QoS: Regulating Packet Flow Configuration Guide, Cisco IOS XE Everest 16.6

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.

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: http://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. (1110R)

© 2014–2017 Cisco Systems, Inc. All rights reserved.

CONTENTS

CHAPTER 1 **Read Me First** 1

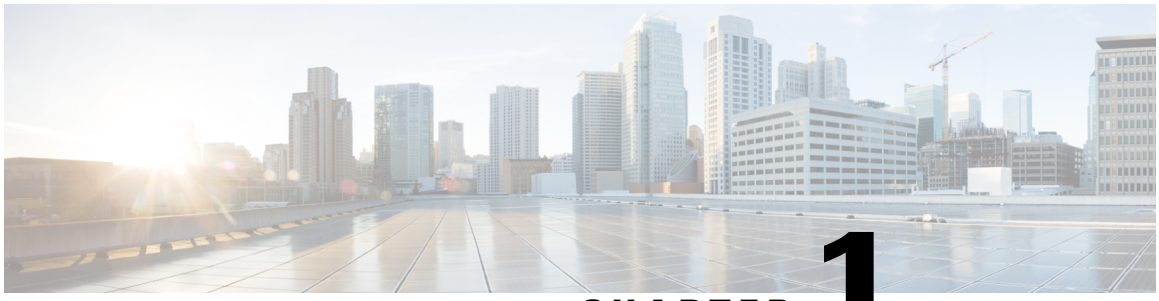
CHAPTER 2 **Regulating Packet Flow Using Traffic Shaping** 3

- Finding Feature Information 3
- Information About Traffic Shaping 3
  - Benefits of Shaping Traffic on a Network 3
  - Token Bucket and Traffic Shaping 4
  - Traffic Shaping and Rate of Transfer 5
  - How Traffic Shaping Regulates Traffic 6
  - Traffic Shaping versus Traffic Policing 6
- Additional References 7

CHAPTER 3 **Regulating Packet Flow on a Per-Class Basis Using Class-Based Traffic Shaping** 11

- Finding Feature Information 11
- Prerequisites for Configuring Class-Based Traffic Shaping 12
- Restrictions for Configuring Class-Based Traffic Shaping 12
- Information About Class-Based Traffic Shaping 12
  - Class-Based Traffic Shaping Functionality 12
  - Benefits of Class-Based Traffic Shaping 13
  - Hierarchical Policy Map Structure of Class-Based Traffic Shaping 13
- How to Configure Class-Based Traffic Shaping 14
  - Configuring Class-Based Traffic Shaping in a Primary-Level Policy Map 14
    - What to Do Next 16
  - Configuring the Secondary-Level Policy Map 16
- Configuration Examples for Class-Based Traffic Shaping 18
  - Example Class-Based Traffic Shaping Configuration 18
- Where to Go Next 18
- Additional References 19

Feature Information for Class-Based Traffic Shaping 20



CHAPTER 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.

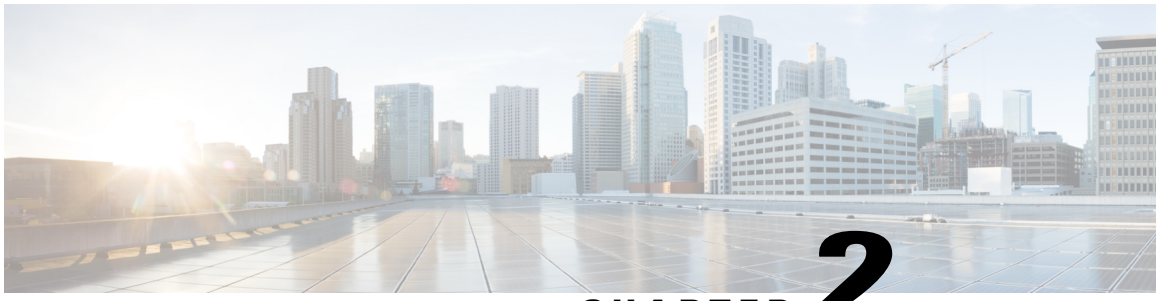
Related References

- 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.



CHAPTER 2

Regulating Packet Flow Using Traffic Shaping

This module contains an overview of regulating the packet flow on a network. Regulating the packet flow (that is, the flow of traffic) on the network is also known as traffic shaping. Traffic shaping allows you to control the speed of traffic that is leaving an interface. This way, you can match the flow of the traffic to the speed of the interface that is receiving the packet. Cisco provides a traffic-regulating mechanism called Class-Based Traffic Shaping. Before configuring this mechanism, it is important that you understand the overview presented in this module.

- Finding Feature Information, page 3
- Information About Traffic Shaping, page 3
- Additional References, page 7

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.

Information About Traffic Shaping

Benefits of Shaping Traffic on a Network

- Traffic shaping allows you to control the traffic going out an interface, matching the traffic flow to the speed of the interface.
- It ensures that traffic conforms to the policies contracted for it.
- It helps to ensure that a packet adheres to a stipulated contract, and it determines the appropriate quality of service to apply to the packet.

- It avoids bottlenecks and data-rate mismatches. For instance, central-to-remote site data speed mismatches.
- It prevents packet loss.

Here are some scenarios for which you would use traffic shaping:

- Control access to bandwidth when, for example, policy dictates that the rate of a given interface should not on the average exceed a certain rate even though the access rate exceeds the speed.
- Configure traffic shaping on an interface if you have a network with differing access rates. Suppose that one end of the link in a network runs at 256 kbps and the other end of the link runs at 128 kbps. Sending packets at 256 kbps could cause failure of the applications using the link.

A similar, more complicated case would be a link-layer network giving indications of congestion that has differing access rates on different attached data terminal equipment (DTE); the network may be able to deliver more transit speed to a given DTE device at one time than another. (This scenario warrants that the token bucket be derived and that then its rate be maintained.)

- Offer a subrate service. In this case, traffic shaping enables you to use the router to partition your T1 or T3 links into smaller channels.

Token Bucket and Traffic Shaping

Traffic shaping uses a token bucket metaphor to shape traffic. A token bucket is a formal definition of a rate of transfer. It has three components: a burst size, a mean rate, and a time interval (Tc). Although the mean rate is generally represented as bits per second, any two values may be derived from the third by the relation shown as follows:

```
mean rate = burst size / time interval
```

Here are some definitions of these terms:

- Mean rate--Also called the committed information rate (CIR), it specifies how much data can be sent or forwarded per unit time on average.
- Burst size--Also called the committed burst (Bc) size, it specifies in bits (or bytes) per burst how much traffic can be sent within a given unit of time to not create scheduling concerns. (For a traffic shaper, it specifies bits per burst.)
- Time interval--Also called the measurement interval, it specifies the time quantum in seconds per burst.

By definition, over any integral multiple of the interval, the bit rate of the interface will not exceed the mean rate. The bit rate, however, may be arbitrarily fast within the interval.

A token bucket is used to manage a device that regulates the data in a flow. For example, the regulator might be a traffic shaper. A token bucket itself has no discard or priority policy. Rather, a token bucket discards tokens and leaves to the flow the problem of managing its transmission queue if the flow overdrives the regulator.

In the token bucket metaphor, tokens are put into the bucket at a certain rate. The bucket itself has a specified capacity. If the bucket fills to capacity, newly arriving tokens are discarded. Each token is permission for the source to send a certain number of bits into the network. To send a packet, the regulator must remove from the bucket a number of tokens equal in representation to the packet size.

If not enough tokens are in the bucket to send a packet, the packet waits until the bucket has enough tokens. If the bucket is already full of tokens, incoming tokens overflow and are not available to future packets. Thus,

at any time, the largest burst a source can send into the network is roughly proportional to the size of the bucket.

Note that the token bucket mechanism used for traffic shaping has both a token bucket and a data buffer, or queue; if it did not have a data buffer, it would be a traffic policer. For traffic shaping, packets that arrive that cannot be sent immediately are delayed in the data buffer.

For traffic shaping, a token bucket permits burstiness but bounds it. It guarantees that the burstiness is bounded so that the flow will never send faster than the capacity of the token bucket plus the time interval multiplied by the established rate at which tokens are placed in the bucket. It also guarantees that the long-term transmission rate will not exceed the established rate at which tokens are placed in the bucket.

Traffic Shaping and Rate of Transfer

Traffic shaping limits the rate of transmission of data. You can limit the data transfer to one of the following:

- A specific configured rate
- A derived rate based on the level of congestion

As mentioned, the rate of transfer depends on these three components that constitute the token bucket: burst size, mean rate, time (measurement) interval. The mean rate is equal to the burst size divided by the interval.

When traffic shaping is enabled, the bit rate of the interface will not exceed the mean rate over any integral multiple of the interval. In other words, during every interval, a maximum of burst size can be sent. Within the interval, however, the bit rate may be faster than the mean rate at any given time.

One additional variable applies to traffic shaping: excess burst (Be) size. The Be size corresponds to the number of noncommitted bits--those outside the CIR--that are still accepted by the switch but marked as discard eligible (DE).

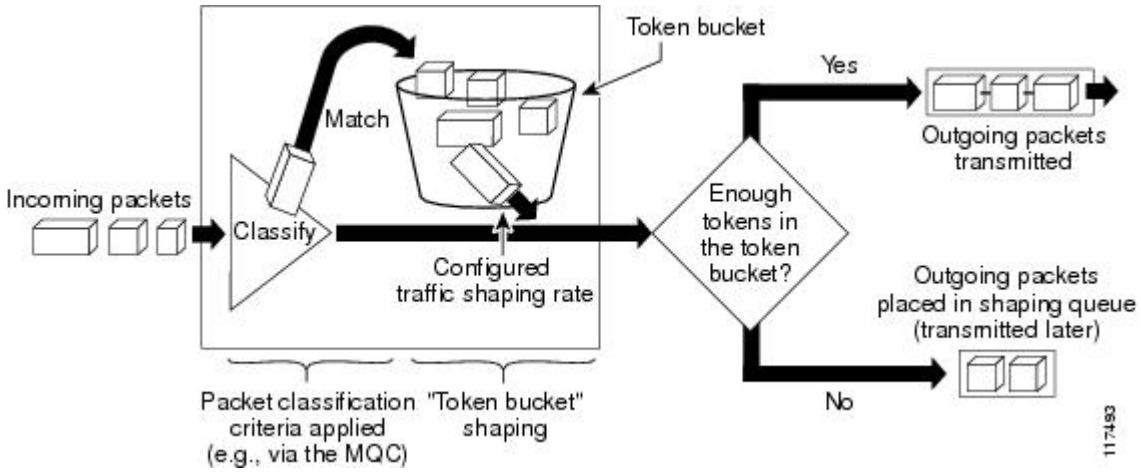
In other words, the Be size allows more than the burst size to be sent during a time interval in certain situations. The switch will allow the packets belonging to the excess burst to go through but it will mark them by setting the DE bit. Whether the packets are sent depends on how the switch is configured.

When the Be size equals 0, the interface sends no more than the burst size every interval, achieving an average rate no higher than the mean rate. However, when the Be size is greater than 0, the interface can send as many as Bc plus Be bits in a burst, if in a previous time period the maximum amount was not sent. Whenever less than the burst size is sent during an interval, the remaining number of bits, up to the Be size, can be used to send more than the burst size in a later interval.

How Traffic Shaping Regulates Traffic

The figure below illustrates how a traffic shaping mechanism regulates traffic.

Figure 1: How a Traffic-Shaping Mechanism Regulates Traffic



In the figure above, incoming packets arrive at an interface. The packets are classified using a "classification engine," such as an access control list (ACL) or the Modular Quality of Service Command-Line Interface (MQC). If the packet matches the specified classification, the traffic shaping mechanism continues. Otherwise, no further action is taken.

Packets matching the specified criteria are placed in the token bucket. The maximum size of the token bucket is the Bc size plus the Be size. The token bucket is filled at a constant rate of Bc worth of tokens at every Tc. This is the configured traffic shaping rate.

If the traffic shaping mechanism is active (that is, packets exceeding the configured traffic shaping rate already exist in a transmission queue), at every Tc, the traffic shaper checks to see if the transmission queue contains enough packets to send (that is, up to either Bc (or Bc plus Be) worth of traffic).

If the traffic shaper is not active (that is, there are no packets exceeding the configured traffic shaping rate in the transmission queue), the traffic shaper checks the number of tokens in the token bucket. One of the following occurs:

- If there are enough tokens in the token bucket, the packet is sent (transmitted).
- If there are not enough tokens in the token bucket, the packet is placed in a shaping queue for transmission at a later time.

Traffic Shaping versus Traffic Policing

Although traffic shaping and traffic policing can be implemented together on the same network, there are distinct differences between them, as shown in the table below.

Table 1: Differences Between Traffic Shaping and Traffic Policing

	Traffic Shaping	Traffic Policing
Triggering Event	• Occurs automatically at regular intervals (Tc). or Occurs whenever a packet arrives at an interface.	• Occurs whenever a packet arrives at an interface.
What it Does	• Classifies packets. • If packet does not meet match criteria, no further action is taken. • Packets meeting match criteria are sent (if there are enough tokens in the token bucket) or Packets are placed in a queue for transmission later. • If the number of packets in the queue exceed the queue limit, the packets are dropped.	• Classifies packets. • If packet does not meet match criteria, no further action is taken. • Packets meeting match criteria and conforming to, exceeding, or violating a specified rate, receive the configured policing action (for example, drop, send, mark then send). • Packets are not placed in queue for transmission later.

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
QoS commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	*Cisco IOS Quality of Service Solutions Command Reference*
Packet classification	"Classifying Network Traffic" module
MQC, policy maps, class maps, and hierarchical policy maps	"Applying QoS Features Using the MQC" module
WFQ, CBWFQ, PQ, CQ, FIFO and other queueing mechanisms	"Congestion Management Overview" module

Related Topic	Document Title
Class-Based Traffic Shaping	"Regulating Packet Flow on a Per-Class Basis -- Using Class-Based Traffic Shaping" module
GTS	"Regulating Packet Flow on a Per-Interface Basis -- Using Generic Traffic Shaping" module
FRTS	"MQC-Based Frame Relay Traffic Shaping" module

Standards

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

MIBs

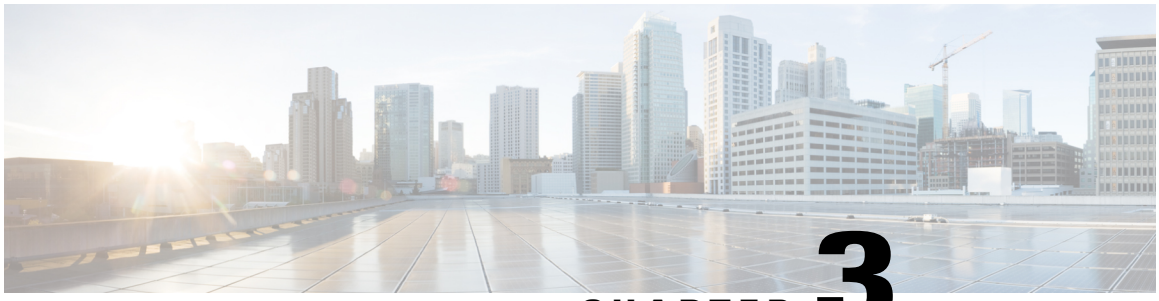
MIBs	MIBs Link
No new or modified MIBs are supported, and support for existing MIBs has not been modified.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	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



CHAPTER 3

Regulating Packet Flow on a Per-Class Basis Using Class-Based Traffic Shaping

Packet flow on a network can be regulated using a traffic shaping mechanism. One such traffic shaping mechanism is a Cisco feature called Class-Based Traffic Shaping. Class-Based Traffic Shaping allows you to regulate the flow of packets (on a per-traffic-class basis) going out an interface, matching the packet flow to the speed of the interface. This module describes the concepts and tasks related to configuring Class-Based Traffic Shaping.

- Finding Feature Information, page 11
- Prerequisites for Configuring Class-Based Traffic Shaping, page 12
- Restrictions for Configuring Class-Based Traffic Shaping, page 12
- Information About Class-Based Traffic Shaping, page 12
- How to Configure Class-Based Traffic Shaping, page 14
- Configuration Examples for Class-Based Traffic Shaping, page 18
- Where to Go Next, page 18
- Additional References, page 19
- Feature Information for Class-Based Traffic Shaping, page 20

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.

Prerequisites for Configuring Class-Based Traffic Shaping

Be familiar with the concepts in the "Regulating Packet Flow Using Traffic Shaping" module.

Use Feature Navigator to determine if the platform in use supports Class-Based Traffic Shaping. Access Cisco Feature Navigator at http://www.cisco.com/go/fn .

Distributed Cisco Express Forwarding (dCEF) must be enabled if the customer is using a Versatile Interface Processor (VIP) on the router.

A policy map and a class map must be created first using the Modular Quality of Service (QoS) Command-Line Interface (MQC).

Restrictions for Configuring Class-Based Traffic Shaping

Adaptive traffic shaping for Frame Relay networks is supported for Frame Relay networks only.

Class-Based Traffic Shaping applies to outbound traffic only.

Class-Based Traffic Shaping does not support the following commands:

- **traffic-shape adaptive**
- **traffic shape fecn-adaptive**
- **traffic-shape group**
- **traffic-shape rate**

Information About Class-Based Traffic Shaping

Class-Based Traffic Shaping Functionality

Class-Based Traffic Shaping is a traffic shaping mechanism (also known as a "traffic shaper"). A traffic shaper typically delays excess traffic using a buffer, or queueing mechanism, to hold packets and shape the flow when the data rate of the source is higher than expected. It holds and shapes traffic to a particular bit rate by using the token bucket mechanism. For more information about token buckets and traffic shaping, see the "Regulating Packet Flow Using Traffic Shaping" module.

Class-Based Traffic Shaping is the Cisco-recommended traffic shaping mechanism.

Note Class-Based Traffic Shaping should be used instead of what was previously referred to as Distributed Traffic Shaping (DTS). Class-Based Traffic Shaping can and should be used on the Cisco 7500 series router with a VIP2-40, VIP2-50, or greater processor.

Using the Class-Based Traffic Shaping, you can perform the following tasks:

- Configure traffic shaping on a per-traffic-class basis. It allows you to fine-tune traffic shaping for one or more classes and it allows you to configure traffic shaping on a more granular level.

- Specify average rate or peak rate traffic shaping. Specifying peak rate shaping allows you to make better use of available bandwidth by allowing more data than the configured traffic shaping rate to be sent if the bandwidth is available.
- Configure traffic shaping in a hierarchical policy map structure. That is, traffic shaping is configured in a primary-level (parent) policy map and other QoS features (for instance, CBWFQ and traffic policing) can be configured in the secondary-level (child) policy maps. For more information, see the Hierarchical Policy Map Structure of Class-Based Traffic Shaping, on page 13.

Benefits of Class-Based Traffic Shaping

All of the benefits associated with traffic shaping also apply to Class-Based Traffic Shaping, but on a more granular level. For information about the benefits of traffic shaping, see the "Regulating Packet Flow Using Traffic Shaping" module.

Hierarchical Policy Map Structure of Class-Based Traffic Shaping

With the Class-Based Traffic Shaping mechanism, traffic shaping can be configured in a hierarchical policy map structure; that is, traffic shaping is enabled in a primary-level (parent) policy map and other QoS features used with traffic shaping, such as CBWFQ and traffic policing, can be enabled in a secondary-level (child) policy map.

Traffic shaping is enabled by using the **shape** command (and specifying a rate) in a policy map. When traffic shaping is enabled, one the following actions occur:

- Packets exceeding the specified rate are placed in a queue using an appropriate queueing mechanism.
- Packets conforming to the specified rate are transmitted.

When packets are placed in a queue, the default queueing mechanism used is weighted fair queueing (WFQ). However, with Class-Based Traffic Shaping, class-based WFQ (CBWFQ) can be configured as an alternative queueing mechanism.

CBWFQ allows you to fine-tune the way traffic is placed in a queue. For instance, you can specify that all voice traffic be placed in a high-priority queue and all traffic from a specific class be placed in a lower-priority queue.

If you want to use CBWFQ with the Class-Based Traffic Shaping mechanism, the following conditions must be met:

- A secondary-level (child) policy map *must* be created. This secondary-level (child) policy map is then used to configure CBWFQ by enabling the **bandwidth** command.
- Traffic shaping *must* be configured in the primary-level (parent) policy map.

Note CBWFQ is supported in both the primary-level (parent) policy map and the secondary-level (child) policy map. However, to use CBWFQ at the secondary-level (child) policy map, traffic shaping *must* be configured in the primary-level (parent) policy map.

The following sample configuration illustrates how the Class-Based Traffic Shaping mechanism is configured in a hierarchical policy map structure:

```
enable
configure terminal
 policy-map policy_parent        ! This is the primary-level policy map.
  class class-default
   shape average 1000000         ! This enables traffic shaping.
   service-policy policy_child   ! This associates the policy maps.
```

Traffic shaping must be configured in the primary-level (parent) policy map. With this configuration, WFQ is used as the default queueing mechanism for placing all the traffic in a queue.

In the following secondary-level (child) policy map, the alternative queueing mechanism CBWFQ is configured:

```
enable
configure terminal
 policy-map policy_child     ! This is the secondary-level policy map.
  class class-default
   bandwidth percent 50      ! This enables CBWFQ.
```

In the secondary-level (child) policy map, additional QoS features used with traffic shaping (for example, CBWFQ and traffic policing) are typically configured. For Class-Based Traffic Shaping, the only two QoS features supported at the secondary-level (child) policy map are CBWFQ and traffic policing.

How to Configure Class-Based Traffic Shaping

Configuring Class-Based Traffic Shaping in a Primary-Level Policy Map

Traffic shaping is configured in a policy map. Policy maps determine the specific quality of service (QoS) feature that will be applied to traffic on a network. In this module, the QoS feature being applied is traffic shaping.

Traffic shaping is configured in the primary-level (parent) policy map in the hierarchy.

Before You Begin

Before configuring traffic shaping, you must use the MQC to create a policy map and a class map.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map** *policy-map-name*
4. **class** {*class-name* | **class-default**}
5. **shape** [**average** | **peak**] *mean-rate* [*burst-size*] [*excess-burst-size*]
6. **service-policy** *policy-map-name*
7. **end**
8. **show policy-map**
9. **show policy-map interface** *type number*
10. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**policy-map** *policy-map-name* **Example:** `Router(config)# policy-map policy_parent`	Specifies the name of the policy map created earlier and enters policy-map configuration mode. See Prerequisites for Configuring Class-Based Traffic Shaping, on page 12 for more information. • Enter the policy map name.
Step 4	**class** {*class-name* | **class-default**} **Example:** `Router(config-pmap)# class class-default`	Specifies the name of the class whose policy you want to create and enters policy-map class configuration mode. • Enter the name of the class or enter the **class-default**keyword.
Step 5	**shape** [**average** | **peak**] *mean-rate* [*burst-size*] [*excess-burst-size*] **Example:** `Router(config-pmap-c)# shape average 1000000`	Shapes traffic according to the keyword and rate specified. • Enter the keyword and rate.
Step 6	**service-policy** *policy-map-name* **Example:** `Router(config-pmap-c)# service-policy policy_child`	Uses a service policy as a QoS policy within a policy map (called a hierarchical service policy). • Enter the policy map name.
Step 7	**end** **Example:** `Router(config-pmap-c)# end`	Returns to privileged EXEC mode.
Step 8	**show policy-map** **Example:** `Router# show policy-map`	(Optional) Displays all configured policy maps.

	Command or Action	Purpose

Step 9	**show policy-map interface** *type number*
	
	Example:
	
	`Router#`
	`show policy-map interface serial4/0`
		(Optional) Displays the packet statistics of all classes that are configured for all service policies either on the specified interface or subinterface or on a specific PVC on the interface.
		
		• Enter the interface type and number.

Step 10	**exit** **Example:** `Router# exit`	(Optional) Exits privileged EXEC mode.

What to Do Next

To configure a secondary-level (child) policy map in the hierarchical policy map structure (an optional task), proceed with the instructions in Configuring the Secondary-Level Policy Map.

Configuring the Secondary-Level Policy Map

Note CBWFQ is supported in both the primary-level (parent) policy map and the secondary-level (child) policy map. However, to use CBWFQ in the secondary-level (child) policy map, traffic shaping *must* be configured in the primary-level (parent) policy map. For more information about CBWFQ in a secondary-level (child) policy map, see the Hierarchical Policy Map Structure of Class-Based Traffic Shaping, on page 13.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map** *policy-map-name*
4. **class** {*class-name* | **class-default**}
5. **bandwidth** {*bandwidth-kbps* | **remaining percent** *percentage* | **percent** *percentage*}
6. **end**
7. **show policy-map**
8. **show policy-map interface** *type number*
9. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**policy-map** *policy-map-name* **Example:** `Router(config)# policy-map policy1`	Specifies the name of the policy map created earlier and enters policy-map configuration mode. See Prerequisites for Configuring Class-Based Traffic Shaping, on page 12 for more information. Enter the policy map name.
Step 4	**class** {*class-name* | **class-default**} **Example:** `Router(config-pmap)# class class-default`	Specifies the name of the class whose policy you want to create and enters policy-map class configuration mode. • Enter the name of the class or enter the **class-default** keyword.
Step 5	**bandwidth** {*bandwidth-kbps* | **remaining percent** *percentage* | **percent** *percentage*} **Example:** `Router(config-pmap-c)# bandwidth percent 50` **Example:**	Specifies or modifies the bandwidth allocated for a class belonging to a policy map. • Enter the amount of bandwidth as a number of kbps, a relative percentage of bandwidth, or an absolute amount of bandwidth. **Note** The **bandwidth** command used here is only an example of a QoS feature than can be configured. The **bandwidth** command configures CBWFQ. You could also use the **police** command to configure traffic policing.
Step 6	**end** **Example:** `Router(config-pmap-c)# end`	Returns to privileged EXEC mode.
Step 7	**show policy-map** **Example:** `Router# show policy-map`	(Optional) Displays all configured policy maps.

	Command or Action	Purpose

Step 8	**show policy-map interface** *type number*
	
	Example:
	
	`Router#`
	`show policy-map interface serial4/0`
		(Optional) Displays the packet statistics of all classes that are configured for all service policies either on the specified interface or subinterface or on a specific PVC on the interface.
		
		• Enter the interface type and number.

Step 9	**exit** **Example:** `Router# exit`	(Optional) Exits privileged EXEC mode.

Configuration Examples for Class-Based Traffic Shaping

Example Class-Based Traffic Shaping Configuration

The following is an example of Class-Based Traffic Shaping configured in a hierarchical policy map structure. In this example, two policy maps have been created; the primary-level (parent) policy map called "policy_parent," and a secondary-level (child) policy map called "policy_child." Traffic shaping is configured in the policy_parent policy map, and CBWFQ has been configured in the policy_child policy map.

The **service-policy** command associates the two policy maps in the hierarchical policy map structure.

```
enable
configure terminal
 policy-map policy_parent
  class class-default
   shape average 1000000         ! This enables traffic shaping.
   service-policy policy_child   ! This associates the policy maps.
   exit
  exit
 policy-map policy_child
  class class-default
   bandwidth percent 50   ! This enables CBWFQ.
   end
```

Where to Go Next

To configure Generic Traffic Shaping (GTS), see the "Regulating Packet Flow on a Per-Interface Basis Using Generic Traffic Shaping" module.

To configure Frame Relay Traffic Shaping (FRTS), see the "MQC-Based Frame Relay Traffic Shaping" module.

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
QoS commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	*Cisco IOS Quality of Service Solutions Command Reference*
Packet classification	"Classifying Network Traffic" module
MQC, policy maps, class maps, and hierarchical policy maps	"Applying QoS Features Using the MQC" module
CBWFQ and other queueing mechanisms	"Configuring Weighted Fair Queueing" module
Overview information about using traffic shaping to regulate packet flow on a network	"Regulating Packet Flow Using Traffic Shaping" module
GTS	"Regulating Packet Flow on a Per-Interface Basis Using Generic Traffic Shaping" module
FRTS	"MQC-Based Frame Relay Traffic Shaping" 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: 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 Class-Based Traffic Shaping

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 Class-Based Traffic Shaping

Feature Name	Software Releases	Feature Configuration Information
Distributed Traffic Shaping	12.2(8)T	Distributed Traffic Shaping (DTS) is a legacy method for regulating the flow of packets going out an interface. Class-Based Traffic Shaping should be used instead of (DTS).
Generic Traffic Shaping (GTS)	15.0(1)S	The GTS feature was integrated into the Cisco IOS Release 15.0(1)S release.