tag**]<br>**Example:**<br>`Device(config)# interface ATM 0.1 point-to-point` | Configures an interface type and enters interface configuration mode.<br>• Enter the interface type, number, and name. |
| **Step 4** | **pvc** *vpi/vci*<br>**Example:**<br>`Device(config-if)# pvc 4/46` | Creates an ATM permanent virtual circuit (PVC), and enters ATM virtual circuit configuration mode.<br>• Enter the ATM network virtual path identifier (VPI) and ATM network virtual channel identifier (VCI) for this PVC. |
| **Step 5** | **vbr-nrt** *output-pcr output-scr output-maxburstsize*<br>**Example:**<br>`Device(config-if-atm-vc)# vbr-nrt 738 738 32` | Configures the variable bit rate-nonreal time (VBR-NRT) quality of service (QoS) and specifies the output peak cell rate (PCR), output sustainable cell rate (SCR), and output maximum burst cell size for an ATM permanent virtual circuit (PVC). |
| **Step 6** | **dialer pool-member** *number*<br>**Example:** | Configures a physical interface to be a member of a dialer profiles dialing pool. |

| | Command or Action | Purpose |
|---|---|---|
| | `Device(config-if-atm-vc)# dialer pool-member 1` | |
| **Step 7** | **protocol** *protocol*<br>**Example:**<br>`Device(config-if-atm-vc)# protocol ppp dialer` | Configures a static map for an ATM permanent virtual circuit (PVC), switched virtual circuit (SVC), or virtual circuit (VC) class. |
| **Step 8** | **exit**<br>**Example:**<br>`Device(config-if-atm-vc)# exit` | Exits ATM virtual circuit configuration mode. |
| **Step 9** | **exit**<br>**Example:**<br>`Device(config-if)# exit` | Exits interface configuration mode. |
| **Step 10** | **interface** *type number* [**name-tag**]<br>**Example:**<br>`Device(config)# interface Dialer 0` | Configures an interface type and enters interface configuration mode.<br>• Enter the interface type and number. |
| **Step 11** | **mtu** *ip-address*<br>**Example:**<br>`Device(config-if)# mtu 1200` | Adjusts the maximum packet size or maximum transmission unit (MTU) size. |
| **Step 12** | **ip address** *ip-address mask*<br>**Example:**<br>`Device(config-if)# ip address 172.16.0.0 255.0.0.0` | Sets the primary IP address for the interface.<br>• Enter the IP address and the IP address mask. |
| **Step 13** | **encapsulation** *encapsulation-type*<br>**Example:**<br>`Device(config-if)# encapsulation ppp` | Sets the encapsulation method used by the interface. |
| **Step 14** | **dialer pool** *number*<br>**Example:**<br>`Device(config-if)# dialer pool 1` | Specifies the dialing pool that the dialer interface uses to connect to a specific destination subnetwork. |
| **Step 15** | **dialer-group** *number*<br>**Example:**<br>`Device(config-if)# dialer-group 1` | Controls access by configuring the interface to belong to a specific dialing group. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 16** | **service-policy output** *name*<br>**Example:**<br>`Device(config-if)# service-policy output dialer-output-sp` | Attaches a policy map to an output interface that will be used as the service policy for the interface. |
| **Step 17** | **exit**<br>**Example:**<br>`Device(config-if)# exit` | Exits interface configuration mode. |
| **Step 18** | **dialer-list** *dialer-group* **protocol** *protocol-name* **permit**<br>**Example:**<br>`Device(config)# dialer-list 1 protocol ip permit` | Defines a dial-on-demand routing (DDR) dialer list for dialing by protocol or by a combination of a protocol and a previously defined access list, . |

## Configuring QoS for Multiple Sessions on Dialer Interfaces

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number* [**name-tag**]
4. **ppp enable group** *group-name*
5. **pppoe-client dial-pool-number** *number*
6. **pppoe-client dial-pool-number** *number*
7. **pppoe-client dial-pool-number** *number*
8. **exit**
9. **interface** *type number* [**name-tag**]
10. **dialer pool** *number*
11. **service-policy output** *name*
12. **exit**
13. **interface** *type number* [**name-tag**]
14. **dialer pool** *number*
15. **service-policy output** *name*
16. **exit**
17. **interface** *type number* [**name-tag**]
18. **dialer pool** *number*
19. **service-policy output** *name*
20. **exit**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **interface** *type number* [**name-tag**]<br>**Example:**<br>`Device(config)# interface Ethernet 0/0` | Configures an interface type and enters interface configuration mode.<br>• Enter the interface type, number, and name. |
| **Step 4** | **ppp enable group** *group-name*<br>**Example:**<br>`Device(config-if)# ppp enable group global` | Enables PPPoE sessions on an Ethernet interface or subinterface. |
| **Step 5** | **pppoe-client dial-pool-number** *number*<br>**Example:**<br>`Device(config-if)# pppoe-client dial-pool-number 1` | Configures a PPPoE client and to specify the dial-on-demand routing (DDR) functionality. |
| **Step 6** | **pppoe-client dial-pool-number** *number*<br>**Example:**<br>`Device(config-if)# pppoe-client dial-pool-number 2` | Configures a PPPoE client and to specify the dial-on-demand routing (DDR) functionality. |
| **Step 7** | **pppoe-client dial-pool-number** *number*<br>**Example:**<br>`Device(config-if)# pppoe-client dial-pool-number 3` | Configures a PPPoE client and to specify the dial-on-demand routing (DDR) functionality. |
| **Step 8** | **exit**<br>**Example:**<br>`Device(config-if)# exit` | Exits interface configuration mode. |
| **Step 9** | **interface** *type number* [**name-tag**]<br>**Example:** | Configures an interface type and enters interface configuration mode.<br>• Enter the interface type and number. |

| | Command or Action | Purpose |
|---|---|---|
| | `Device(config)# interface Dialer 0` | |
| **Step 10** | **dialer pool** *number*<br>**Example:**<br>`Device(config-if)# dialer pool 1` | Specifies the dialing pool that the dialer interface uses to connect to a specific destination subnetwork. |
| **Step 11** | **service-policy output** *name*<br>**Example:**<br>`Device(config-if)# service-policy output dialer-output-sp` | Attaches a policy map to an output interface that will be used as the service policy for the interface. |
| **Step 12** | **exit**<br>**Example:**<br>`Device(config-if)# exit` | Exits interface configuration mode. |
| **Step 13** | **interface** *type number* [**name-tag**]<br>**Example:**<br>`Device(config)# interface Dialer 1` | Configures an interface type and enters interface configuration mode.<br>• Enter the interface type and number. |
| **Step 14** | **dialer pool** *number*<br>**Example:**<br>`Device(config-if)# dialer pool 2` | Specifies the dialing pool that the dialer interface uses to connect to a specific destination subnetwork. |
| **Step 15** | **service-policy output** *name*<br>**Example:**<br>`Device(config-if)# service-policy output dialer-output-sp` | Attaches a policy map to an output interface that will be used as the service policy for the interface. |
| **Step 16** | **exit**<br>**Example:**<br>`Device(config-if)# exit` | Exits interface configuration mode. |
| **Step 17** | **interface** *type number* [**name-tag**]<br>**Example:**<br>`Device(config)# interface Dialer 2` | Configures an interface type and enters interface configuration mode.<br>• Enter the interface type and number. |
| **Step 18** | **dialer pool** *number*<br>**Example:** | Specifies the dialing pool that the dialer interface uses to connect to a specific destination subnetwork. |

| | Command or Action | Purpose |
|---|---|---|
| | `Device(config-if)# dialer pool 3` | |
| **Step 19** | **service-policy output** *name*<br>**Example:**<br>`Device(config-if)# service-policy output dialer-output-sp` | Attaches a policy map to an output interface that will be used as the service policy for the interface. |
| **Step 20** | **exit**<br>**Example:**<br>`Device(config-if)# exit` | Exits interface configuration mode. |

## Applying CoS Values to a Dialer Interface

Class of Service (CoS) values are set by applying a policy to the dialer interface.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map** *policy-map-name*
4. **class class-default**
5. **set cos** *cos-value*
6. **exit**
7. **exit**
8. **interface** *type number* [**name-tag**]
9. **service-policy output** *name*
10. **exit**
11. **interface** *type number* [**name-tag**]
12. **encapsulation** *encapsulation-type*
13. **pppoe-client dial-pool-number** *number*
14. **exit**

### DETAILED STEPS

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

| | Command or Action | Purpose |
|---|---|---|
| | `Device# configure terminal` | |
| **Step 3** | **policy-map** *policy-map-name*<br>**Example:**<br>`Device(config)# policy-map output_cos` | Specifies the name of the policy map created earlier and enters policy-map configuration mode.<br>• Enter the policy map name. |
| **Step 4** | **class class-default**<br>**Example:**<br>`Device(config-pmap)# class class-default` | Creates the default class for traffic classification and enters policy-map class configuration mode. |
| **Step 5** | **set cos** *cos-value*<br>**Example:**<br>`Device(config-pmap-c)# set cos 1` | Specifies an IEEE 802.1Q CoS value from 0 to 7. |
| **Step 6** | **exit**<br>**Example:**<br>`Device(config-pmap-c)# exit` | Returns to policy-map configuration mode. |
| **Step 7** | **exit**<br>**Example:**<br>`Device(config-pmap)# exit` | Returns to global configuration mode. |
| **Step 8** | **interface** *type number* [**name-tag**]<br>**Example:**<br>`Device(config)# interface Dialer 1` | Configures an interface type and enters interface configuration mode.<br>• Enter the interface type and number. |
| **Step 9** | **service-policy output** *name*<br>**Example:**<br>`Device(config-if)# service-policy output output-cos` | Attaches a policy map to an output interface that will be used as the service policy for the interface. |
| **Step 10** | **exit**<br>**Example:**<br>`Device(config-if)# exit` | Exits interface configuration mode. |
| **Step 11** | **interface** *type number* [**name-tag**]<br>**Example:**<br>`Device(config)# interface Ethernet 0.10` | Configures an interface type and enters sub-interface configuration mode.<br>• Enter the interface type and number. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 12** | **encapsulation** *encapsulation-type*<br>**Example:**<br>`Device(config-subif)# encapsulation dot1q 10` | Sets the encapsulation method used by the interface. |
| **Step 13** | **pppoe-client dial-pool-number** *number*<br>**Example:**<br>`Device(config-subif)# pppoe-client dial-pool-number 1` | Configures a PPPoE client and to specify the dial-on-demand routing (DDR) functionality. |
| **Step 14** | **exit**<br>**Example:**<br>`Device(config-subif)# exit` | Returns to global configuration mode. |

# Configuration Examples for Shaping on Dialer Interfaces

## Example: Configuring Output Queuing Policy for a Dialer Interface

The following example shows how to configure parent and child policy maps and how to attach the parent map to the dialer interface:

```
Device(config)# policy-map childExample
 Device(config-pmap)# class voice
  Device(config-pmap-c)# priority percent 30
  Device(config-pmap-c)# exit

 Device(config-pmap)# class video
  Device(config-pmap-c)# bandwidth percent 50
  Device(config-pmap-c)# exit

 Device(config-pmap)# class class-default
  Device(config-pmap-c)# fair-queue
  Device(config-pmap-c)# exit

Device(config)# policy-map parent
 Device(config-pmap)# class class-default
  Device(config-pmap-c)# shape average 1000000
  Device(config-pmap-c)# service-policy child
  Device(config-pmap-c)# exit

Device(config)# interface dialer 0
 Device(config-if)# service-policy output parent
```

## Example: Configuring QoS for PPPoEoA for a Dialer Interface

```
Device(config)# interface ATM 0
 Device(config-if)# no ip address
 Device(config-if)# no atm ilmi-keepalive
```

```
 Device(config-if)# exit

Device(config)# interface ATM 0.1 point-to-point
 Device(config-if)# ip address 192.168.0.0 255.255.255.224
 Device(config-if)# pvc 4/46
  Device(config-if-atm-vc)# vbr-nrt 738 738
  Device(config-if-atm-vc)# pppoe-client dial-pool-number 1
  Device(config-if-atm-vc)# exit
 Device(config-if)# exit

Device(config)# interface Dialer 0
 Device(config-if)# mtu 1200
 Device(config-if)# ip address 172.16.0.0 255.0.0.0
 Device(config-if)# encapsulation ppp
 Device(config-if)# dialer pool 1
 Device(config-if)# dialer-group 1
 Device(config-if)# service-policy output dialer-output-sp
!
Device(config)# dialer-list 1 protocol ip permit
```

## Example: Configuring QoS for a PPPoE on a Dialer Interface

```
Device(config)# interface ethernet 0/0
 Device(config-if)# pppoe enable group global
 Device(config-if)# pppoe-client dial-pool-number 1
 Device(config-if)# exit

Device(config)# interface Dialer 0
 Device(config-if)# mtu 1200
 Device(config-if)# ip address 172.16.0.0 255.0.0.0
 Device(config-if)# encapsulation ppp
 Device(config-if)# dialer pool 1
 Device(config-if)# dialer-group 1
 Device(config-if)# service-policy output dialer-output-sp
 Device(config-if)# exit

Device(config)# dialer-list 1 protocol ip permit
```

## Example: Configuring QoS for PPPoA on a Dialer Interface

```
Device(config)# interface ATM 0.1 point-to-point
 Device(config-if)# ip address 192.168.0.0 255.255.255.224
 Device(config-if)# pvc 4/46
  Device(config-if-atm-vc)# vbr-nrt 738 738
  Device(config-if-atm-vc)# dialer pool-member 1
  Device(config-if-atm-vc)# protocol ppp dialer
  Device(config-if-atm-vc)# exit
 Device(config-if)# exit

Device(config)# interface Dialer 0
 Device(config-if)# mtu 1200
 Device(config-if)# ip address 172.16.0.0 255.0.0.0
 Device(config-if)# encapsulation ppp
 Device(config-if)# dialer pool 1
 Device(config-if)# dialer-group 1
 Device(config-if)# service-policy output dialer-output-sp
 Device(config-if)# exit
```

```
Device(config)# dialer-list 1 protocol ip permit
```

## Example: Configuring QoS for Multiple Sessions on a Dialer Interface

```
Device(config)# interface ethernet 0/0
 Device(config-if)# pppoe enable group global
 Device(config-if)# pppoe-client dial-pool-number 1
 Device(config-if)# pppoe-client dial-pool-number 2
 Device(config-if)# pppoe-client dial-pool-number 3
 Device(config-if)# exit

Device(config)# interface Dialer 0
 Device(config-if)# dialer pool 1
 Device(config-if)# service-policy output dialer-output-sp
 Device(config-if)# exit

Device(config)# interface Dialer 1
 Device(config-if)# dialer pool 2
 Device(config-if)# service-policy output dialer-output-sp
 Device(config-if)# exit

Device(config)# interface Dialer 2
 Device(config-if)# dialer pool 3
 Device(config-if)# service-policy output dialer-output-sp
 Device(config-if)# exit
```

## Example: Applying CoS Values to a Dialer Interface

```
Device> enable
Device# configure terminal
Device(config)# policy-map output_cos
Device(config-pmap)# class class-default
Device(config-pmap-c)# set cos 1
Device(config-pmap-c)# exit
Device(config-pmap)# exit
Device(config)# interface Dialer 1
Device(config-if)# service-policy output output-cos
Device(config-if)# exit
Device(config)# interface Ethernet 0.10
Device(config-subif)# encapsulation dot1q 10
Device(config-subif)# pppoe-client dial-pool-number 1
Device(config-subif)# exit
```

# Additional References for Shaping on Dialer Interfaces

### Related Documents

| Related Topic | Document Title |
|---|---|
| Cisco IOS commands | Cisco IOS Master Commands List, All Releases |

| Related Topic | Document Title |
|---|---|
| QoS commands | *Cisco IOS Quality of Service Solutions Command Reference* |
| MQC | *QoS: Modular QoS: Command-Line Interface Configuration Guide* |

### Technical Assistance

| Description | Link |
|---|---|
| The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password. | http://www.cisco.com/cisco/web/support/index.html |

# Feature Information for Shaping on Dialer Interfaces

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

***Table 9: Feature Information for Shaping on Dialer Interfaces***

| Feature Name | Releases | Feature Information |
|---|---|---|
| Shaping on Dialer Interfaces | 15.3(1)T<br>Cisco IOS XE Release 3.13S | The Shaping on Dialer Interfaces feature provides support for PPPoE/A configurations on dialer interfaces. |