Cisco CMTS Router Quality of Service Features Configuration Guide

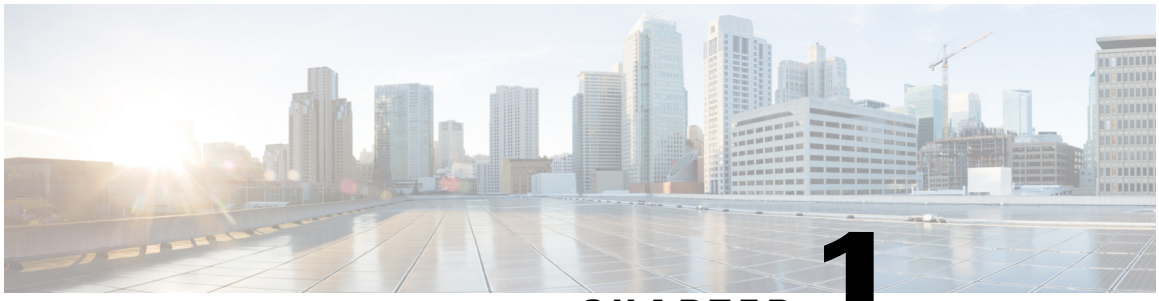
First Published: 2008-02-14

Last Modified: 2015-02-15

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

Text Part Number: OL-27611-02

CONTENTS



CHAPTER 1

Default DOCSIS 1.0 ToS Overwrite

First Published: February 14, 2008

Last Updated: May 10, 2010

Note Cisco IOS Release 12.2(33)SCA and later releases integrate support for this feature on the Cisco CMTS routers. This feature is also supported in Cisco IOS Release 12.3BC, and this document contains information that references many legacy documents related to Cisco IOS 12.3BC. In general, any references to Cisco IOS Release 12.3BC also apply to Cisco IOS Release 12.2SC.

This document describes the Default DOCSIS 1.0 ToS Overwrite feature for the Cisco Cable Modem Termination System (CMTS). This feature eliminates the need to create multiple QoS profiles in order to perform type of service (ToS) overwrite by enabling a default ToS overwrite to be bound to all DOCSIS 1.0 Cable Modem (CM) created profiles.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see 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 document.

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

Contents

Prerequisites for Default DOCSIS 1.0 ToS Overwrite

No special equipment or software is needed to use the Default DOCSIS 1.0 ToS Overwrite feature.

Restrictions for Default DOCSIS 1.0 ToS Overwrite

- The Default DOCSIS 1.0 ToS Overwrite feature is only applicable to CMs running DOCSIS version 1.0.
- Once the Default DOCSIS 1.0 ToS Overwrite feature is configured, all CMs will need to be reset in order for the effect to take place.
- Once the Default DOCSIS 1.0 ToS Overwrite feature is configured, all CMs will display the default values that were configured. After which, overwrite values can only be changed by editing the QoS profiles.

Information About Default DOCSIS 1.0 ToS Overwrite

To configure the Default DOCSIS 1.0 ToS Overwrite feature, you should understand the following topic:

Default DOCSIS 1.0 ToS Overwrite Overview

Currently, ToS overwrite requires the creation of static cable QoS profiles, which are assigned ToS fields and are than associated with 1.0 CMs. This implementation works well if only a few different service types are offered.

However, scalability issues arises when large numbers of service types are presented; each requiring a static QoS profile in order to perform ToS overwrite.

The Default DOCSIS 1.0 ToS Overwrite feature eliminates the need to create multiple QoS profiles in order to perform type-of-service (ToS) overwrite by automatically bounding all DOCSIS 1.0 Cable Modem (CM) created profiles to a default ToS overwrite.

DOCSIS

Created by CableLabs, Data Over Cable Service Interface Specification (DOCSIS) defines the interface standards and requirements for all cable modems associated with high-speed data distribution over a cable television system network.

The DOCSIS architecture consists of the following two components:

- Cable Modem (CM)
- Cable Modem Termination System (CMTS)

Each of these components are situated at different locations, often with the CM located on a customer site and the CMTS on the service provider site, and communication between the CM and CMTS is conducted over cable through DOCSIS.

Note Though there are several versions of DOCSIS available, the Default DOCSIS 1.0 ToS Overwrite feature is only applicable to CMs running DOCSIS 1.0.

Type-of-Service (ToS)

Tools such as type-of-service (ToS) bits identification make it possible to isolate network traffic by the type of application being used. ToS capabilities can be further expanded to isolate network traffic down to the specific brands, by the interface used, by the user type and individual user identification, or by the site address.

How to Configure Default DOCSIS 1.0 ToS Overwrite

The tasks in this section enables the use of the Default DOCSIS 1.0 ToS Overwrite feature.

Enabling Default DOCSIS 1.0 ToS Overwrite

All CMs with a DOCSIS 1.0 configuration file currently have their ToS overwrite default values are set to tos-and: 0xff and tos-or: 0x00. Since there were previously no mechanism in the DOCSIS 1.0 configuration file to specify the ToS overwrite, QoS profiles were created and assigned to the default ToS overwrites.

The following procedures enable the Default DOCSIS 1.0 ToS Overwrite feature, which will allow a default ToS overwrite to be bound to all CM created profiles.

Before You Begin

There are no prerequisites for these procedures.

Note

- The Default DOCSIS 1.0 ToS Overwrite feature is only applicable to CMs running DOCSIS version 1.0.
- Once the Default DOCSIS 1.0 ToS Overwrite feature is configured, all CMs will need to be reset in order for the effect to take place.
- Once the Default DOCSIS 1.0 ToS Overwrite feature is configured, all CMs will display the default values that were configured. After which, overwrite values can only be changed by editing the QoS profiles.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router> enable`	• Enter your password if prompted.
Step 2	**configureterminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable default-tos-qos10 tos-overwrite** *tos-and tos-or* **Example:** `Router(config)# cable default-tos-qos10 tos-overwrite 0x1F 0xE0`	Configures the ToS overwrite default value for the CM. This default value will be bound to all future CM created profiles.
Step 4	**end** **Example:** `Router(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

What to Do Next

After configuring the ToS overwrite default value, reset the CM using the **clear cable modem delete** command to allow the new ToS overwrite default value to take effect.

Editing QoS Profiles

Once the Default DOCSIS 1.0 ToS Overwrite feature is configured, additional ToS overwrite values can be changed by editing the QoS profiles.

DETAILED STEPS

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

	Command or Action	Purpose
Step 3	**cable qos profile** {*groupnum* | *ip-precedence* | *guaranteed-upstream* | *max-burst* | *max-upstream* | *max-downstream* | *priority* | *tos-overwrite* | *value* **Example:** `Router(config)# cable qos profile 4 guaranteed-upstream 2`	Configures the QoS profile.
Step 4	**end** **Example:** `Router(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Additional References

The following sections provide references related to the Default DOCSIS 1.0 ToS Overwrite feature.

Related Documents

Related Topic	Document Title
CMTS Commands	*Cisco Broadband Cable Command Reference Guide,* at the following URL: http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html
Cisco IOS Release 12.3 Commands	Cisco IOS Release 12.3 Configuration Guides and Command References, at the following URL http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/index.htm

Standards

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

MIBs

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

RFCs

RFC	Title
No new or modified RFCs are supported by this feature.	To locate and download Request for Comments (RFCs) and Internet Drafts, see the Internet Engineering Task Force (IETF) web site at the following URL: http://www.ietf.org/index.html

Technical Assistance

Description	Link
The Cisco Technical Support & Documentation website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, tools, and technical documentation. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/cisco/web/support/index.html

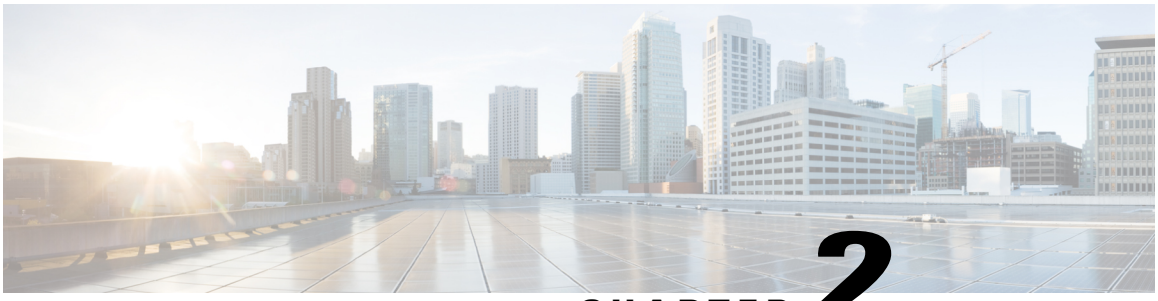
Feature Information for Default DOCSIS 1.0 ToS Overwrite

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note The table below 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.

Table 1: Feature Information for Default DOCSIS 1.0 ToS Overwrite

Feature Name	Releases	Feature Information
Default DOCSIS 1.0 ToS Overwrite	12.3(17a)BC2	This feature eliminates the need to create multiple QoS profiles in order to perform type of service (ToS) overwrite by enabling a default ToS overwrite to be bound to all DOCSIS 1.0 Cable Modem (CM) created profiles. The cable default-tos-qos10 tos-overwrite command was introduced by this feature.
Default DOCSIS 1.0 ToS Overwrite	12.2(33)SCD2	The priority of the QoS profile-2 is now configurable.



CHAPTER 2

DOCSIS 1.1 for the Cisco CMTS Routers

First Published: February 14, 2008

Last Updated: February 15, 2015

Note Cisco IOS Release 12.2(33)SCA integrates support for this feature on the Cisco CMTS routers. This feature is also supported in Cisco IOS Release 12.3BC, and this document contains information that references many legacy documents related to Cisco IOS Release12.3BC. In general, any references to Cisco IOS Release 12.3BC also apply to Cisco IOS Release 12.2SC.

This document describes how to configure the Cisco CMTS router for Data-over-Cable Service Interface Specifications (DOCSIS) 1.1 operations.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see 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 document.

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

Contents

Prerequisites for DOCSIS 1.1 Operations

To support DOCSIS 1.1 operations, the CMTS must be running Cisco IOS Release 12.1(4)BC1 or later Cisco IOS Release 12.2 BC, and the cable modem must also support the DOCSIS 1.1 feature set. In addition, before you power on and configure the Cisco CMTS, check the following points:

- Ensure that your network supports reliable broadband data transmission. Your plant must be swept, balanced, and certified, based on NTSC or appropriate international cable plant recommendations. Ensure that your plant meets all DOCSIS downstream and upstream RF requirements.
- Ensure that your Cisco CMTS is installed according to the instructions provided in the appropriate Hardware Installation Guide. The chassis must contain at least one port adapter to provide backbone connectivity and one Cisco cable line card to serve as the RF cable TV interface.
- Ensure that all other required headend or distribution hub routing and network interface equipment is installed, configured, and operational, based on the services to support. This includes all routers, servers (DHCP, TFTP, and ToD), network management systems, and other configuration or billing systems. This includes IP telephony equipment including gatekeepers and gateways; backbone and other equipment if supporting virtual private networks (VPNs); and dialup access servers, telephone circuits and connections and other equipment if supporting telco return.
- Ensure that DHCP and DOCSIS configuration files have been created and pushed to appropriate servers such that each cable modem, when initialized, can transmit a DHCP request, receive an IP address, obtain TFTP and ToD server addresses, and download DOCSIS configuration files. Optionally, ensure that your servers can also download updated software images to DOCSIS 1.0 and DOCSIS 1.1 cable modems.
- Ensure that customer premises equipment (CPE)—cable modems or set-top boxes, PCs, telephones, or facsimile machines—meet the requirements for your network and service offerings.
- Familiarize yourself with your channel plan to ensure assigning of appropriate frequencies. Outline your strategies for setting up bundling or VPN solution sets, if applicable, to your headend or distribution hub. Know your dial plan if using H.323 for VoIP services and setting up VoIP-enabled cable modem configuration files. Obtain passwords, IP addresses, subnet masks, and device names, as appropriate.
- Ensure that the system clocks on the Cisco CMTS and on the time-of-day (ToD) servers are synchronized. If this does not occur, the clocks on the CMs will not match the clocks on the Cisco CMTS, which could interfere with BPI+ operations. In particular, this could prevent the proper verification of the digital certificates on the cable modem (CM).

After these prerequisites are met, you are ready to configure the Cisco CMTS. This includes, at a minimum, configuring a host name and password for the Cisco CMTS and configuring the Cisco CMTS to support IP over the cable plant and network backbone.

Caution If you plan to use service-class-based provisioning, the service classes must be configured at the Cisco CMTS before cable modems attempt to make a connection. Use the **cable service class** command to configure service classes.

Restrictions for DOCSIS 1.1 Operations

DOCSIS 1.1 operations includes the following restrictions:

Baseline Privacy Interface Plus Requirements

BPI+ encryption and authentication must be supported and enabled by both the cable modem and CMTS. In addition, the cable modem must contain a digital certificate that conforms to the DOCSIS 1.1 and BPI+ specifications.

Also, ensure that the system clocks on the CMTS and on the time-of-day (ToD) servers are synchronized. If this does not occur, the clocks on the CMs will not match the clocks on the CMTS, which could interfere with BPI+ operations. In particular, this could prevent the proper verification of the digital certificates on the CM.

Note Ensure that the system clocks on the CMTS and on the time-of-day (ToD) servers are synchronized. If this does not occur, the clocks on the CMs will not match the clocks on the CMTS, which could interfere with BPI+ operations. In particular, this could prevent the proper verification of the digital certificates on the CM.

BPI+-Encrypted Multicast Not Supported with Bundled Subinterfaces on the Cisco uBR10012 Router

The current Cisco IOS releases do not support using BPI+ encrypted multicast on bundled cable subinterfaces on the Cisco uBR10012 router. Encrypted multicast is supported on bundled cable interfaces or on non-bundled cable subinterfaces, but not when a subinterface is bundled on the Cisco uBR10012 router. This restriction does not apply to Cisco uBR7200 series routers.

BPI+ Not Supported with High Availability Configurations

The current Cisco IOS releases do not support using BPI+ encrypted multicast on a cable interface when the interface has also been configured for N+1 (1:n) High Availability or Remote Processor Redundancy Plus (RPR+) High Availability redundancy.

In addition, BPI+ is not automatically supported after a switchover from the Working cable interface to the Protect cable interface, because the cable interface configurations that are required for BPI+ encryption are not automatically synchronized between the two interfaces. A workaround for this is to manually configure the Protect cable interfaces with the required configurations.

Cable Interface Cards

DOCSIS 1.1 traffic is supported on Cisco uBR-MC1XC and Cisco uBR-MC28C cable interface line cards. The Cisco uBR-MC11 (FPGA) and Cisco uBR-MC16B line cards do not support DOCSIS 1.1.

Cable Privacy Hotlist CLI Not Supported on Cisco uBR10012 Router

The **cable privacy hotlist** command is not supported on the Cisco uBR10012 router running Cisco IOS releases prior to Cisco IOS release 12.3(23)BC9, Cisco IOS release 12.2(33)SCB5, and Cisco IOS release12.2(33)SCC.

To add a manufacturer's or CM certificate to the hotlist on the Cisco uBR10012 router, use SNMP commands to set the appropriate attributes in DOCS-BPI-PLUS-MIB . See the Adding a Certificate as a Trusted Certificate Using SNMP Commands, on page 33.

DOCSIS Root Certificates

The Cisco CMTS supports only one DOCSIS Root CA certificate.

Maximum Burst Size

Previously, the maximum concatenated burst size parameter could be set to zero to specify an unlimited value. In a DOCSIS 1.1 environment, this parameter should be set to a nonzero value, with a maximum value of 1522 bytes for DOCSIS 1.0 cable modems.

If a cable modem attempts to register with a maximum concatenation burst size of zero, the DOCSIS 1.1 CMTS refuses to allow the cable modem to come online. This avoids the possibility that a DOCSIS 1.0 cable modem could interfere with voice traffic on the upstream by sending extremely large data packets. Since DOCSIS 1.0 does not support fragmentation, transmitting such data packets could result in unwanted jitter in the voice traffic.

In addition, DOCSIS 1.1 requires that the maximum transmit burst size be set to either 1522 bytes or the maximum concatenated burst size, whichever is larger. Do not set the maximum concatenation burst size to values larger than 1522 bytes for DOCSIS 1.0 cable modems.

Note This change requires you to change any DOCSIS configuration files that specify a zero value for the maximum concatenation burst size. This limitation does not exist for DOCSIS 1.1 cable modems unless fragmentation has been disabled.

Performance

DOCSIS 1.0 cable modems lack the ability to explicitly request and provide scheduling parameters for advanced DOCSIS 1.1 scheduling mechanisms, such as unsolicited grants and real-time polling. DOCSIS 1.1 cable modems on the same upstream channel can benefit from the advanced scheduling mechanisms and a DOCSIS 1.1 CMTS can still adequately support voice traffic from DOCSIS 1.1 cable modems with DOCSIS 1.0 cable modems on the same upstream channel.

Provisioning

The format and content of the TFTP configuration file for a DOCSIS 1.1 cable modem are significantly different from the file for a DOCSIS 1.0 cable modem. A dual-mode configuration file editor is used to generate a DOCSIS 1.0 style configuration file for DOCSIS 1.0 cable modems and a DOCSIS 1.1 configuration file for DOCSIS 1.1 cable modems.

Registration

A DOCSIS 1.1 CMTS must handle the existing registration Type/Length/Value parameters from DOCSIS 1.0 cable modems as well as the new type TLVs from DOCSIS 1.1 cable modems. A DOCSIS 1.0 and DOCSIS 1.1 cable modem can successfully register with the same DOCSIS 1.1 CMTS.

A DOCSIS 1.1 cable modem can be configured to make an indirect reference to a service class that has been statically defined at the CMTS instead of explicitly asking for the service class parameters. When this registration request is received by a DOCSIS 1.1 CMTS, it encodes the actual parameters of the service class in the registration response and expects a DOCSIS 1.1-specific registration-acknowledge MAC message from the cable modem.

When a DOCSIS 1.0 cable modem registers with a DOCSIS 1.1 CMTS, the registration request explicitly requests all nondefault service-class parameters in the registration. The absence of an indirect service class

reference eliminates the need for the DOCSIS 1.1 TLVs and eliminates the need to establish a local registration acknowledge wait state.

When a DOCSIS 1.1 CMTS receives a registration request from a DOCSIS 1.0 cable modem, it responds with the DOCSIS 1.0 style registration response and does not expect the cable modem to send the registration-acknowledge MAC message.

Information about DOCSIS 1.1

DOCSIS 1.1 is the first major revision of the initial DOCSIS 1.0 standard for cable networks. Although the initial standard provided quality data traffic over the coaxial cable network, the demands of real-time traffic such as voice and video required many changes to the DOCSIS specification.

The DOCSIS 1.1 specification provides the following feature enhancements over DOCSIS 1.0 networks:

Baseline Privacy Interface Plus

DOCSIS 1.0 introduced a Baseline Privacy Interface (BPI) to protect user data privacy across the shared-medium cable network and to prevent unauthorized access to DOCSIS-based data transport services across the cable network. BPI encrypts traffic across the RF interface between the cable modem and CMTS, and also includes authentication, authorization, and accounting (AAA) features.

BPI supports access control lists (ACLs), tunnels, filtering, protection against spoofing, and commands to configure source IP filtering on RF subnets to prevent subscribers from using source IP addresses that are not valid. DOCSIS 1.1 enhances these security features with BPI Plus (BPI+), which includes the following enhancements:

- X.509 Digital certificates provide secure user identification and authentication. The Cisco CMTS supports both self-signed manufacturer's certificates and certificates that are chained to the DOCSIS Root CA certificate.
- Key encryption uses 168-bit Triple DES (3DES) encryption that is suitable for the most sensitive applications.
- 1024-bit public key with Pkcs#1 Version 2.0 encryption.
- Support for encrypted multicast broadcasts, so that only authorized service flows receive a particular multicast broadcast.
- Secure software download allows a service provider to upgrade a cable modem's software remotely, without the risk of interception, interference, or alteration.

Concatenation

Concatenation allows a cable modem to make a single time-slice request for multiple upstream packets, sending all of the packets in a single large burst on the upstream. Concatenation can send multiple upstream packets as part of one larger MAC data frame, allowing the cable modem to make only one time-slot request for the entire concatenated MAC frame, reducing the delay in transmitting the packets on the upstream channel. This avoids wasting upstream bandwidth when sending a number of very small packets, such as TCP acknowledgement packets.

Dynamic MAC Messages

Dynamic Service MAC messages allow the cable modem to dynamically create service flows on demand. These messages are DOCSIS link layer equivalents of the higher layer messages that create, tear down, and modify a service flow.

The DOCSIS 1.1 dynamic services state machine supports the following messages:

- Dynamic Service Add (DSA)—This message is used to create a new service flow.
- Dynamic Service Change (DSC)—This message is used to change the attributes of an existing service flow.
- Dynamic Service Deletion (DSD)—This message is used to delete an existing service flow.

Note These messages are collectively known as DSX messages.

Enhanced Quality of Service

DOCSIS 1.1 provides enhanced quality of service (QoS) capabilities to give priority for real-time traffic such as voice and video:

- The DOCSIS 1.0 QoS model (a service ID (SID) associated with a QoS profile) has been replaced with a service flow and service class model that allows greater flexibility in assigning QoS parameters to different types of traffic and in responding to changing bandwidth conditions.
- Support for multiple service flows per cable modem allows a single cable modem to support a combination of data, voice, and video traffic.
- Greater granularity in QoS per cable modem in either direction, using unidirectional service flows.
- Upstream service flows can be assigned one of the following QoS scheduling types, depending on the type of traffic and application being used:
  - Best-effort—Data traffic sent on a non-guaranteed best-effort basis. This type of service flow is similar to the method used in DOCSIS 1.0 networks.
  - Real-time polling (rtPS)—Real-time service flows, such as video, that produce unicast, variable size packets at fixed intervals.
  - Non-real-time polling service (nrtPS)—Similar to the rtPS type, in that the cable modem is guaranteed regular opportunities to request data bursts of varying length, except that the CMTS can vary the time between its polling of the cable modem depending on the amount of traffic and congestion on the network.
  - Unsolicited grants (UGS)—Constant bit rate (CBR) or committed information rate (CIR) traffic, such as voice, that is characterized by fixed-size packets at fixed intervals, providing a guaranteed minimum data rate.
  - Unsolicited grants with activity detection (USG-AD)—Combination of UGS and rtPS, to accommodate real-time traffic that might have periods of inactivity (such as voice using silence

suppression). The service flow uses UGS fixed grants while active, but switches to rtPS polling during periods of inactivity to avoid wasting unused bandwidth.

Fragmentation

DOCSIS fragmentation allows the upstream MAC scheduler to slice large data requests to fit into the scheduling gaps between UGS (voice slots). This prevents large data packets from affecting real-time traffic, such as voice and video.

Fragmentation reduces the run-time jitter experienced by the UGS slots when large data grants preempt the UGS slots. Disabling fragmentation increases the run-time jitter, but also reduces the fragmentation reassembly overhead for fragmented MAC frames.

Note DOCSIS fragmentation should not be confused with the fragmentation of IP packets, which is done to fit the packets on network segments with smaller maximum transmission unit (MTU) size. DOCSIS Fragmentation is Layer 2 fragmentation that is primarily concerned with efficiently transmitting lower-priority packets without interfering with high-priority real-time traffic, such as voice calls. IP fragmentation is done at Layer 3 and is primarily intended to accommodate routers that use different maximum packet sizes.

Interoperability

DOCSIS 1.1 cable modems can coexist with DOCSIS 1.0 and 1.0+ cable modems in the same network. The Cisco CMTS provides the levels of service that are appropriate for each cable modem.

Payload Header Suppression

Payload header suppression (PHS) conserves link-layer bandwidth by suppressing repetitive or redundant packet headers on both upstream and downstream service flows. PHS is enabled or disabled per service flow, and each service flow can support a separate set of PHS rules that determine which parts of the header are suppressed. This ensures that PHS is done in the most efficient manner for each service flow and its particular type of application.

Downstream ToS Overwrite

Starting with Cisco IOS Release 12.2(33)SCI1, Downstream ToS Overwrite is supported in DOCSIS 1.1. It can be used in IPv4 and IPv6 environment. You can use CLI command **cable service class** *class-index* **tos-overwrite** *and-mask or-mask* or the cable modem configuration file to configure downstream ToS overwrite. For more information, see Cisco IOS CMTS Cable Command Reference Guide.

Note This feature is supported only by the Cisco uBR10012 router.

DOCSIS 1.1 Quality of Service

The DOCSIS 1.1 QoS framework is based on the following objects:

- Service flow—A unidirectional sequence of packets on the DOCSIS link. Separate service flows are used for upstream and downstream traffic, and define the QoS parameters for that traffic.
- Service class—A collection of settings maintained by the CMTS that provide a specific QoS service tier to a cable modem that has been assigned a service flow associated with that service class.
- Packet classifier—A set of packet header fields used to classify packets onto a service flow to which the classifier belongs. The CMTS uses the packet classifiers to match the packet to the appropriate service flow.
- Payload header suppression (PHS) rule—A set of packet header fields that are suppressed by the sending entity before transmitting on the link, and are restored by the receiving entity after receiving a header-suppressed frame transmission. PHS increases the bandwidth efficiency by removing repeated packet headers before transmission.

See the following sections for more information on these components.

Service Flow

In DOCSIS 1.1, the basic unit of QoS is the service flow, which is a unidirectional sequence of packets transported across the RF interface between the cable modem and CMTS. A service flow defines a set of QoS parameters such as latency, jitter, and throughput assurances, and these parameters can be applied independently to the upstream and downstream traffic flows. This is a major difference from DOCSIS 1.0 networks, where the same QoS parameters were applied to both the downstream and upstream flows.

Note DOCSIS 1.0 networks used service IDs (SIDs) to identify the QoS parameter set for a particular flow. DOCSIS 1.1 networks use the service flow ID (SFID) to identify the service flows that have been assigned to a particular upstream or downstream. DOCSIS 1.1 networks still use the term SID, but it applies exclusively to upstream service flows.

Every cable modem establishes primary service flows for the upstream and downstream directions, with a separate SFID for the upstream and the downstream flows. The primary flows maintain connectivity between the cable modem and CMTS, allowing the CMTS to send MAC management messages at all times to the cable modem.

In addition, a DOCSIS 1.1 cable modem can establish multiple secondary service flows. The secondary service flows either can be permanently created (by configuring them in the DOCSIS configuration file that is downloaded to the cable modem), or the service flows can be created dynamically to meet the needs of the on-demand traffic, such as voice calls. Permanent service flows remain in effect, even if they are not being used, while dynamic service flows are deleted when they are no longer needed.

At any given time, a service flow might be in one of three states (provisioned, admitted, or active). Only active flows are allowed to pass traffic on the DOCSIS network. Every service flow is identified by an SFID, while upstream service flows in the admitted and active state have an extra Layer 2 SID associated with them. The SID is the identifier used by the MAC scheduler when specifying time-slot scheduling for different service flows.

Service Class

Each service flow is associated with a service class, which defines a particular class of service and its QoS characteristics, such as the maximum bandwidth for the service flow and the priority of its traffic. The service class attributes can be inherited from a preconfigured CMTS local service class (class-based flows), or they can be individually specified when a cable modem dynamically requests a service flow and the CMTS creates it.

The DOCSIS 1.1 service class also defines the MAC-layer scheduling type for the service flow. The schedule type defines the type of data burst requests that the cable modem can make, and how often it can make those requests. The following types of schedule types are supported:

- Best-effort (BE)—A cable modem competes with the other cable modems in making bandwidth requests and must wait for the CMTS to grant those requests before transmitting data. This type of service flow is similar to the method used in DOCSIS 1.0 networks.
- Real-time polling service (rtPS)—A cable modem is given a periodic time slot in which it can make bandwidth requests without competing with other cable modems. This allows real-time transmissions with data bursts of varying length.
- Non-real-time polling service (nrtPS)—A cable modem is given regular opportunities to make bandwidth requests for data bursts of varying size. This type of flow is similar to the rtPS type, in that the cable modem is guaranteed regular opportunities to request data bursts of varying length, except that the CMTS can vary the time between its polling of the cable modem, depending on the amount of traffic and congestion on the network.
- Unsolicited grant service (UGS)—A cable modem can transmit fixed data bursts at a guaranteed minimum data rate and with a guaranteed maximum level of jitter. This type of service flow is suitable for traffic that requires a Committed Information Rate (CIR), such as Voice-over-IP (VoIP) calls.
- Unsolicited grant service with activity detection (UGS-AD)—Similar to the UGS type, except that the CMTS monitors the traffic to detect when the cable modem is not using the service flow (such as voice calls when nobody is speaking). When the CMTS detects silence on the service flow, the CMTS temporarily switches the service flow to an rtPS type. When the cable modem begins using the flow again, the CMTS switches the flow back to the UGS type. This allows the CMTS to more efficiently support VoIP calls.

Each service flow is assigned a single service class, but the same service class can be assigned to multiple service flows. Also, a cable modem can be assigned multiple service flows, allowing it to have multiple traffic flows that use different service classes.

Packet Classifiers

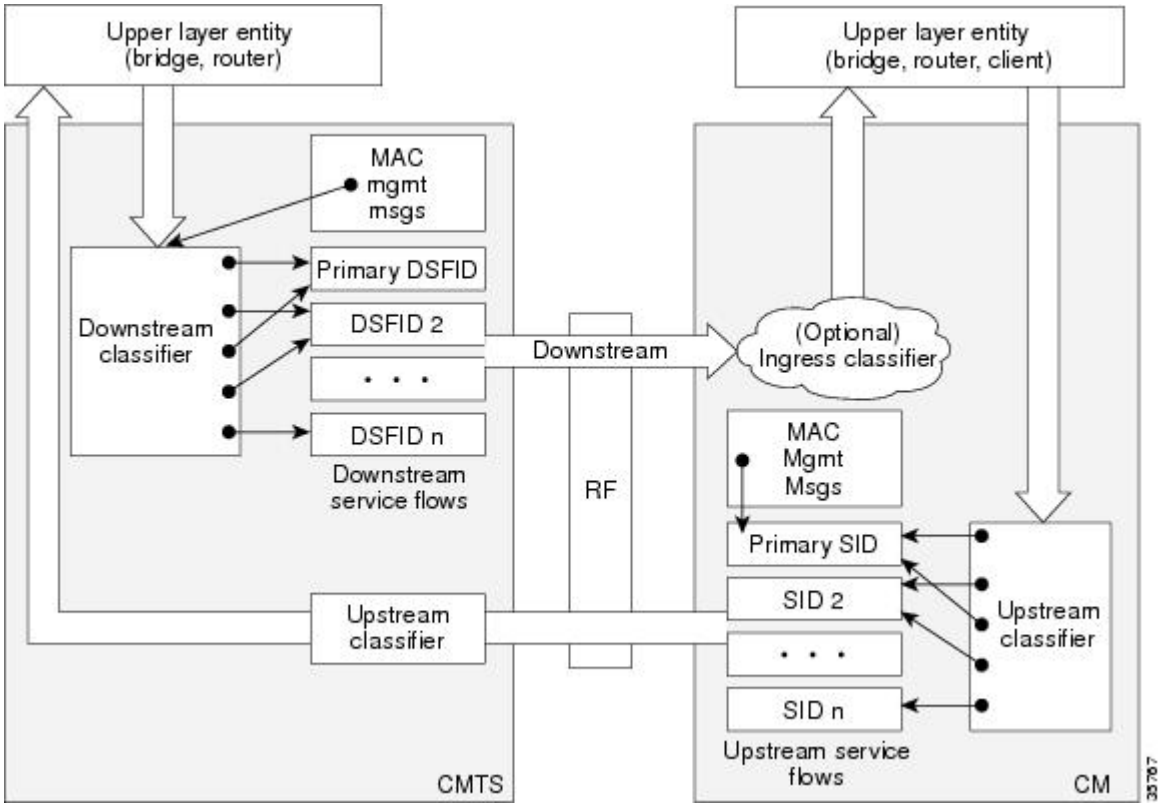
In DOCSIS 1.0 networks, a cable modem used only one set of QoS parameters for all of its traffic, so the CMTS simply had to route packets to and from the appropriate cable modems. In DOCSIS 1.1 networks, however, cable modems can be using multiple service flows, and each service flow can be given a different level of service. To quickly assign upstream and downstream packets to their proper service flows, the CMTS uses the concept of packet classifiers.

Each packet classifier specifies one or more packet header attributes, such as source MAC address, destination IP address, or protocol type. The classifier also specifies the service flow to be used when a packet matches this particular combination of headers. Separate classifiers are used for downstream and upstream service flows.

When the CMTS receives downstream and upstream packets, it compares each packet's headers to the contents of each packet classifier. When the CMTS matches the packet to a classifier, the CMTS then assigns the proper SFID to the packet and transmits the packet to or from the cable modem. This ensures that the packet is assigned its proper service flow, and thus its proper QoS parameters.

Figure below illustrates the mapping of packet classifiers.

Figure 1: Classification Within the MAC Layer



Packet Header Suppression Rules

Because many data and real-time applications may use fixed values in their packet header fields, DOCSIS 1.1 supports PHS to suppress the duplicate portions of the packet headers when a group of packets is transmitted during a session. Each service flow can support a separate set of PHS rules that determine which parts of the header are suppressed.

When PHS is being used, the transmitting CMTS suppresses the specified headers in all the packets for that service flow. The receiving CMTS then restores the missing headers before forwarding the packets on to their ultimate destination.

Proper use of PHS can increase the efficiency of packetized transmissions, especially for real-time data that is encapsulated by other protocols, such as VoIP traffic.

Quality of Service Comparison

This section summarizes the differences in QoS between DOCSIS 1.0, DOCSIS 1.0+, and DOCSIS 1.1 networks.

Note Cisco CMTS routers running Cisco IOS Release 12.1(4)CX or later can transparently interoperate with cable modems running DOCSIS 1.0, DOCSIS 1.0+ extensions, or DOCSIS 1.1. If a cable modem indicates at system initialization that it is DOCSIS 1.1-capable, the Cisco CMTS router uses the DOCSIS 1.1 features. If the cable modem is not DOCSIS 1.1-capable, but does support the DOCSIS 1.0+ QoS extensions (for example, a Cisco uBR924 cable access router running Cisco IOS Release 12.1(1)T or later release), the Cisco CMTS automatically supports the cable modem's requests for dynamic services. Otherwise, the cable modem is treated as a DOCSIS 1.0 device.

DOCSIS 1.0

DOCSIS1.0 uses a static QoS model that is based on a class of service (CoS) that is preprovisioned in the DOCSIS configuration file that is downloaded to the cable modem. The CoS is a bidirectional QoS profile that applies to both the upstream and downstream directions, and that has limited control, such as peak rate limits in either direction, and relative priority on the upstream.

DOCSIS 1.0 defines the concept of a service identifier (SID), which identifies the cable modems that are allowed to transmit on the network. In DOCSIS 1.0 networks, each cable modem is assigned only one SID for both the upstream and downstream directions, creating a one-to-one correspondence between a cable modem and its SID. All traffic originating from, or destined for, a cable modem is mapped to that particular SID.

Typically, a DOCSIS 1.0 cable modem has one CoS and treats all traffic the same, which means that data traffic on a cable modem can interfere with the quality of a voice call in progress. The CMTS, however, has a limited ability to prioritize downstream traffic based on IP precedent type-of-service (ToS) bits.

For example, voice calls using higher IP precedence bits receive a higher queueing priority (but without a guaranteed bandwidth or rate of service). A DOCSIS 1.0 cable modem could increase voice call quality by permanently reserving bandwidth for voice calls, but then that bandwidth would be wasted whenever a voice call is not in progress.

DOCSIS 1.0+

In response to the limitations of DOCSIS 1.0 networks in handling real-time traffic, such as voice calls, Cisco created the DOCSIS 1.0+ extensions to provide the more important QoS enhancements that were expected in DOCSIS 1.1. In particular, the DOCSIS 1.0+ enhancements provide basic Voice-over-IP (VoIP) service over the DOCSIS link.

Cisco's DOCSIS 1.0+ extensions include the following DOCSIS 1.1 features:

- Multiple SIDs per cable modem, creating separate service flows for voice and data traffic. This allows the CMTS and cable modem to give higher priority for voice traffic, preventing the data traffic from affecting the quality of the voice calls.
- Cable modem-initiated dynamic MAC messages—Dynamic Service Addition (DSA) and Dynamic Service Deletion (DSD). These messages allow dynamic SIDs to be created and deleted on demand, so

that the bandwidth required for a voice call can be allocated at the time a call is placed and then freed up for other uses when the call is over.

- Unsolicited grant service (CBR-scheduling) on the upstream—This helps provide a higher-quality channel for upstream VoIP packets from an Integrated Telephony Cable Modem (ITCM) such as the Cisco uBR925 cable access router.
- Ability to provide separate downstream rates for any given cable modem, based on the IP-precedence value in the packet. This helps separate voice signaling and data traffic that goes to the same ITCM to address rate shaping purposes.
- Concatenation allows a cable modem to send several packets in one large burst, instead of having to make a separate grant request for each.

Caution All DOCSIS 1.0 extensions are available only when using a cable modem (such as the Cisco uBR924 cable access router) and CMTS (such as the Cisco uBR7200 series universal broadband router) that supports these extensions. The cable modem activates the use of the extensions by sending a dynamic MAC message. DOCSIS 1.0 cable modems continue to receive DOCSIS 1.0 treatment from the CMTS.

Interoperability with Different Versions of DOCSIS Networks

DOCSIS 1.1 cable modems have additional features and better performance than earlier DOCSIS 1.0 and 1.0+ models, but all three models can coexist in the same network. DOCSIS 1.0 and 1.0+ cable modems will not hamper the performance of a DOCSIS 1.1 CMTS, nor will they interfere with operation of DOCSIS 1.1 features.

Table below shows the interoperability of a DOCSIS 1.1 CMTS with different versions of cable modems.

Table 2: DOCSIS 1.1 Interoperability

For this configuration...	The result is...
DOCSIS 1.1 CMTS with DOCSIS 1.0 cable modems	DOCSIS 1.0 cable modems receive DOCSIS 1.0 features and capabilities. BPI is supported if available and enabled on the CMTS.

For this configuration...	The result is...
DOCSIS 1.1 CMTS with DOCSIS 1.0+ cable modems	DOCSIS 1.0+ cable modems receive basic DOCSIS 1.0 support. BPI is supported if available and enabled on the CMTS. In addition, DOCSIS 1.0+ cable modems also receive the following DOCSIS 1.1 features: • Multiple SIDs per cable modem • Dynamic service MAC messaging initiated by the cable modem • Unsolicited grant service (UGS, CBR-scheduling) on the upstream • Separate downstream rates for any given cable modem, based on the IP-precedence value • Concatenation
DOCSIS 1.1 CMTS with DOCSIS 1.1 cable modems	DOCSIS 1.1 cable modems receive all the DOCSIS 1.1 features listed in this document. BPI+ is supported if available and enabled on the CMTS.

Enhanced Rate Bandwidth Allocation (ERBA) Support for DOCSIS 1.0 Cable Modems

Cisco IOS release 12.3(13a)BC introduces Enhanced Rate Bandwidth Allocation (ERBA) support for DOCSIS 1.0 cable modems on the Cisco uBR7246VXR router. Cisco IOS release 12.3(21)BC extends this support to the Cisco uBR10012 router with Performance Routing Engine 2 modules. To define ERBA on the downstream for DOCSIS 1.0 cable modems, use the cable qos promax-ds-burst command in global configuration mode.

The ERBA feature in Cisco IOS release 12.3(21)BC is characterized by the following enhancements:

- Enables support for the DOCSIS1.1 Downstream Maximum Transmit Burst parameter on the Cisco CMTS by using the **cable ds-max-burst** configuration command. This command is not required on the Cisco uBR7225VXR, Cisco uBR7246VXR and the Cisco uBR7100 Series routers, as this parameter is supported by default.
- Allows DOCSIS1.0 modems to support the DOCSIS1.1 Downstream Maximum Transmit Burst parameter by mapping DOCSIS1.0 modems to overriding DOCSIS 1.1 QoS profile parameters on the Cisco CMTS.

ERBA allows DOCSIS1.0 modems to burst their temporary transmission rate up to the full line rate for short durations of time. This capability provides higher bandwidth for instantaneous bandwidth requests, such as those in Internet downloads, without having to make changes to existing service levels in the QoS Profile.

This feature allows you to set the DOCSIS 1.0 cable modems burst transmissions, with mapping to overriding DOCSIS 1.1 QoS profile parameters on the Cisco CMTS. DOCSIS 1.0 cable modems require DOCSIS 1.0 parameters when registering to a matching QoS profile. This feature enables maximum downstream line rates, and the ERBA setting applies to all cable modems that register to the corresponding QoS profile.

Note QoS definitions must previously exist on the Cisco CMTS headend to support this feature.

ERBA for DOCSIS 1.0 cable modems is supported with these new or enhanced commands or keywords:

- cable qos pro max-ds-burst burst-size
- show cable qos profile n [verbose]

DOCSIS 3.0 Downstream Peak Traffic Rate TLV Support for ERBA

The downstream peak traffic rate TLV (DOCSIS 3.0 TLV 25.27) support for the ERBA feature was introduced in Cisco IOS Release 12.2(33)SCB1 for the Cisco uBR10012 router. This feature support was extended to Cisco uBR7246VXR and Cisco uBR7225VXR routers in Cisco IOS Release 12.2(33)SCD.

The DOCSIS WFQ Scheduler allows each service flow to have one dedicated queue. When ERBA is enabled for the service flow, the peak rate is implemented as the queue shape rate within the scheduler, while the maximum sustained rate is set as the token bucket refill rate. When ERBA is turned off, the burst size and the peak rate value are not used.

The maximum traffic burst parameter is used to control a service flow burst duration, to burst up to the channel line rate or a configured peak rate, when it is within its maximum burst size allowance. On the Cisco uBR10012 Universal Broadband Router, the **cable ds-max-burst** command is used to control this behavior explicitly.

In Cisco IOS Release 12.2(33)SCB1, the *peak-rate* keyword was introduced to specify the peak rate an ERBA-enabled service flow can use. The peak rate value is a global value and is applied to all service flows created after the configuration of the **cable ds-max-burst** command.

If the DOCSIS 3.0 TLV 25.27 is specified for a service flow, the *peak rate* value is set as the TLV value. However, if ERBA is not turned on for a service flow, the *peak rate* value is ignored.

The *peak rate* value can also be configured using the cable service class command, which forms part of the service class template. During modem registration or Dynamic Service Addition (DSA) operation, the service class name TLV 25.4 is sent to create the static or dynamic downstream service flow that matches the service class template. These downstream service flows are created with a specific *peak rate* . If the *peak rate* is not specified, then the value specified by the **cable ds-max-burst** command is used.

If a service flow has both service class and TLV 25.27 defined *peak rate* , then the *peak rate* value specified in the TLV is used.

Some of the DOCSIS 1.x an DOCSIS 2.0 cable modems, which are not fully DOCSIS 1.x or DOCSIS 2.0 compliant, may fail to come online when the downstream peak rate TLV 25.27 is received from the CMTS during registration. To overcome this failure, you can configure the cable service attribute withhold-TLVs command to restrict sending of the peak traffic rate TLVs to DOCSIS1.x and DOCSIS 2.0 cable modems. For more information on how to suppress peak rate TLVs, see Suppressing Upstream and Downstream Peak Rate TLVs for pre DOCSIS 3.0 Cable Modems, on page 23.

Note The ERBA feature is not applicable for high priority service flows and multicast service flows.

Table below summarizes the ERBA support for the Cisco uBR10012 router.

Table 3: Enhanced Rate Bandwidth Allocation Support for the Cisco uBR10012 Router

	Policer Rate	Policer Exceed Action	Policer Token Bucket Size	Queue Shape Rate
Traditional Service Flow	Maximum Sustained Traffic Rate (unused)	Transmit	A value computed internally by CMTS (unused)	Maximum Sustained Traffic Rate
ERBA-Enabled Service Flow	Maximum Sustained Traffic Rate	Drop	Maximum Traffic Burst TLV	Peak Traffic Rate

In Cisco uBR7246VXR and Cisco uBR7225VXR routers, the dual token bucket-based shaper is used to support ERBA on the Cisco uBR-MC88V line card (the ERBA feature is always enabled on the Cisco uBR-MC88V line card). The dual token bucket shaper has two independent token buckets for each service flow. The maximum rate of one bucket is configured to MSR and the maximum tokens are set to maximum traffic burst. The other bucket is configured with the refilling rate of the *peak rate* and the maximum tokens are set to the default level of 4 milliseconds. Packets are shaped if any of the two buckets are exhausted.

Table below summarizes the ERBA dual token bucket configuration for the Cisco uBR7246VXR and Cisco uBR7225VXR routers.

Table 4: ERBA Dual Token Bucket Configuration

	Token Bucket Rate (One)	Token Bucket Size (One)	Token Bucket Rate (Two)	Token Bucket Size (Two)
Traditional Service Flow	Maximum Sustained Traffic Rate	4ms * MSR	N/A	N/A
ERBA-enabled Service Flow	Maximum Sustained Traffic Rate	Maximum Traffic Burst or 4ms * MSR	Peak Rate	4ms * Peak Rate

Note The **cable ds-max-burst** command is not supported on the Cisco uBR7246VXR and Cisco uBR7225VXR routers.

Suppressing Upstream and Downstream Peak Rate TLVs for pre DOCSIS 3.0 Cable Modems

The DOCSIS 3.0 upstream (US) peak rate TLV 24.27 and downstream (DS) peak rate TLV 25.27 are enabled on the Cisco CMTS through the cable service class command or the CM configuration file. The DOCSIS 1.x and DOCSIS 2.0 CMs do not support these TLVs. Ideally, if a DOCSIS 1.x or DOCSIS 2.0 CM receives peak rate TLVs during registration, it should ignore these TLVs and proceed with the registration. However there are a few old non-compliant pre DOCSIS 3.0 CMs, which may fail to come online when peak-rate TLVs are

received in the registration response from the Cisco CMTS. To overcome this, the Cisco CMTS enables suppression of the DOCSIS 3.0 peak rate TLVs for the pre-DOCSIS3.0 CMs.

To suppress the DOCSIS 3.0 US and DS peak rate TLVs, use the **cable service attribute withhold-TLVs command with the peak-rate** keyword in global configuration mode. When configured, this command restricts the Cisco CMTS from sending US and DS peak rate TLVs to the DOCSIS 1.x and DOCSIS 2.0 CMs. The decision to send the TLVs is based on the DOCSIS version of the CM received during registration. If the registration request is from a pre DOCSIS 3.0 CM, the peak rate TLVs are not sent in the registration response. However this command does not restrict sending of DOCSIS 3.0 peak-rate TLVs to DOCSIS 3.0 CMs.

For more information on the **cable service attribute withhold-TLVs** command, see Cisco IOS CMTS Cable Command Reference Guide .

Downstream Classification Enhancement with MAC Addresses

Downstream classifiers, specified in the cable modem configuration file, are used to map packets to service flows based on DOCSIS specifications. New combinations of downstream classifiers with a destination MAC address are supported in Cisco IOS Release 12.2(33)SCH and later. This enhancement enables service providers to better manage high priority service flows associated with a downstream classifier. For example, a single User Datagram Protocol (UDP) port can be shared by high priority and low priority traffic.

Downstream classification is automatically enabled on the Cisco CMTS router. Table below lists the downstream classifier combinations that are supported on the router.

Table 5: Downstream Classifier Combinations

Cisco IOS Release 12.2(33)SCG and Earlier	Cisco IOS Release 12.2(33)SCH and Later
Without Combination • IPv4 • IPv6 • TCP/UDP • Destination MAC With Combination • IPv4 + TCP/UDP • IPv6 + TCP/UDP	Without Combination • IP (IPv4) • IPv6 • TCP/UDP • Destination MAC With Combination • IPv4 + TCP/UDP • IPv6 + TCP/UDP • Destination MAC + IPv4 (with the exception of a destination IP address) • Destination MAC + IPv6 (with the exception of a destination IPv6 address) • Destination MAC + TCP/UDP • Destination MAC + IPv4 + TCP/UDP (with the exception of a destination IP address) • Destination MAC + IPv6 + TCP/UDP (with the exception of a destination IPv6 address)

Benefits

DOCSIS 1.1 includes a rich set of features that provide advanced and flexible QoS capabilities for various types of traffic (voice, data, and video) over the cable network. It also provides enhanced security and authentication features.

Baseline Privacy Interface Plus Enhancement

The Plus (+) version of the Baseline Privacy Interface (BPI+) in DOCSIS 1.1 provides a set of extended services within the MAC sublayer that increase performance and system security. Digital certificates provide secure authentication for each cable modem, to prevent identity theft on the basis of MAC and IP addresses. Advanced encryption provides a secure channel between the cable modem and CMTS, and secure software download allows a service provider to upgrade the software on cable modems, without the threat of interception, interference, or alteration of the software code.

Dynamic Service Flows

The dynamic creation, modification, and deletion of service flows allows for on-demand reservation on Layer 2 bandwidth resources. The CMTS can now provide special QoS to the cable modem dynamically for the duration of a voice call or video session, as opposed to the static provisioning and reservation of resources at the time of cable modem registration. This provides a more efficient use of the available bandwidth.

Concatenation

The cable modem concatenates multiple upstream packets into one larger MAC data frame, allowing the cable modem to make only one time-slot request for the entire concatenated MAC frame, as opposed to requesting a time slot for each packet. This reduces the delay in transferring the packet burst upstream.

Enhanced QoS

Extensive scheduling parameters allow the CMTS and the cable modem to communicate QoS requirements and achieve more sophisticated QoS on a per service-flow level.

Different new time-slot scheduling disciplines help in providing guaranteed delay and jitter bound on shared upstream. Activity detection helps to conserve link bandwidth by not issuing time slots for an inactive service flow. The conserved bandwidth can then be reused for other best-effort data slots.

Packet classification helps the CMTS and cable modem to isolate different types of traffic into different DOCSIS service flows. Each flow could be receiving a different QoS service from CMTS.

Fragmentation

Fragmentation splits large data packets so that they fit into the smaller time slots inbetween UGS slots. This reduces the jitter experienced by voice packets when large data packets are transmitted on the shared upstream channel and preempt the UGS slots used for voice.

Multiple Subflows per SID

This feature allows the cable modem to have multiple calls on a single hardware queue. This approach scales much better than requiring a separate SID hardware queue on the cable modem for each voice call.

Payload Header Suppression

Payload Header Suppression (PHS) allows the CMTS and cable modem to suppress repetitive or redundant portions in packet headers before transmitting on the DOCSIS link. This conserves link bandwidth, especially with types of traffic such as voice, where the header size tends to be as large as the size of the actual packet.

Service Classes

The use of the service class provides the following benefits for a DOCSIS 1.1 network:

- It allows operators to move the burden of configuring service flows from the provisioning server to the CMTS. Operators provision the modems with the service class name; the implementation of the name is configured at the CMTS. This allows operators to modify the implementation of a given service to local circumstances without changing modem provisioning. For example, some scheduling parameters might need to be set differently for two different CMTSs to provide the same service. As another example, service profiles could be changed by time of day.
- It allows CMTS vendors to provide class-based-queuing if they choose, where service flows compete within their class and classes compete with each other for bandwidth.
- It allows higher-layer protocols to create a service flow by its service class name. For example, telephony signaling might direct the cable modem to instantiate any available provisioned service flow of class G.711.

Note The service class is optional. The flow scheduling specification may always be provided in full; a service flow may belong to no service class whatsoever. CMTS implementations *may* treat such unclassed flows differently from classed flows with equivalent parameters.

How to Configure the Cisco CMTS for DOCSIS 1.1 Operations

See the following sections for the configuration tasks for DOCSIS 1.1 operations. Each task in the list is identified as either required or optional.

Note This section describes only the configuration tasks that are specific for DOCSIS 1.1 operations. For complete configuration information, see the software configuration documents listed in the Additional References, on page 64.

Configuring Baseline Privacy Interface

BPI+ encryption is by default enabled for 56-bit DES encryption on all cable interfaces. If BPI+ encryption has been previously disabled, or if you want to reconfigure BPI+ encryption on a cable interface on the CMTS, use the following procedure.

Note If you have disabled BPI+ encryption on a cable interface, and a cable modem attempts to register on that interface using BPI+ encryption, the CMTS will reject its registration request, displaying a %UBR7200-4-SERVICE_PERMANENTLY_UNAVAILABLE error message. The **show cable modem** command will also show that this cable modem has been rejected with a MAC status of reject(c).

Before You Begin

BPI+ encryption is supported on all Cisco CMTS images that include "k1", "k8", or "k9" in its file name or BPI in the feature set description. All BPI images support 40-bit and 56-bit DES encryption.

By default, BPI+ encryption is enabled for 56-bit DES encryption. Also, when a cable modem is running DOCSIS 1.1 software, BPI+ encryption is enabled by default, unless the service provider has disabled it by setting the Privacy Enable field (TLV 29) in the DOCSIS configuration file to 0. Therefore, both the CMTS and cable modem are set to use BPI+ encryption when using the default configurations.

DETAILED STEPS

	Command or Action	Purpose

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

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

Step 3	**interface cable***slot /port*
	
	Example:
	
	`Router(config)# interface cable 6/0`
	`Router(config-if)#`
		Enters interface configuration mode for the cable interface line card at this particular slot.

Step 4	**cable privacy**
	
	Example:
	
	`Router(config-if)# cable privacy`
	`Router(config-if)#`
		(Optional) Enables BPI+ 56-bit DES encryption on the cable interface (default).

Step 5	**cable privacy 40-bit-des** **Example:** `Router(config-if)# cable privacy 48-bit-des`	(Optional) Enables BPI+ 40-bit DES encryption on the cable interface. Cisco does not recommend this option for production systems because 40-bit encryption is not as secure as the 56-bit DES or 168-bit 3DES encryption algorithms.

	Command or Action	Purpose
	`Router(config-if)#`	

Step 6	**cable privacyaccept-self-signed-certificate**
	
	Example:
	
	`Router(config-if)# cable privacy accept-self-signed-certificate`
	`Router(config-if)#`
		(Optional) Allows cable modems to register using self-signed manufacturer certificates, as opposed to the default of allowing only manufacturer's certificates that are chained to the DOCSIS root certificate.
		
		Caution Use the above command sparingly, as it bypasses DOCSIS BPI+ certificates. Otherwise, self-signed certificates provide workaround registration for cable modems that are not compliant with DOCSIS BPI+ certificates. This functionality is strictly intended for troubleshooting of a short duration or in the context of additional security measures.
		
		Note By default, the CMTS does not accept self-signed certificates. In the default configuration, if a cable modem attempts to register with self-signed certificates, the CMTS will refuse to allow the cable modem to register.

Step 7	**cable privacy authenticate-modem**
	
	Example:
	
	`Router(config-if)# cable privacy authenticate-modem`
	`Router(config-if)#`
		(Optional) Enables BPI+ encryption on the cable interface and uses the Cisco IOS Authentication, Authorization and Accounting (AAA) service together with BPI to authenticate the CMs.

Step 8	**cable privacy authorize-multicast**
	
	Example:
	
	`Router(config-if)# cable privacy authorize-multicast`
	`Router(config-if)#`
		(Optional) Enables BPI+ encryption on the cable interface and uses AAA protocols to authorize all multicast stream (IGMP) join requests.
		
		Note If you use this command to authorize multicast streams, you must also use the **cable privacy authenticate-modem** command to enable AAA services on the cable interface.

Step 9	**cable privacy mandatory**
	
	Example:
	
	`Router(config-if)# cable privacy mandatory`
	`Router(config-if)#`
		(Optional) Requires baseline privacy be active for all CMs with BPI/BPI+ enabled in the DOCSIS configuration files, else the CMs are forced to go offline.
		
		If a CM does not have BPI enabled in its DOCSIS configuration file, it will be allowed to come online without BPI.

Step 10	**cable privacy oaep-support**
	
	Example:
	
	`Router(config-if)# cable privacy oaep-support`
	`Router(config-if)#`
		(Optional) Enables BPI+ encryption on the cable interface and enables Optimal Asymmetric Encryption Padding (OAEP). This option is enabled by default. Disabling this option could have a performance impact.

	Command or Action	Purpose

Step 11	**cable privacy kek** {**life-time** *seconds* }
	
	Example:
	
	`Router(config-if)# cable privacy kek life-time 302400`
	`Router(config-if)#`
		(Optional) Configures the life-time values for the key encryption keys (KEKs) for BPI+ operations on all cable interfaces.

Step 12	**cable privacy tek** {**life-time** *seconds*}
	
	Example:
	
	`Router(config-if)# cable privacy tek life-time 86400`
	`Router(config-if)#`
		(Optional) Configures the life-time values for the traffic encryption keys (TEKs) for BPI+ operations on all cable interfaces.

Step 13	**exit**
	
	Example:
	
	`Router(config-if)# exit`
	`Router(config)#`
		Exits interface configuration mode.
		
		Note Repeat steps Step 3, on page 27 through Step 13, on page 29 for each cable interface.

Step 14	**exit**
	
	Example:
	
	`Router(config)# exit`
	`Router#`
		Exits global configuration mode.

What to Do Next

You can also configure the following additional timers for BPI+ operations in the DOCSIS configuration file for each cable modem. As a general rule, you do not need to specify these timers in the DOCSIS configuration file unless you have a specific reason for changing them from their default values.

Table 6: Individual Cable Modem BPI+ Timer Values

Timer	Description
Authorize Wait Timeout	The amount of time a cable modem will wait for a response from a CMTS when negotiating a KEK for the first time.
Reauthorize Wait Timeout	The amount of time a cable modem will wait for a response from a CMTS when negotiating a new KEK because the Authorization Key (KEK) lifetime is about to expire.

Timer	Description
Authorize Reject Wait Timeout	The amount of time a cable modem must wait before attempting to negotiate a new KEK if the CMTS rejects its first attempt to negotiate a KEK.
Operational Wait Timeout	The amount of time a cable modem will wait for a response from a CMTS when negotiating a TEK for the first time.
Rekey Wait Timeout	The amount of time a cable modem will wait for a response from a CMTS when negotiating a new TEK because the TEK lifetime is about to expire.

Downloading the DOCSIS Root Certificate to the CMTS

DOCSIS 1.1 allows cable modems to identify themselves using a manufacturer's chained X.509 digital certificate that is chained to the DOCSIS root certificate. The DOCSIS root certificate is already installed on the bootflash of the CMTS router. However, if you want to install another root certificate, for example, the Euro-DOCSIS certificate, download the certificate and save it on the bootflash as "euro-root-cert".

Tip For more information about the DOCSIS root certificate provided by Verisign, see the information at the following URL: http://www.verisign.com/products-services/index.html

Note This document previously claimed that the Cisco CMTS supports only one root certificate. This information has changed effective with Cisco IOS Release 12.3(9a)BC. In this IOS release and later releases in the 12.3 BC train, you may load the DOCSIS root certificate and a EuroDOCSIS or PacketCable root certificate. Cisco recommends that the EuroDOCSIS PacketCable root certificates be copied into bootflash. In prior Cisco IOS Releases, with the prior limitation, EuroDOCSIS or PacketCable devices could still come online, however, if they used self-signed manufacturer's digital certificates.

To download the DOCSIS root certificate to the Cisco CMTS, which is required if any cable modems on the network are using chained certificates, use the following procedure:

Step 1 Download the DOCSIS root certificate from the DOCSIS certificate signer, Verisign. At the time of this document's printing, the DOCSIS root certificate is available for download at the following URL: http://www.verisign.com/products-services/index.html

Step 2 Verisign distributes the DOCSIS root certificate in a compressed ZIP archive file. Extract the DOCSIS root certificate from the archive and copy the certificate to a TFTP server that the CMTS can access.

Tip To avoid possible confusion with other certificates, keep the file's original filename of "CableLabs_DOCSIS.509" when saving it to the TFTP server.

Step 3 Log in to the Cisco CMTS using either a serial port connection or a Telnet connection. Enter the **enable** command and password to enter Privileged EXEC mode:

Example:

```
Router> enable

Password: <password>
Router#
```

Step 4 Use the **dir bootflash** command to verify that the bootflash has sufficient space for the DOCSIS root certificate (approximately 1,000 bytes of disk space):

Example:

```
Router# dir bootflash:

Directory of bootflash:/
    1  -rw-     3229188   Dec 30 2002 15:53:23  ubr7200-boot-mz.122-11.BC2.bin
3407872 bytes total (250824 bytes free)
Router#
```

Tip If you delete files from the bootflash to make room for the DOCSIS root certificate, remember to use the **squeeze** command to reclaim the free space from the deleted files.

Step 5 Use the **copy tftp bootflash** command to copy the DOCSIS root certificate to the router's bootflash memory. (The file must be named "root-cert" on the bootflash for the CMTS to recognize it as the root certificate.)

Example:

```
Router# copy tftp bootflash:

Address or name of remote host []? tftp-server-ip-address

Source filename []? CableLabs_DOCSIS.509

Destination filename [CableLabs_DOCSIS.509]? root-cert

Loading CableLabs_DOCSIS.509 from tftp-server-ip-address (via FastEthernet0/0): !
[OK - 996/1024 bytes]
996 bytes copied in 4.104 secs (249 bytes/sec)
Router#
```

Tip If you are using Cisco IOS Release 12.2(4)BC1 or later software release, you can also copy the root certificate to a PCMCIA Flash Disk (disk0 or disk1). However, because Flash Disks are not secure and easily removed from the router, we recommend that you keep the root certificate in the bootflash for both operational and security reasons.

Step 6 Verify that the DOCSIS root certificate has been successfully copied to the bootflash memory:

Example:

```
Router# dir bootflash:

Directory of bootflash:/
    1  -rw-     3229188   Dec 30 2002 15:53:23  ubr7200-boot-mz.122-11.BC2.bin
    2  -rw-         996   Mar 06 2002 16:03:46  root-cert
3408876 bytes total (248696 zxbytes free)
Router#
```

Step 7 (Optional) After the first cable modem has registered using BPI+, you can use the **show crypto ca trustpoints** command to display the Root certificate that the CMTS has learned:

Note The **show crypto ca trustpoints** command does not display the root certificate until after at least one cable modem has registered with the CMTS using BPI+ encryption. Alternatively, you can use the unsupported command **test cable generate** in privileged EXEC mode to force the CMTS to register the root certificate.

Example:

```
Router# show crypto ca trustpoints
Root certificate
  Status: Available
  Certificate Serial Number: D54BB68FE934324F6B8FD0E41A65D867
  Key Usage: General Purpose
  Issuer:
    CN = DOCSIS Cable Modem Root Certificate Authority
     OU = Cable Modems
     O = Data Over Cable Service Interface Specifications
     C = US
  Subject Name:
    CN = "BPI Cable Modem Root Certificate Authority "
     OU = DOCSIS
     O = BPI
     C = US
  Validity Date:
    start date: 07:00:00 UTC Mar 27 2001
    end   date: 06:59:59 UTC Jan 1 2007
```

What to Do Next

Tip To display all certificates (Root, Manufacturers, CM) that the CMTS has learned, use the **show crypto ca certificates** command.

Adding a Manufacturer's Certificate as a Trusted Certificate

To DOCSIS specifications allow operators to control which manufacturer's and CM certificates are allowed on each CMTS by marking them as either trusted or untrusted. You can add a certificate to the list of trusted certificates on the Cisco CMTS using either CLI commands or SNMP commands, as described in the following sections:

Note Unless you cannot use SNMP to configure the cable modem, or have a particular application that requires the use of CLI commands to add certificates, you should also use the SNMP method to add certificates to a cable modem.

Adding a Certificate as a Trusted Certificate Using the Command Line Interface

To add a manufacturer's certificate to the list of trusted certificates on the CMTS, use the following procedure:

DETAILED STEPS

	Command or Action	Purpose

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

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

Step 3	**cable privacy add-certificate manufacturer** *serial-number*
	
	Example:
	
	`Router(config)# cable privacy add-certificate manufacturer 000102`
	`Router(config)#`
		(Optional) Specifies the serial number of the manufacturer CA certificate to be added as a trusted certificate.

Step 4	**exit**
	
	Example:
	
	`Router(config)# exit`
	`Router#`
		Exits global configuration mode.

Adding a Certificate as a Trusted Certificate Using SNMP Commands

You can also use an SNMP manager to create and add certificates to the CMTS list of trusted certificates by manipulating the tables and attributes in the DOCS-BPI-PLUS-MIB . To add a manufacturer's certificate, add an entry to the docsBpi2CmtsCACertTable table. Specify the following attributes for each entry:

- docsBpi2CmtsCACertStatus—Set to 4 to create the row entry.
- docsBpi2CmtsCACert—The hexadecimal data, as an X509Certificate value, for the actual X.509 certificate.
- docsBpi2CmtsCACertTrust—An Integer value from 1 to 4 specifying the certificate's trust status: 1=trusted, 2=untrusted, 3= chained, 4=root. Specify 1 for certificates that should be trusted and 3 for chained certificates that should be verified with the root certificate.

Similarly, to add a CM certificate to the list of trusted certificates, add an entry to the docsBpi2CmtsProvisionedCmCertTable table. Specify the following attributes for each entry:

- docsBpi2CmtsProvisionedCmCertStatus—Set to 4 to create the row entry.

- docsBpi2CmtsProvisionedCmCert—The hexadecimal data, as an X509Certificate value, for the actual X.509 certificate.
- docsBpi2CmtsProvisionedCmCertTrust—An Integer value from 1 to 2 specifying the certificate's trust status: 1=trusted, 2=untrusted. Specify 1 for CM certificates that should be trusted.

Tip Always set the CertStatus attributes before loading the actual certificate data, because otherwise the CMTS will assume the certificate is chained and will immediately attempt to verify it with the manufacturers and root certificates.

For example, to use the Unix command-line SNMP utility to add a manufacturer's certificate to the list of trusted certificates on the CMTS at IP address 192.168.100.134, enter the following command (be sure to substitute a valid index pointer for the table entry for the <*index*> value).

```
% setany -v2c 192.168.100.134 private docsBpi2CmtsCACertStatus.
<index>
 -i 4
 docsBpi2CmtsCACert.
<index>
 -o
 '<hex_data>' docsBpi2CmtsCACertTrust.
<index>
 -i 1
```

To do the same thing for a CM certificate, use the following command:

```
% setany -v2c 192.168.100.134 private docsBpi2CmtsProvisionedCmCertStatus.
<index>
 -i 4 docsBpi2CmtsProvisionedCmCert.
<index>
 -o
 '<hex_data>' docsBpi2CmtsProvisionedCmCertTrust.
<index>
 -i 1
```

Tip Most operating systems cannot accept input lines that are as long as needed to input the hexadecimal decimal string that specifies a certificate. For this reason, you should use a graphical SNMP manager to set these attributes. For a number of certificates, you can also use a script file, if more convenient.

Note If you are adding self-signed certificates, you must also use the **cable privacy accept-self-signed-certificate** command before the CMTS will accept the certificates.

Adding a Manufacturer's or CM Certificate to the Hotlist

The DOCSIS specifications allow operators to add a digital manufacturer's or CM certificate to a hotlist (also known as the certificate revocation list, or CRL) on the CMTS, to indicate that this particular certificate should no longer be accepted. This might be done when a user reports that their cable modem has been stolen, or when the service provider decides not to support a particular manufacturer's brand of cable modems.

You can add a certificate to the hotlist on the Cisco CMTS using either CLI commands or SNMP commands, as described in the following sections:

Note Unless you cannot use SNMP to configure the cable modem, or have a particular application that requires the use of CLI commands to add certificates, you should also use the SNMP method to add certificates to a cable modem.

Adding a Certificate to the Hotlist Using the Command Line Interface

To add a manufacturer's or CM certificate to the certificate hotlist on a Cisco uBR7100 series or Cisco uBR7200 series router, use the following procedure.

This procedure is not supported on the Cisco uBR10012 router running Cisco IOS releases prior to Cisco IOS release 12.3(23)BC9, Cisco IOS release 12.2(33)SCB5, and Cisco IOS Release12.2(33)SCC and later releases.

Use the following section, Adding a Certificate to the Hotlist Using SNMP Commands, on page 36, to add certificates to the hotlist on the Cisco uBR10012 router.

DETAILED STEPS

	Command or Action	Purpose

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

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

Step 3	**cable privacy hotlist manufacturer***certificate-serial-number*
	
	Example:
	
	`Router(config)# cable privacy hotlist manufacturer 010A0BC304DFEE1CA98371`
	`Router(config)#`
		Sets the trust state of the specified CA certificate to "Untrusted." Ensure that this certificate exists on the CMTS.
		
		The *certificate-serial-number* is the serial number of the CA certificate.
		
		This is not a persistent command.

Step 4	**exit**
	
	Example:
	
	`Router(config)# exit`
	`Router#`
		Exits global configuration mode.

What to Do Next

Cable modems that use a MAC address or a certificate of the manufacturer that matches the one in the hotlist will not be allowed to register. For example, the following command will put the certificate of the manufacturer with the indicated serial number in the hotlist, preventing any cable modem that uses that certificate from registering:

```
Router# config terminal

Router(config)# cable privacy hotlist cm 00 00 0C 0a 0b 0c

Oct 31 13:06:29.112:  Successfully added CM hotlist 0000.0C0A.0B0C
Router#
```

The following command will put the manufacturer's certificate with the indicated serial number in the hotlist, preventing any cable modem that uses that manufacturer's certificate from registering:

```
Router(config)# cable privacy hotlist manufacturer 00 90 83 00 00 00 00 01

Oct 31 13:06:34.478:  Successfully added MFG hotlist 00 90 83 00 00 00 00 01
Router(config)# exit

Router#
```

To remove a cable modem or certificate from the hotlist, add the **no** prefix to the command. For example:

```
Router# config terminal

Router(config)# no cable privacy hotlist cm 00 00 0C 0a 0b 0c

Router(config)# no cable privacy hotlist manufacturer 00 90 83 00 00 00 00 01

Router(config)# exit

Router#
```

Adding a Certificate to the Hotlist Using SNMP Commands

You can also use an SNMP manager to create and add certificates to the hotlist by manipulating the tables and attributes in the DOCS-BPI-PLUS-MIB . To add a manufacturer's certificate, add an entry to the docsBpi2CmtsCACertTable table. Specify the following attributes for each entry:

- docsBpi2CmtsCACertStatus—Set to 4 to create the row entry.
- docsBpi2CmtsCACert—The hexadecimal data, as an X509Certificate value, for the actual X.509 certificate.
- docsBpi2CmtsCACertTrust—An Integer value from 1 to 4 specifying the certificate's trust status: 1=trusted, 2=untrusted, 3= chained, 4=root. When adding a certificate to the hotlist, set this attribute to 2 for untrusted.

Similarly, to add a CM certificate to the hotlist, add an entry to the docsBpi2CmtsProvisionedCmCertTable table. Specify the following attributes for each entry:

- docsBpi2CmtsProvisionedCmCertStatus—Set to 4 to create the row entry.
- docsBpi2CmtsProvisionedCmCert—The hexadecimal data, as an X509Certificate value, for the actual X.509 certificate.
- docsBpi2CmtsProvisionedCmCertTrust—An Integer value from 1 to 2 specifying the certificate's trust status: 1=trusted, 2=untrusted. When adding a certificate to the hotlist, set this attribute to 2 for untrusted.

Tip Always set the CertStatus attributes before loading the actual certificate data, because otherwise the CMTS will assume the certificate is chained and will immediately attempt to verify it with the manufacturers and root certificates.

Note This procedure is identical to the one given for adding a certificate as a trusted certificate in the Adding a Certificate as a Trusted Certificate Using SNMP Commands, on page 33, except that the docsBpi2CmtsProvisionedCmCertTrust attribute is set to 2 instead of 1.

For example, to use the Unix command-line SNMP utility to add a manufacturer's certificate to the hotlist on the CMTS at IP address 192.168.100.113, enter the following command (be sure to substitute a valid index pointer for the table entry for the <*index*> value).

```
% setany -v2c 192.168.100.113 private docsBpi2CmtsCACertStatus.
<index>
 -i 4
 docsBpi2CmtsCACert.
<index>
 -o
 '<hex_data>' docsBpi2CmtsCACertTrust.
<index>
 -i 2
```

To do the same thing for a CM certificate, use the following command:

```
% setany -v2c 192.168.100.113 private docsBpi2CmtsProvisionedCmCertStatus.
<index>
 -i 4
 docsBpi2CmtsProvisionedCmCert.
<index>
 -o
 '<hex_data>' docsBpi2CmtsProvisionedCmCertTrust.
<index>
 -i 2
```

Tip Most operating systems cannot accept input lines that are as long as needed to input the hexadecimal decimal string that specifies a certificate. For this reason, you should use a graphical SNMP manager to set these attributes. For a number of certificates, you can also use a script file, if more convenient.

Enabling Concatenation

To enable concatenation for one or more upstreams on a cable interface (which is the default configuration), use the following procedure:

DETAILED STEPS

	Command or Action	Purpose

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

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

Step 3	**interface cable***slot* / *port*
	
	Example:
	
	`Router(config)# interface cable 6/0`
	`Router(config-if)#`
		Enters interface configuration mode for the cable interface line card at this particular slot.

Step 4	**cable upstream** *n* **concatenation**
	
	Example:
	
	`Router(config-if)# cable upstream 0 concatenation`
	`Router(config-if)# cable upstream 1 concatenation`
	
	`Router(config-if)#`
		Enables concatenation for the specified upstream on the cable interface.
		
		Note Repeat this command for each upstream on the interface.

Step 5	**exit**
	
	Example:
	
	`Router(config-if)# exit`
	`Router(config)#`
		Exits interface configuration mode.

Step 6	**exit**
	
	Example:
	
	`Router(config)# exit`
	`Router#`
		Exits global configuration mode.

Enabling DOCSIS Fragmentation

To enable DOCSIS fragmentation for one or more upstreams on a cable interface (which is the default configuration), use the following procedure:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface cable***slot* /*port*
4. **cable upstream***n* **fragmentation**
5. **cable upstream** *n* **unfrag-slot-jitter** [**limit***jitter* | **cac-enforce**]
6. **exit**
7. **exit**

DETAILED STEPS

	Command or Action	Purpose

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

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

Step 3	**interface cable***slot* /*port*
	
	Example:
	`Router(config)# interface cable 6/0`
	`Router(config-if)#`
		Enters interface configuration mode for the cable interface line card at this particular slot.

Step 4	**cable upstream***n* **fragmentation**
	
	Example:
	`Router(config-if)# cable upstream 2 fragmentation`
	`Router(config-if)# cable upstream 3 fragmentation`
	`Router(config-if)#`
		Enables fragmentation for the specified upstream on the cable interface.
		Note Repeat this command for each upstream on the interface.

Step 5	**cable upstream** *n* **unfrag-slot-jitter** [**limit***jitter*	**cac-enforce**] **Example:** `Router(config-if)# cable upstream 0`	(Optional) Specifies the amount of jitter that can be tolerated on the upstream due to unfragmentable slots. The **limit** option specifies the allowable *jitter* limit in microseconds (0 to 4,294,967,295. The **cac-enforce** option configures the upstream so that it rejects service flows requesting jitter less than the fragmentable slot jitter.

	Command or Action	Purpose
	unfrag-slot-jitter limit 2000 cac-enforce Router(config-if)#	**Note** By default, *jitter* is set to a limit of 0 microseconds, and the **cac-enforce** option is enabled.
Step 6	**exit** **Example:** Router(config-if)# **exit** Router(config)#	Exits interface configuration mode.
Step 7	**exit** **Example:** Router(config)# **exit** Router#	Exits global configuration mode.

The following example of the **show cable qos profile** command illustrates that the maximum downstream burst has been defined, and is a management-created QoS profile:

```
Router# show cable qos profile
ID  Prio Max       Guarantee Max        Max   TOS  TOS   Create  B     IP prec.
         upstream  upstream  downstream tx    mask value by      priv  rate
         bandwidth bandwidth bandwidth  burst                     enab  enab
1   0    0         0         0          0     0xFF 0x0   cmts(r) no    no
2   0    64000     0         1000000    0     0xFF 0x0   cmts(r) no    no
3   7    31200     31200     0          0     0xFF 0x0   cmts    yes   no
4   7    87200     87200     0          0     0xFF 0x0   cmts    yes   no
6   1    90000     0         90000      1522  0xFF 0x0   mgmt    yes   no
10  1    90000     0         90000      1522  0x1  0xA0  mgmt    no    no
50  0    0         0         96000      0     0xFF 0x0   mgmt    no    no
51  0    0         0         97000      0     0xFF 0x0   mgmt    no    no
```

The following example illustrates the maximum downstream burst size in sample QoS profile 10 with the **show cable qos profileverbose** command in privileged EXEC mode:

```
Router# show cable qos profile 10 verbose
Profile Index                          10
Name
Upstream Traffic Priority              1
Upstream Maximum Rate (bps)            90000
Upstream Guaranteed Rate (bps)         0
Unsolicited Grant Size (bytes)         0
Unsolicited Grant Interval (usecs)     0
Upstream Maximum Transmit Burst (bytes) 1522
Downstreamam Maximum Transmit Burst (bytes) 100000
IP Type of Service Overwrite Mask      0x1
IP Type of Service Overwrite Value     0xA0
Downstream Maximum Rate (bps)          90000
Created By                             mgmt
Baseline Privacy Enabled               no
```

Enabling DOCSIS 1.1 Downstream Maximum Transmit Burst on the Cisco uBR10012 Router

Perform the following steps to configure ERBA on the Cisco uBR10012 router with PRE2 or PRE4 modules and Cisco IOS Release 12.3(21)BC or Cisco IOS Release 12.2(33)SCB or later releases. This procedure and the associated commands are subject to the guidelines and restrictions cited in this document.

Restriction The **cable ds-max-burst** and related commands are supported strictly on the Cisco uBR10012 router with PRE2 or PRE4 modules and Cisco IOS Release 12.3(21)BC or Cisco IOS Release 12.2(33)SCB or later releases.

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`
	`Router(config)#`
		Enters global configuration mode.

Step 3	**no**] **cable ds-max-burst** [**burst-threshold** *threshold*] [**peak-rate** *peak-rate* **Example:** `Router(config)# no cable ds-max-burst burst-threshold 2048 peak-rate 1000`	Enables the support for DOCSIS 1.1 downstream max burst. To remove this configuration, use the **no** form of this command. • **burst-threshold***threshold* —Optional keyword and value defines the burst threshold in Kbytes, with a valid range from 64 Kbyte to 2 GB. By default, this setting is 1MB. This value is used to compare with the per-service flow maximum traffic burst value as defined in DOCSIS 2.0. • **peak-rate***peak-rate* —Peak rate in kbps. The default value of peak-rate is zero, which represents the line rate. The peak-rate value is a global value and is applied to all the service flows created after the configuration of cable ds-max-burst command.

Step 4	**Ctrl^Z**
	
	Example:
	
	`Router(config)# Ctrl^Z`
	`Router#`
		Returns to privileged EXEC mode.

Step 5	**show cr10k-rp cable** *slot* / *subslot* /*port* **sid service-flow ds**	Displays service flows on the Cisco uBR10012 router with PRE2 or PRE4, and identifies which service flows have maximum burst enabled.

	Command or Action	Purpose
	Example: `Router(config)# show cr10k-rp cable 6/1/0 sid service-flow ds`	• *slot* —5 to 8 • *subslot* —0 or 1 • *port* —0 to 4 (depending on the cable interface)

When this feature is enabled, new service flows with burst size larger than the burst threshold are supported. However, the existing service flows are not affected.

When this feature is disabled, no new service flows are configured with the *Downstream Maximum Transmit Burst* parameter—the **cable ds-max-burst** command settings. However, the existing service flows are not affected.

The following example illustrates the **cable ds max-burst** command on the Cisco uBR10012 router in Cisco IOS Release 12.3(21)BC:

```
Router(config)# cable ds-max-burst burst-threshold 2048
```

The following example illustrates configuration of the ERBA maximum burst for the specified service flow:

```
Router# sh cr10k-rp c7/0/0 1 service-flow ds
RP SFID  LC SFID   Conform   Conform    Exceed    Exceed    Total   Total   QID
Bytes    Pkts      Bytes     Pkts       Bytes     Pkts

32781    4         538       1        0           0          538    1       279    #
32782    4         0         0        0           0          0      0       0
#: DS max burst enabled
```

The following example illustrates the **cable ds max-burst** command on the Cisco uBR10012 router in Cisco IOS Release 12.2(33)SCB:

```
Router(config)# cable ds-max-burst burst-threshold 2048 peak-rate 1000
```

The following example illustrates configuration of the ERBA maximum burst for the specified service flow:

```
Router# sh cr10k-rp c7/0/0 1 service-flow ds
RP SFID  LC SFID  Conform    Exceed     Conform    Exceed     Total      QID
                  Xmit Pkts  Xmit Pkts  Drop Pkts  Drop Pkts  Pkts
32930    10       41         0          0          0          41         131349
Forwarding interface: Modular-Cable1/0/0:0
32931    13       0          0          0          0          0          131350
Forwarding interface: Modular-Cable1/0/0:0
```

Monitoring DOCSIS Operations

The following sections describe the commands that provide information about the DOCSIS network and its cable modems, the RF network and cable interfaces on the CMTS, and BPI+ operations.

Monitoring the DOCSIS Network

The **show cable modem** command is the primary command to display the current state of cable modems and the DOCSIS network. This command has many options that provide information on different aspects of DOCSIS operations.

Tip For a complete description of the **show cable modem** command and its options, see the "Cisco Cable Modem Termination System Commands" chapter in the *Cisco Broadband Cable Command Reference Guide* (see Additional References, on page 64).

Displaying the Status of Cable Modems

The following sample output from the **show cable modem** command shows a list of known cable modems and their current status.

```
Router# show cable modems

MAC Address    IP Address      I/F       MAC         Prim RxPwr  Timing  Num BPI
                                         State       Sid  (db)   Offset  CPE Enb
0010.9507.01db 144.205.151.130 C5/1/0/U5 online(pt)  1     0.25    938   1    Y
0080.37b8.e99b 144.205.151.131 C5/1/0/U5 online      2    -0.25   1268   0    N
0002.fdfa.12ef 144.205.151.232 C6/1/0/U0 online(pt)  13   -0.25   1920   1    Y
0002.fdfa.137d 144.205.151.160 C6/1/0/U0 online      16   -0.50   1920   1    N
0003.e38f.e9ab 144.205.151.237 C6/1/0/U0 online      3    -0.50   1926   1    N
0003.e3a6.8173 144.205.151.179 C6/1/1/U2 offline     4     0.50   1929   0    N
0003.e3a6.8195 144.205.151.219 C6/1/1/U2 online(pt)  22   -0.50   1929   1    Y
0006.28dc.37fd 144.205.151.244 C6/1/1/U2 online(pt)  61    0.00   1925   2    Y
0006.28e9.81c9 144.205.151.138 C6/1/1/U2 online(pt)  2    !0.75   1925   1    Y
0006.28f9.8bbd 144.205.151.134 C6/1/1/U2 #online     25   -0.25   1924   1    N
0002.fdfa.12db 144.205.151.234 C7/0/0/U0 online      15   -0.75   1914   1    N
0002.fdfa.138d 144.205.151.140 C7/0/0/U5 online      4     0.00   1917   1    N
0003.e38f.e85b 144.205.151.214 C7/0/0/U5 online      17   *0.25   1919   1    N
```

You can also display a particular cable modem by specifying its MAC address or IP address with the **show cable modem** command. If you specify the MAC address or IP address for a CPE device, the command will display the information for the cable modem that is associated with that device.

Note If the CPE IP address is no longer associated with a cable modem, the **show cable modem** command might not display information about the cable modem. To display the IP address of the CPE device for the cable modem, use the **clear cable host ip-address** command to clear the IP address of the modem from the router database, and then enter the **ping docsis mac-address** command, which resolves the MAC address by sending the DOCSIS ping to the CM.

```
Router# show cable modem 0010.7bb3.fcd1

MAC Address    IP Address      I/F     MAC         Prim RxPwr Timing Num  BPI
                                       State       Sid  (db)  Offset CPEs Enbld
0010.7bb3.fcd1 10.20.113.2     C5/0/U5 online      1    0.00  1624   0    yes
```

To display a list of cable modems sorted by their manufacturer, use the **vendor** option.

```
Router# show cable modem vendor

Vendor     MAC Address    I/F       MAC         Prim  RxPwr  Timing  Num BPI
                                    State       Sid   (db)   Offset  CPE Enb
```

```
Thomson    0010.9507.01db C5/1/0/U5 online      1     0.00    938   1    N
Ericsson   0080.37b8.e99b C5/1/0/U5 online      2     -0.25   1268  0    N
Cisco      0002.fdfa.12ef C6/1/0/U0 online      13    0.00    1920  1    N
Cisco      0002.fdfa.137d C6/1/0/U0 online      16    -0.50   1920  1    N
Cisco      0003.e38f.e9ab C6/1/0/U0 online      3     -0.25   1926  1    N
Cisco      0003.e3a6.7f69 C6/1/0/U0 online      15    0.50    1927  1    N
Cisco      0003.e3a6.816d C6/1/0/U0 online      4     0.00    1929  1    N
Cisco      0006.28f9.8be5 C6/1/0/U0 online      12    0.75    1922  1    N
Cisco      0001.9659.519f C6/1/1/U2 online      26    0.25    1930  1    N
Cisco      0002.b96f.fdbb C6/1/1/U2 online      29    -0.75   1929  1    N
Cisco      0002.b96f.fdf9 C6/1/1/U2 online      39    -0.50   1931  1    N
Cisco      0002.fdfa.12e9 C6/1/1/U2 online      5     -0.25   1925  1    N
Motorola   0020.4005.3f06 C7/0/0/U0 online      2     0.00    1901  1    N
Motorola   0020.4006.b010 C7/0/0/U5 online      3     0.25    1901  1    N
Cisco      0050.7302.3d83 C7/0/0/U0 online      18    -0.25   1543  1    N
Cisco      00b0.6478.ae8d C7/0/0/U5 online      44    0.50    1920  21   N
Cisco      00d0.bad3.c0cd C7/0/0/U5 online      19    0.00    1543  1    N
```

The MAC state field in each of these displays shows the current state of the cable modem:

Table 7: Descriptions for the MAC State Field

MAC State Value	Description
Registration and Provisioning Status Conditions	
init(r1)	The CM sent initial ranging.
init(r2)	The CM is ranging. The CMTS received initial ranging from the Cm and has sent RF power, timing offset, and frequency adjustments to the CM.
init(rc)	Ranging has completed.
init(d)	The DHCP request was received. This also indicates that the first IP broadcast packet has been received from the CM.
init(i)	The DHCP reply was received and the IP address has been assigned, but the CM has not yet replied with an IP packet.
init(o)	The CM has begun to download the option file (DOCSIS configuration file) using the Trivial File Transfer Protocol (TFTP), as specified in the DHCP response. If the CM remains in this state, it indicates that the download has failed.
init(t)	Time-of-day (TOD) exchange has started.
resetting	The CM is being reset and will shortly restart the registration process.
Non-error Status Conditions	
offline	The CM is considered offline (disconnected or powered down).

MAC State Value	Description
online	The CM has registered and is enabled to pass data on the network.
online(d)	The CM registered, but network access for the CM has been disabled through the DOCSIS configuration file.
online(pk)	The CM registered, BPI is enabled and KEK is assigned.
online(pt)	The CM registered, BPI is enabled and TEK is assigned. BPI encryption is now being performed.
expire(pk)	The Cm registered, BPI is enabled, KEK was assigned but has since expired.
expire(pt)	The Cm registered, BPI is enabled, TEK was assigned but has since expired.
Error Status Conditions	
reject(m)	The CM attempted to register but registration was refused due to a bad Message Integrity Check (MIC) value. This also could indicate that the shared secret in the DOCSIS configuration file does not match the value configured on the CMTS with the **cable shared-secret** command. In Cisco IOS Release 12.1(11b)EC1 and Cisco IOS Release 12.2(8)BC2 or later releases, this could also indicate that the **cable tftp-enforce** command has been used to require that a CM attempt a TFTP download of the DOCSIS configuration file before registering, but the CM did not do so.

MAC State Value	Description
reject(c)	The CM attempted to register, but registration was refused due to a a number of possible errors: • The CM attempted to register with a minimum guaranteed upstream bandwidth that would exceed the limits imposed by the **cable upstream admission-control** command. • The CM has been disabled because of a security violation. • A bad class of service (COS) value in the DOCSIS configuration file. • The CM attempted to create a new COS configuration but the CMTS is configured to not permit such changes.
reject(pk)	KEK key assignment is rejected, BPI encryption has not been established.
reject(pt)	TEK key assignment is rejected, BPI encryption has not been established.
reject(ts)	The CM attempted to register, but registration failed because the TFTP server timestamp in the CM registration request did not match the timestamp maintained by the CMTS. This might indicate that the CM attempted to register by replaying an old DOCSIS configuration file used during a prior registration attempt.
reject(ip)	The CM attempted to register, but registration failed because the IP address in the CM request did not match the IP address that the TFTP server recorded when it sent the DOCSIS configuration file to the CM. IP spoofing could be occurring.
reject(na)	The CM attempted to register, but registration failed because the CM did not send a Registration-Acknowledgement (REG-ACK) message in reply to the Registration-Response (REG-RSP) message sent by the CMTS. A Registration-NonAcknowledgement (REG-NACK) is assumed.

Displaying a Summary Report for the Cable Modems

The **show cable modem** command also can provide a summary report of the cable modems by using the **summary** and **total** options.

```
Router# show cable modem summary

Interface                       Cable Modem
                   Total Registered Unregistered Offline
Cable5/1/0/U5      2     2          0            0
Cable6/1/0/U0      14    13         1            0
Cable6/1/1/U2      14    14         0            0
Cable7/0/0/U0      2     2          0            0
Cable7/0/0/U5      4     3          1            1
Router# show cable modem summary total
Interface                       Cable Modem
                   Total Registered Unregistered Offline
Cable5/1/0/U5      2     2          0            0
Cable6/1/0/U0      14    13         1            0
Cable6/1/1/U2      14    14         0            0
Cable7/0/0/U0      2     2          0            0
Cable7/0/0/U5      4     3          1            1
Total:             36    34         2            1
```

You can also use the **summary** and **total** options to display information for a single interface or a range of interfaces.

```
 Router# show cable modem summary c5/0 total

Interface     Total      Active      Registered
              Modems     Modems      Modems
Cable5/0/U0   294         272         271
Cable5/0/U1   256         248         246
Cable5/0/U2   196         194         194
Total:        746         714         711
Router# show cable modem summary c6/1/1 c7/0/0 total

Interface                       Cable Modem
                   Total Registered Unregistered Offline
Cable6/1/1/U2      14    14         0            0
Cable7/0/0/U0      2     2          0            0
Cable7/0/0/U5      4     3          1            1
Total:             20    19         1            1
```

Displaying the Capabilities of the Cable Modems

To display the capabilities and current DOCSIS provisioning for cable modems, use the **mac** option.

```
Router# show cable modem mac

MAC Address    MAC          Prim  Ver     Prov    Frag  Concat PHS   Priv  DS    US
               State        Sid                                             Saids Sids
0010.64ff.e4ad online       1     DOC1.1  DOC1.0 yes   yes    yes   BPI+  0     4
0010.f025.1bd9 init(rc)     2     DOC1.0  DOC1.0 no    no     no    BPI   0     0
0010.9659.4447 online(pt)   3     DOC1.0  DOC1.0 no    yes    no    BPI   0     0
0010.9659.4461 online(pt)   4     DOC1.0  DOC1.0 no    yes    no    BPI   0     0
0010.64ff.e459 online       5     DOC1.0  DOC1.0 no    yes    no    BPI   0     0
0020.4089.7ed6 online       6     DOC1.0  DOC1.0 no    no     no    BPI   0     0
0090.9607.3831 online(pt)   7     DOC1.0  DOC1.0 no    no     no    BPI   0     0
0090.9607.3830 online(pt)   1     DOC1.0  DOC1.0 no    no     no    BPI   0     0
0050.7366.12fb init(i)      2     DOC1.0  DOC1.0 no    no     no    BPI   0     0
0010.fdfa.0a35 online(pt)   3     DOC1.1  DOC1.1 yes   yes    yes   BPI+  0     4
```

To get a summary report of the cable modems and their capabilities, use the **mac** option with the **summary** and **total** options.

```
Router# show cable modem mac summary
 total

                            Cable Modem Summary
                            -------------------
                         Mac Version                  Provision Mode
Interface       Total   DOC1.1  DOC1.0   Reg/Online   DOC1.1       DOC1.0
Cable5/1/0/U5   1       0       1        1            0            1
Cable6/1/0/U0   11      0       11       8            0            8
Cable6/1/1/U2   17      1       16       15           0            15
Cable7/0/0/U0   2       0       2        1            0            1
Cable7/0/0/U5   1       0       1        0            0            0
Total:          32      1       31       25           0            25
```

Displaying Detailed Information About a Particular Cable Modem

Several options for the show cable modem command display detailed information about a particular cable modem (as identified by its MAC address). The **verbose** option displays the most comprehensive output.

```
Router# show cable modem 0010.7bb3.fcd1 verbose

MAC Address                          : 0010.7bb3.fcd1
IP Address                           : 10.20.113.2
Prim Sid                             : 1
Interface                            : C5/0/U5
Upstream Power                       : 0 dBmV (SNR = 33.25 dBmV)
Downstream Power                     : 0 dBmV (SNR = ----- dBmV)
Timing Offset                        : 1624
Received Power                       :   0.25
MAC Version                          : DOC1.0
Capabilities                         : {Frag=N, Concat=N, PHS=N, Priv=BPI}
Sid/Said Limit                       : {Max Us Sids=0, Max Ds Saids=0}
Optional Filtering Support           : {802.1P=N, 802.1Q=N}
Transmit Equalizer Support           : {Taps/Symbol= 0, Num of Taps= 0}
Number of CPEs                       : 0(Max CPEs = 0)
Flaps                                : 373(Jun 1  13:11:01)
Errors                               : 0 CRCs, 0 HCSes
Stn Mtn Failures                     : 0 aborts, 3 exhausted
Total US Flows                       : 1(1 active)
Total DS Flows                       : 1(1 active)
Total US Data                        : 1452082 packets, 171344434 bytes
Total US Throughput                  : 0 bits/sec, 0 packets/sec
Total DS Data                        : 1452073 packets, 171343858 bytes
Total DS Throughput                  : 0 bits/sec, 0 packets/sec
```

The **connectivity** and **maintenance** options also provide information that can be useful in troubleshooting problems with a particular cable modem.

The following example shows sample output for the **maintenance** option for a particular CM:

```
Router# show cable modem 0010.7bb3.fcd1 connectivity

Prim  1st time    Times  %online     Online time            Offline time
Sid   online      Online           min     avg     max     min     avg     max
1     May 30 2000 4      99.85   48:20   11h34m  1d2h23m 00:01   00:59   03:00
Router# show cable modem 0010.7bb3.fcd1 maintenance

MAC Address    I/F         Prim  SM Exhausted          SM Aborted
                           Sid   Count Time            Count Time
0010.7bb3.fcd1 C5/0/U5     1     3     Jun 1  10:24:52 0     Jan 1  00:00:00
```

Monitoring the RF Network and Cable Interfaces

You can use the **show interface cable** command to display information about the operation of the RF network and the cable interfaces on the CMTS.

Tip For a complete description of the **show cable interface** command and its options, see the "Cisco Cable Modem Termination System Commands" chapter in the *Cisco Broadband Cable Command Reference Guide* (see http://www.cisco.com/c/en/us/td/docs/cable/cbr/configuration/guide/b_cmts_quality_of_services/docsis_1_1.html#ref_1239231).

Displaying Information About Cloned Cable Modems

To display the list of cable modems detected as cloned, use the **privacy hotlist** option with the **show interface cable** command.

The following example shows how to display the cloned cable modems on a particular cable interface:

```
Router# show interface cable 5/1/0 privacy hotlist
                          Last
MAC Address               Ranged On                 Type
00a0.73b0.4c43            Oct 27 21:57:39           Permanent
001a.c3ff.d2d4            Oct 27 21:57:40           Permanent
0018.6852.7746            Never                     Permanent
000e.9bb3.b946            Never                     Permanent
```

Denying RF Access For Cable Modems

To deny radio frequency (RF) access for cable modems during ranging, use the **cable privacy hotlist cm** *mac-address* command.

The following example shows how to block cloned cable modems using their own MAC address:

```
Router(config)# cable privacy hotlist cm 00C0.0102.0304
Router(config)#
```

When an operator identifies a modem's MAC address that should not be registered on a specific CMTS, the operator can add this MAC address to the CMTS using the above command. This command ensures that the modem will not be allowed to come online on any interface on that CMTS.

Displaying Information About the Mac Scheduler

To display information about the DOCSIS MAC layer scheduler that is operating on each cable interface, use the **mac-scheduler** option with the **show cable interface** command. You can display information for all of the upstreams on an interface, or you can display information for a single upstream on an interface.

The following example shows how to display information for the second upstream (U1) on a particular cable interface:

```
Router# show interface cable 3/0 mac-scheduler 1

     DOCSIS 1.1 MAC scheduler for Cable3/0/U1
     Queue[Rng Polls] 0/64, 0 drops
```

```
Queue[CIR Grants] 0/64, 0 drops
Queue[BE(7) Grants] 0/64, 0 drops
Queue[BE(6) Grants] 0/64, 0 drops
Queue[BE(5) Grants] 0/64, 0 drops
Queue[BE(4) Grants] 0/64, 0 drops
Queue[BE(3) Grants] 0/64, 0 drops
Queue[BE(2) Grants] 0/64, 0 drops
Queue[BE(1) Grants] 0/64, 0 drops
Queue[BE(0) Grants] 0/64, 0 drops
Req Slots 81256509, Req/Data Slots 0
Init Mtn Slots 568433, Stn Mtn Slots 68664
Short Grant Slots 2261, Long Grant Slots 2064698
Awacs Slots 0
Fragmentation count 6
Fragmentation test disabled
Avg upstream channel utilization : 1%
Avg percent contention slots : 97%
Avg percent initial ranging slots : 2%
Avg percent minislots lost on late MAPs : 0%
Sched Table Adm-State: Grants 1, Reqpolls 1, Util 20%
UGS    : 0 SIDs, Reservation-level in bps 0
UGS-AD : 1 SIDs, Reservation-level in bps 412800
RTPS   : 0 SIDs, Reservation-level in bps 0
NRTPS  : Not Supported
BE     : 8 SIDs, Reservation-level in bps 0
```

Displaying Information About QoS Parameter Sets

To display information about the DOCSIS 1.1 QoS parameter sets that have been defined on a cable interface, use the **qos paramset** option with the **show cable interface** command.

```
Router# show interface cable 3/0 qos paramset

Index Name              Dir   Sched  Prio MaxSusRate  MaxBurst    MinRsvRate
1                       US    BE     0    64000       0           0
2                       DS    BE     0    1000000     0           0
3                       US    BE     0    200000      1600        0
4                       DS    BE     0    1500000     1522        0
5                       US    BE     0    500000      1522        0
6                       US    UGS_AD
7                       DS    BE     0    2000000     1522        0
8                       US    BE     0    128000      1600        0
9                       DS    BE     0    1000000     1522        0
10                      DS    BE     0    100000      1522        50000
```

You can also display detailed information for a particular parameter set by specifying the index number for its Class of Service along with the **verbose** option.

```
Router# show interface cable 3/0 qos paramset 8 verbose

Index:                                  8
Name:
Direction:                              Upstream
Minimum Packet Size                     64 bytes
Admitted QoS Timeout                    200 seconds
Active QoS Timeout                      0 seconds
Scheduling Type:                        Unsolicited Grant Service(AD)
Request/Transmission Policy:            0x1FF
Nominal Polling Interval:               10000 usecs
Tolerated Poll Jitter:                  2000 usecs
Unsolicited Grant Size:                 500 bytes
Nominal Grant Interval:                 10000 usecs
Tolerated Grant Jitter:                 2000 usecs
Grants per Interval:                    1
IP ToS Overwrite [AND-mask,OR-mask]:    0xFF,0x0
Parameter Presence Bitfield:            {0x0, 0x3FC000}
```

Displaying Information About Service Flows

To display the service flows and their QoS parameter sets that are configured on a cable interface, use the **service-flow** option with the **show interface cable** command.

```
Router# show interface cable 3/0 service-flow

Sfid  Sid   Mac Address     QoS Param Index   Type    Dir    Curr   Active
                           Prov  Adm  Act                  State  Time
4     N/A   0001.9659.4447   4     4    4     prim    DS     act    1d0h39m
3     1     0001.9659.4447   3     3    3     prim    US     act    1d0h39m
6     N/A   0001.64ff.e4ad   6     6    6     prim    DS     act    1d0h39m
14    N/A   0006.2854.7319   9     9    9     prim    DS     act    1d0h2m
457   N/A   0006.2854.7319   10    10   0     sec(S)  DS     adm    00:00
13    6     0006.2854.7319   7     7    7     prim    US     act    1d0h2m
456   155   0006.2854.7319   8     8    8     sec(S)  US    act    21h31m
458   156   0006.2854.7319   0     11   11    dyn(S)  US     act    00:10
16    N/A   0050.7366.12fb   4     4    4     prim    DS     act    1d0h39m
15    7     0050.7366.12fb   3     3    3     prim    US     act    1d0h39m
19    N/A   0090.9607.3831   4     4    4     prim    DS     act    1d0h39m
23    10    0090.9607.3831   3     3    3     prim    US     act    1d0h39m
```

To display the major QoS parameters for each service flow, add the **qos** option to this command.

```
Router# show interface cable 3/0 service-flow qos

Sfid  Dir Curr  Sid   Sched  Prio MaxSusRate  MaxBrst   MinRsvRate  Throughput
          State       Type
14    DS  act   N/A   BE     0    2000000     1522      0           8124
457   DS  adm   N/A   BE     0    100000      1522      50000       0
13    US  act   6     BE     0    500000      1522      0           0
456   US  act   155   UGS_A  0    0           1522      0           57643
19    DS  act   N/A   UGS    0    100000      1522      50000       68715
```

To display the complete QoS parameters for a particular service flow, use the **qos** and **verbose** options. You can use these options separately or together.

```
Router# show interface cable 3/0 service-flow 19 verbose

Sfid                                  : 4
Mac Address                           : 0090.9607.3831
Type                                  : Primary
Direction                             : Downstream
Current State                         : Active
Current QoS Indexes [Prov, Adm, Act]  : [4, 4, 4]
Active Time                           : 21h04m
Sid                                   : N/A
Traffic Priority                      : 0
Maximum Sustained rate                : 100000 bits/sec
Maximum Burst                         : 1522 bytes
Minimum Reserved Rate                 : 0 bits/sec
Admitted QoS Timeout                  : 200 seconds
Active QoS Timeout                    : 0 seconds
Packets                               : 130
Bytes                                 : 123096
Rate Limit Delayed Grants             : 0
Rate Limit Dropped Grants             : 0
Current Throughput                    : 68715 bits/sec, 9 packets/sec
Classifiers: NONE
Router# show interface cable 3/0 service-flow 19 qos verbose

Sfid                                  : 19
Current State                         : Active
Sid                                   : N/A
Traffic Priority                      : 0
Maximum Sustained rate                : 100000 bits/sec
Maximum Burst                         : 1522 bytes
Mimimum Reserved rate                 : 50000 bits/sec
Minimum Packet Size                   : 100 bytes
```

```
Admitted QoS Timeout                    : 200 seconds
Active QoS Timeout                      : 0 seconds
Maximum Latency                         : 20000 usecs
Current Throughput                      : 68715 bits/sec, 9 packets/sec
```

Displaying Information About Service IDs

To display information about Service IDs (SIDs), which are assigned to only upstreams in DOCSIS 1.1 networks, use the **sid** option with the **show interface cable** command.

```
Router# show interface cable 3/0 sid

Sid  Prim  MAC Address    IP Address      Type Age      Admin   Sched  Sfid
                                                        State   Type
1          0090.9607.3831 10.1.1.35       stat 22h26m   enable  BE     3
2          0001.9659.4447 10.1.1.36       stat 22h26m   enable  BE     5
3          0000.f025.1bd9 0.0.0.0         stat 22h26m   enable  BE     7
4          0001.64ff.e4ad 10.1.1.39       stat 22h26m   enable  BE     9
5          0006.2854.7319 10.1.1.41       stat 22h26m   enable  BE     11
6          0001.9659.4461 10.1.1.33       stat 22h26m   enable  BE     13
7          0001.64ff.e459 10.1.1.42       stat 22h26m   enable  BE     15
8    5                                    stat 22h26m   enable  UGS_AD 17
9    5                                    stat 22h26m   enable  BE     18
10         0050.7366.12fb 10.1.1.43       stat 22h26m   enable  BE     20
11         0020.4089.7ed6 10.1.1.40       stat 22h26m   enable  BE     22
12   5                                    dyn  22h26m   enable  UGS    24
13   5                                    dyn  22h26m   enable  BE     25
```

Add the **qos** option to display the major QoS parameters associated with each SID.

```
Router# show interface cable 3/0 sid qos

Sid  Pr MaxSusRate MinRsvRate Sched  Grant Grant  GPI Poll   Thrput
                              Type   Size  Intvl      Intvl
1    0  200000     0          BE     100   100000 1   100000 848
2    0  200000     0          BE     100   100000 1   100000 0
3    0  64000      0          BE     0     0      0   0      0
4    0  128000     0          BE     100   100000 1   100000 0
5    0  500000     0          BE     100   100000 1   100000 0
6    0  200000     0          BE     100   100000 1   100000 848
7    0  128000     0          BE     100   100000 1   100000 0
8    0  0          0          UGS_AD 500   10000  1   10000  3468
9    0  100000     0          BE     100   100000 1   100000 0
10   0  200000     0          BE     100   100000 1   100000 848
11   0  200000     0          BE     100   100000 1   100000 848
12   0  0          0          UGS    150   100000 1   100000 0
13   0  7000       0          BE     100   100000 1   100000 0
```

To display detailed information about a particular SID and its QoS parameters, use both the **qos** and **verbose** options.

```
Router# show interface cable 3/0 sid 1 qos verbose

Sid                                     : 1
Traffic Priority                        : 0
Maximum Sustained Rate                  : 200000 bits/sec
Maximum Burst                           : 1600 bytes
Minimum Reserved Rate                   : 0 bits/sec
Minimum Packet Size                     : 64 bytes
Admitted QoS Timeout                    : 200 seconds
Active QoS Timeout                      : 0 seconds
Maximum Concatenated Burst              : 1600 bytes
Scheduling Type                         : Best Effort
Nominal Grant Interval                  : 100000 usecs
Tolerated Grant Jitter                  : 2000 usecs
Nominal Polling Interval                : 100000 usecs
Tolerated Polling Jitter                : 2000 usecs
Unsolicited Grant Size                  : 100 bytes
Grants per Interval                     : 1
```

```
Request/Transmission Policy             : 0x0
IP ToS Overwrite [AND-mask, OR-mask]    : 0xFF, 0x0
Current Throughput                      : 863 bits/sec, 0 packets/sec
```

Monitoring BPI+ Operations

See the following sections to monitor the state of BPI operations on the CMTS and its connected cable modems:

Displaying the Current BPI+ State of Cable Modems

To display the current BPI+ state of cable modems, use the **show cable modem** command. If used without any options, this command displays the status for cable modems on all interfaces. You can also specify a particular cable interface on the CMTS, or the IP address or MAC address for a specific cable modem:

```
Router# show cable modem
 [ip-address
 | interface
 | mac-address
```

The following display shows a typical display for cable modems on all interfaces:

```
Router# show cable modem

MAC Address    IP Address      I/F     MAC         Prim RxPwr Timing Num  BPI
                                       State       Sid  (db)  Offset CPEs Enbld
0010.7b6b.58c1 0.0.0.0         C4/0/U5 offline     5   -0.25  2285   0    yes
0010.7bed.9dc9 0.0.0.0         C4/0/U5 offline     6   -0.75  2290   0    yes
0010.7bed.9dbb 0.0.0.0         C4/0/U5 online(pt)  7    0.50  2289   0    yes
0010.7b6b.58bb 0.0.0.0         C4/0/U5 reject(pk)  8    0.00  2290   0    yes
0010.7bb3.fcd1 10.20.113.2     C5/0/U5 online(pt)  1    0.00  1624   0    yes
0010.7bb3.fcdd 0.0.0.0         C5/0/U5 online(pk)  2   -20.00 1624   0    yes
0010.7b43.aa7f 0.0.0.0         C5/0/U5 reject(pt)  3    7.25  1623   0    yes
```

The following shows a typical display for a Cisco uBR10012 router for a specific interface:

```
Router# show cable modems c7/0/0

MAC Address    IP Address      I/F       MAC         Prim RxPwr  Timing  Num BPI
                                         State       Sid  (db)   Offset  CPE Enb
0002.fdfa.12db 144.205.151.234 C7/0/0/U0 offline     15    -0.75   1914  1    Y
0002.fdfa.138d 144.205.151.140 C7/0/0/U5 online(pk)  4     0.00    1917  1    Y
0003.e38f.e85b 144.205.151.214 C7/0/0/U5 reject(pk)  17   *0.25    1919  1    Y
0003.e38f.f4cb 144.205.151.238 C7/0/0/U5 online(pt)  16    0.00   !2750  1    Y
0003.e3a6.7fd9 144.205.151.151 C7/0/0/U5 online(pt)  1     0.25    1922  0    Y
0020.4005.3f06 144.205.151.145 C7/0/0/U0 online(pt)  2     0.00    1901  1    Y
0020.4006.b010 144.205.151.164 C7/0/0/U5 online(pt)  3     0.00    1901  1    Y
0050.7302.3d83 144.205.151.240 C7/0/0/U0 online(pt)  18    -0.25   1543  1    Y
00b0.6478.ae8d 144.205.151.254 C7/0/0/U5 online(pt)  44    0.25    1920  21   Y
00d0.bad3.c0cd 144.205.151.149 C7/0/0/U5 online(pk)  19    0.25    1543  1    Y
00d0.bad3.c0cf 144.205.151.194 C7/0/0/U0 online(pt)  13    0.00    1546  1    Y
00d0.bad3.c0d5 144.205.151.133 C7/0/0/U0 reject(pt)  12   *0.50    1546  1    Y
```

The following shows a typical display for a particular cable modem:

```
Router# show cable modem 00C0.abcd.ef01

MAC Address    IP Address      I/F     MAC         Prim RxPwr Timing Num  BPI
                                       State       Sid  (db)  Offset CPEs Enbld
00c0.abcd.ef01 10.20.113.2     C5/0/U5 online(pt)  1    0.00  1624   0    yes
```

The MAC State column displays the current status of each cable modem. The following are the possible BPI-related values for this field:

Table 8: Possible show cable modem BPI+ States

State	Description
online	A cable modem has come online and, if configured to use BPI+, is negotiating its privacy parameters for the session. If the modem remains in this state for more than a couple of minutes, it is online but not using BPI+. Check that the cable modem is running DOCSIS-certified software and is using a DOCSIS configuration file that enables BPI+.
online(pk)	The cable modem is online and has negotiated a Key Encryption Key(KEK) with the CMTS. If BPI+ negotiation is successful, this state will be shortly followed by online(pt).
online(pt)	The cable modem is online and has negotiated a Traffic Encryption Key (TEK) with the CMTS. The BPI+ session has been established, and the cable modem is encrypting all user traffic with the CMTS using the specified privacy parameters.
reject(pk)	The cable modem failed to negotiate a KEK with the CMTS, typically because the cable modem failed authentication. Check that the cable modem is properly configured for BPI+ and is using valid digital certificates. If the CMTS requires BPI+ for registration, the cable modem will go offline and have to reregister. Check that the cable modem is properly registered in the CMTS provisioning system. **Note** If a cable modem fails BPI+ authentication, a message similar to the following appears in the CMTS log: `%UBR7200-5-UNAUTHSIDTIMEOUT: CMTS deleted BPI unauthorized Cable Modem 00c0.abcd.ef01`
reject(pt)	The cable modem failed to successfully negotiate a TEK with the CMTS. If the CMTS requires BPI+ for registration, the cable modem will have to reregister.

Displaying the BPI+ Timer Values on the CMTS

To display the values for the KEK and TEK lifetime timers on a particular cable interface, use the **show interface cable** *x/y* **privacy** [**kek** | **tek**] command. For example:

```
Router# show interface cable 4/0 privacy kek

Configured KEK lifetime value = 604800
Router# show interface cable 4/0 privacy tek
```

```
Configured TEK lifetime value = 60480
```

Displaying the Certificate List on the CMTS

Use the **show crypt ca certificates** command to display the list of known certificates on the CMTS. For example:

```
Router# show crypto ca certificates

Certificate
  Status: Available
  Certificate Serial Number: 7DBF85DDDD8358546BB1C67A16B3D832
  Key Usage: General Purpose
  Subject Name
    Name: Cisco Systems
  Validity Date:
    start date: 00:00:00 UTC Sep 12 2001
    end   date: 23:59:59 UTC Sep 11 2021
Root certificate
  Status: Available
  Certificate Serial Number: 5853648728A44DC0335F0CDB33849C19
  Key Usage: General Purpose
    CN = DOCSIS Cable Modem Root Certificate Authority
     OU = Cable Modems
     O = Data Over Cable Service Interface Specifications
     C = US
  Validity Date:
    start date: 00:00:00 UTC Feb 1 2001
    end   date: 23:59:59 UTC Jan 31 2031
```

Configuration Examples for DOCSIS 1.1 Operations

This section lists the following sample configurations for DOCSIS 1.1 operations on the Cisco CMTS:

Example: DOCSIS 1.1 Configuration for Cisco uBR7246VXR Router (without BPI+)

```
version 12.2
no service pad
service timestamps log datetime localtime
service password-encryption
service udp-small-servers max-servers no-limit
!
hostname 7246VXR
!
enable password 7 030A69CE09
!
cable qos profile 8
cable qos profile 10
cable qos profile 10 grant-size 1500
cable qos profile 12 guaranteed-upstream 100000
no cable qos permission create
no cable qos permission update
cable qos permission modems
cable timeserver
!
cable config-file disable.cm
 access-denied
 service-class 1 max-upstream 1
```

```
 service-class 1 max-downstream 1600
 cpe max 1
 timestamp
!
cable config-file platinum.cm
 service-class 1 max-upstream 128
 service-class 1 guaranteed-upstream 10
 service-class 1 max-downstream 10000
 service-class 1 max-burst 1600
 cpe max 10
 timestamp
!
clock timezone PDT -8
clock summer-time PDT recurring
clock calendar-valid
ip subnet-zero
ip cef
ip cef accounting per-prefix
no ip finger
ip tcp synwait-time 5
no ip domain-lookup
ip host vxr 192.100.168.103
ip domain-name cisco.com
ip name-server 192.100.168.70
ip name-server 192.100.168.132
ip name-server 192.100.168.250
no ip dhcp relay information check
!
!
!
ip dhcp pool cm-platinum
network 10.10.4.0 255.255.255.0
   bootfile platinum.cm
   next-server 10.10.4.1
   default-router 10.10.4.1
   option 7 ip 10.10.4.1
   option 4 ip 10.10.4.1
   option 2 hex ffff.8f80
   lease 7 0 10
!
ip dhcp pool pcs-c4
   network 192.100.168.0 255.255.255.224
   next-server 192.100.168.1
   default-router 192.100.168.1
   dns-server 192.100.168.2
   domain-name cisco.com
   lease 7 0 10
!
!
interface Ethernet2/0
 ip address 192.100.168.4 255.255.255.192
 no ip mroute-cache
 half-duplex
!
interface Cable4/0
 ip address 192.100.168.1 255.255.255.224 secondary
 ip address 10.10.4.1 255.255.255.0
 no ip route-cache cef
 no keepalive
 cable downstream rate-limit token-bucket shaping
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream frequency 555000000
 cable upstream 0 frequency 40000000
 cable upstream 0 power-level 0
 no cable upstream 0 shutdown
 cable upstream 1 shutdown
 cable upstream 2 shutdown
 cable upstream 3 shutdown
 cable upstream 4 shutdown
 cable upstream 5 shutdown
 cable dhcp-giaddr policy
```

```
!
!
router eigrp 202
 redistribute connected
 redistribute static
 network 10.0.0.0
 network 192.100.168.0
 no auto-summary
 no eigrp log-neighbor-changes
!
router rip
 version 2
 redistribute connected
 redistribute static
 network 10.0.0.0
 network 192.100.168.0
 no auto-summary
!
ip default-gateway 192.100.168.1
ip classless
ip route 0.0.0.0 0.0.0.0 192.100.168.1
ip route 192.100.168.0 255.255.255.0 Ethernet2/0
ip http server
ip http authentication local
!
snmp-server engineID local 00000009020000E01ED77E40
snmp-server community public RO
snmp-server community private RW
tftp-server server
 tftp-server slot0:silver.cm alias silver.cm
 !
line con 0
 exec-timeout 0 0
 transport input none
line aux 0
 speed 19200
line vty 0 4
 session-timeout 60
 login
!
ntp clock-period 17179977
ntp server 192.100.168.51
end
```

Example: DOCSIS 1.1 Configuration for Cisco uBR7246VXR Router (with BPI+)

```
version 12.2
no service pad
service password-encryption
service compress-config
!
hostname uBR7246VXR
!
logging queue-limit 100
enable password 7 03085A09
!
clock summer-time EDT recurring
clock calendar-valid
cable flap-list insertion-time 120
cable flap-list power-adjust threshold 5
cable flap-list aging 1440
cable modem max-cpe 2
cable modulation-profile 2 request 0 16 2 8 qpsk scrambler 152 no-diff 64 fixed uw8
cable modulation-profile 2 initial 5 34 0 48 qpsk scrambler 152 no-diff 128 fixed uw16
cable modulation-profile 2 station 5 34 0 48 qpsk scrambler 152 no-diff 128 fixed uw16
cable modulation-profile 2 short 5 91 14 8 qpsk scrambler 152 no-diff 72 shortened uw8
cable modulation-profile 2 long 8 239 0 8 qpsk scrambler 152 no-diff 80 shortened uw8
cable modulation-profile 3 request 0 16 2 8 qpsk scrambler 152 no-diff 64 fixed uw8
cable modulation-profile 3 initial 5 34 0 48 qpsk scrambler 152 no-diff 128 fixed uw16
```

```
cable modulation-profile 3 station 5 34 0 48 qpsk scrambler 152 no-diff 128 fixed uw16
cable modulation-profile 3 short 8 85 14 8 qpsk scrambler 152 no-diff 72 shortened uw8
cable modulation-profile 3 long 10 235 0 8 qpsk scrambler 152 no-diff 80 shortened uw8
cable modulation-profile 4 request 0 16 2 8 qpsk scrambler 152 no-diff 64 fixed uw8
cable modulation-profile 4 initial 5 34 0 48 qpsk scrambler 152 no-diff 128 fixed uw16
cable modulation-profile 4 station 5 34 0 48 qpsk scrambler 152 no-diff 128 fixed uw16
cable modulation-profile 4 short 10 8 6 8 8 16qam scrambler 152 no-diff 144 shortened uw16
cable modulation-profile 4 long 10 235 0 8 16qam scrambler 152 no-diff 160 shortened uw16
no cable qos permission create
no cable qos permission update
cable qos permission modems
cable logging badipsource 2000000
cable time-server
!
!
ip subnet-zero
no ip source-route
!
!
ip cef
ip domain name sampleclient.com
ip dhcp smart-relay
ip dhcp relay information option
no ip dhcp relay information check
!
crypto ca trustpoint DOCSIS-ROOT-CERT
!
crypto ca certificate chain DOCSIS-ROOT-CERT
 certificate ca 00A0730000000002
  308202B7 30820220 A0030201 02020800 A0730000 00000230 0D06092A 864886F7
  0D010105 05003081 9D310B30 09060355 04061302 5553310E 300C0603 55040A13
  05436F6D 3231310F 300D0603 55040B13 06444F43 53495331 36303406 0355040B
  132D4C4F 43303030 332C2037 35302054 61736D61 6E204472 6976652C 204D696C
  70697461 732C2043 41203935 30333531 35303306 03550403 132C436F 6D323120
  4361626C 65204D6F 64656D20 526F6F74 20436572 74696669 63617465 20417574
  686F7269 7479301E 170D3030 30353038 30373030 30305A17 0D323530 35303830
  37303030 305A3081 9D310B30 09060355 04061302 5553310E 300C0603 55040A13
  05436F6D 3231310F 300D0603 55040B13 06444F43 53495331 36303406 0355040B
  132D4C4F 43303030 332C2037 35302054 61736D61 6E204472 6976652C 204D696C
  70697461 732C2043 41203935 30333531 35303306 03550403 132C436F 6D323120
  4361626C 65204D6F 64656D20 526F6F74 20436572 74696669 63617465 20417574
  686F7269 74793081 9F300D06 092A8648 86F70D01 01010500 03818D00 30818902
  818100D9 C1A4199A 47D4FFAD B43F573C D1232742 748D2C91 B89E9FE9 94277008
  FBA544C8 5CC4FE3F 754BA64B AEE5A362 32A41BFE B9FD03C2 99242D95 0508DC45
  1A007021 FEC688F9 E57D9161 DE43E4EC 29379E9E 3AEB3563 455AF3B6 2C345A31
  70F4FCF6 FB39FC6E 815F05CF EC6E618A 52562F26 098C5BE1 48FD46DE E07078A9
  DD962902 03010001 300D0609 2A864886 F70D0101 05050003 8181001B DFAF32FD
  38FF13E8 CD5063C6 4663D00A 2F3132FB 25D9F6DF 1CC67C1B 5CDB5F02 825F2DD2
  72C07A3C 7EB0B138 F217E0BA CCBCF712 19AB117E 76193E86 3E7C8532 B44228A1
  0E19643A B44D66B6 15F8F142 9ECF54F6 AFCA093E A6D59067 E3F9306C 5696BF5F
  C34999A5 5F36F368 EAFAA8DD BAD93942 8620C59C 879EB625 88C3A1
  quit
!
!
!
 key chain ubr7246-rip
 key 1
  key-string 7 0600066C594C1B4F0E574345460133
!
!
interface FastEthernet0/0
ip address 192.168.10.130 255.255.255.0
 duplex half
 tag-switching ip
 no cdp enable
!
interface Ethernet1/0
 ip address 10.10.0.1 255.255.0.0
 no ip redirects
 no ip proxy-arp
 ip pim dense-mode
 no ip mroute-cache
 duplex half
```

```
 no keepalive
 no cdp enable
!
interface Ethernet1/1
 ip address 10.11.0.1 255.255.0.0
 no ip redirects
 no ip proxy-arp
 ip pim dense-mode
 duplex half
 no keepalive
 no cdp enable
!
interface Ethernet2/0
 ip address 192.168.10.2 255.255.0.0
 shutdown
 duplex half
 no cdp enable
!
interface Ethernet2/1
 ip address 192.168.10.1 255.255.0.0
 duplex half
 no cdp enable
!
interface Cable3/0
 ip address 192.168.10.77 255.255.255.0
 ip mask-reply
 no ip redirects
 no ip proxy-arp
 ip pim sparse-dense-mode
 ip route-cache flow
 ip igmp access-group 96
 no ip mroute-cache
 cable map-advance dynamic 400 1000
 cable insertion-interval automatic 25 500
 cable bundle 1 master
 cable downstream annex B
 cable downstream modulation 256qam
 cable downstream interleave-depth 32
 cable downstream channel-id 0
 cable upstream 0 frequency 5008000
 cable upstream 0 power-level 0
 cable upstream 0 channel-width 1600000 1600000
 cable upstream 0 minislot-size 4
 cable upstream 0 modulation-profile 2
 no cable upstream 0 shutdown
 cable upstream 1 frequency 7008000
 cable upstream 1 power-level 0
 cable upstream 1 channel-width 1600000 1600000
 cable upstream 1 minislot-size 4
 cable upstream 1 modulation-profile 2
 no cable upstream 1 shutdown
 cable upstream 2 frequency 10000000
 cable upstream 2 power-level 0
 cable upstream 2 channel-width 1600000 1600000
 cable upstream 2 minislot-size 4
 cable upstream 2 modulation-profile 2
 no cable upstream 2 shutdown
 cable upstream 3 frequency 13008000
 cable upstream 3 power-level 0
 cable upstream 3 channel-width 1600000 1600000
 cable upstream 3 minislot-size 4
 cable upstream 3 modulation-profile 2
 no cable upstream 3 shutdown
 cable upstream 4 frequency 16000000
 cable upstream 4 power-level 0
 cable upstream 4 channel-width 1600000 1600000
 cable upstream 4 minislot-size 4
 cable upstream 4 modulation-profile 2
 no cable upstream 4 shutdown
 cable upstream 5 frequency 20000000
 cable upstream 5 power-level 0
 cable upstream 5 channel-width 1600000 1600000
 cable upstream 5 minislot-size 4
```

```
 cable upstream 5 modulation-profile 2
 no cable upstream 5 shutdown
 cable dhcp-giaddr policy
 cable privacy accept-self-signed-certificate
 cable privacy authenticate-modem
 cable privacy authorize-multicast
 cable privacy kek life-time 300
 cable privacy tek life-time 180
 no keepalive
!
interface Cable4/0
 ip address 192.168.10.55 255.255.255.0
 ip mask-reply
 no ip redirects
 no ip proxy-arp
 ip multicast ttl-threshold 5
 ip multicast boundary 15
 ip route-cache flow
 no ip mroute-cache
 cable map-advance dynamic 400 1000
 cable insertion-interval automatic 25 500
 cable bundle 1
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream channel-id 1
 cable upstream 0 frequency 30000000
 cable upstream 0 power-level 0
 cable upstream 0 channel-width 1600000 1600000
 cable upstream 0 minislot-size 4
 cable upstream 0 modulation-profile 3
 no cable upstream 0 shutdown
 cable upstream 1 frequency 31008000
 cable upstream 1 power-level 0
 cable upstream 1 channel-width 1600000 1600000
 cable upstream 1 minislot-size 4
 cable upstream 1 modulation-profile 3
 no cable upstream 1 shutdown
 cable upstream 2 frequency 32000000
 cable upstream 2 power-level 0
 cable upstream 2 channel-width 1600000 1600000
 cable upstream 2 minislot-size 4
 cable upstream 2 modulation-profile 3
 no cable upstream 2 shutdown
 cable upstream 3 frequency 33008000
 cable upstream 3 power-level 0
 cable upstream 3 channel-width 1600000 1600000
 cable upstream 3 minislot-size 4
 no cable upstream 3 shutdown
 cable upstream 4 frequency 34000000
 cable upstream 4 power-level 0
 cable upstream 4 channel-width 1600000 1600000
 cable upstream 4 minislot-size 4
 cable upstream 4 modulation-profile 3
 no cable upstream 4 shutdown
 cable upstream 5 frequency 35008000
 cable upstream 5 power-level 0
 cable upstream 5 channel-width 1600000 1600000
 cable upstream 5 minislot-size 4
 cable upstream 5 modulation-profile 3
 no cable upstream 5 shutdown
 cable source-verify leasetimer 5
 cable dhcp-giaddr policy
 cable privacy accept-self-signed-certificate
 cable privacy authenticate-modem
 cable privacy authorize-multicast
 cable privacy kek life-time 300
 cable privacy tek life-time 180
 no keepalive
!
!
router rip
 version 2
```

```
 redistribute bgp 222 metric transparent
 network 10.10.0.0
 no auto-summary
!
!
ip default-gateway 192.168.100.1
ip classless
no ip forward-protocol udp netbios-ns
no ip forward-protocol udp netbios-dgm
 no ip http server
no ip http secure-server
!
!
!
!
snmp-server community private RW
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps config
snmp-server enable traps cable
snmp-server enable traps docsis-cmts
snmp-server enable traps syslog
!
line con 0
 exec-timeout 0 0
 password 7 070C285F4D06
 stopbits 1
line vty 0 4
 session-timeout 60
 exec-timeout 0 0
 password 7 0703204E
line vty 5 15
!
scheduler allocate 4000 200
end
```

Example: DOCSIS 1.1 Configuration for Cisco uBR10012 Router (with BPI+)

```
version 12.2
service timestamps log datetime msec localtime
service password-encryption
!
hostname uBR10012
!
redundancy
 main-cpu
  auto-sync standard
logging queue-limit 100
no logging buffered
no logging rate-limit
enable password my-enable-password
!
ipc cache 5000
card 1/1 2cable-tccplus
card 2/0 1gigethernet-1
card 2/1 2cable-tccplus
card 3/0 1gigethernet-1
card 4/0 1oc12pos-1
card 8/0 5cable-mc520s
card 8/1 5cable-mc520s
cable flap-list insertion-time 60
cable flap-list power-adjust threshold 4
cable flap-list aging 86400
cable modem vendor 00.50.F1 TI
cable spectrum-group 2 band 11000000 16000000
cable spectrum-group 21 band 17000000 25000000
cable spectrum-group 32 shared
cable spectrum-group 32 band 5000000 42000000
cable modulation-profile 2 request 0 16 0 8 qpsk scrambler 152 no-diff 64 fixed uw16
cable modulation-profile 2 initial 5 34 0 48 qpsk scrambler 152 no-diff 128 fixed uw16
```

```
cable modulation-profile 2 station 5 34 0 48 qpsk scrambler 152 no-diff 128 fixed uw16
cable modulation-profile 2 short 6 75 6 8 16qam scrambler 152 no-diff 144 shortened uw8
cable modulation-profile 2 long 8 220 0 8 16qam scrambler 152 no-diff 160 shortened uw8
cable modulation-profile 21 request 0 16 0 22 qpsk scrambler 152 no-diff 32 fixed
cable modulation-profile 21 initial 5 34 0 48 qpsk scrambler 152 no-diff 64 fixed
cable modulation-profile 21 station 5 34 0 48 qpsk scrambler 152 no-diff 64 fixed
cable modulation-profile 21 short 3 76 12 22 qpsk scrambler 152 no-diff 64 shortened
cable modulation-profile 21 long 7 231 0 22 qpsk scrambler 152 no-diff 64 shortened
cable modulation-profile 22 request 0 16 0 22 qpsk scrambler 152 no-diff 32 fixed
cable modulation-profile 22 initial 5 34 0 48 qpsk scrambler 152 no-diff 64 fixed
cable modulation-profile 22 station 5 34 0 48 qpsk scrambler 152 no-diff 64 fixed
cable modulation-profile 22 short 4 76 7 22 16qam scrambler 152 no-diff 128 shortened
cable modulation-profile 22 long 7 231 0 22 16qam scrambler 152 no-diff 128 shortened
cable modulation-profile 23 request 0 16 0 22 qpsk scrambler 152 no-diff 32 fixed
cable modulation-profile 23 initial 5 34 0 48 qpsk scrambler 152 no-diff 64 fixed
cable modulation-profile 23 station 5 34 0 48 qpsk scrambler 152 no-diff 64 fixed
cable modulation-profile 23 short 4 76 7 22 16qam scrambler 152 no-diff 128 shortened
cable modulation-profile 23 long 7 231 0 22 16qam scrambler 152 no-diff 128 shortened
cable qos profile 5 max-downstream 10000
cable qos profile 5 max-upstream 1000
cable qos profile 5 priority 7
cable qos profile 5 tos-overwrite 0x3  0x0
cable qos profile 5 name cm_no_priority
cable qos profile 6 max-downstream 10000
cable qos profile 6 max-upstream 5000
cable qos profile 6 priority 7
cable qos profile 6 tos-overwrite 0x3  0x0
cable qos profile 6 name qos6
cable qos profile 7 max-downstream 128
cable qos profile 7 max-upstream 128
cable qos profile 7 priority 7
cable qos profile 8 max-downstream 10000
cable qos profile 8 max-upstream 1000
cable qos profile 8 priority 3
cable qos profile 8 tos-overwrite 0x3  0x0
cable qos profile 8 name qos8
no cable qos permission create
no cable qos permission update
cable qos permission modems
cable event syslog-server 10.10.10.131
ip subnet-zero
!
!
interface FastEthernet0/0/0
 ip address 10.10.32.21 255.255.0.0
 no cdp enable
!
interface GigabitEthernet2/0/0
 ip address 10.10.31.2 255.0.0.0
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 load-interval 30
 negotiation auto
 no cdp enable
!
interface GigabitEthernet3/0/0
 no ip address
 ip pim sparse-mode
 no ip route-cache cef
 load-interval 30
 shutdown
 negotiation auto
 no cdp enable
!
interface POS4/0/0
 no ip address
 crc 32
 no cdp enable
 pos ais-shut
!
!
interface Cable8/0/0
```

```
 ip address 10.10.10.28 255.255.255.0
 ip helper-address 1.10.10.133
 cable bundle 2 master
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream frequency 669000000
 cable downstream channel-id 0
 no cable downstream rf-shutdown
 cable downstream rf-power 45
 cable upstream 0 connector 0
 cable upstream 0 spectrum-group 32
 cable upstream 0 power-level 0
 cable upstream 0 channel-width 1600000
 cable upstream 0 minislot-size 4
 cable upstream 0 range-backoff 3 6
 cable upstream 0 data-backoff 0 6
 cable upstream 0 modulation-profile 23
 no cable upstream 0 rate-limit
 no cable upstream 0 shutdown
 cable upstream 1 connector 1
 cable upstream 1 spectrum-group 32
 cable upstream 1 power-level 0
 cable upstream 1 channel-width 1600000
 cable upstream 1 minislot-size 4
 cable upstream 1 data-backoff 0 6
 cable upstream 1 modulation-profile 23
 no cable upstream 1 shutdown
 cable upstream 2 connector 2
 cable upstream 2 spectrum-group 32
 cable upstream 2 power-level 0
 cable upstream 2 channel-width 1600000
 cable upstream 2 minislot-size 4
 cable upstream 2 data-backoff 3 6
 cable upstream 2 modulation-profile 23
 no cable upstream 2 shutdown
 cable upstream 3 connector 3
 cable upstream 3 spectrum-group 32
 cable upstream 3 channel-width 1600000
 cable upstream 3 minislot-size 4
 cable upstream 3 modulation-profile 21
 no cable upstream 3 shutdown
 cable source-verify
 cable privacy kek life-time 300
 cable privacy tek life-time 180
 no keepalive
!
interface Cable8/0/1
 ip address 10.10.11.121
 cable bundle 2
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream frequency 453000000
 cable downstream channel-id 0
 no cable downstream rf-shutdown
 cable upstream max-ports 6
 cable upstream 0 connector 4
 cable upstream 0 spectrum-group 2
 cable upstream 0 power-level 0
 cable upstream 0 channel-width 1600000
 cable upstream 0 minislot-size 4
 cable upstream 0 range-backoff 3 6
 cable upstream 0 data-backoff 0 6
 cable upstream 0 modulation-profile 23 21
 no cable upstream 0 rate-limit
 cable upstream 0 shutdown
 cable upstream 1 connector 5
 cable upstream 1 channel-width 1600000
 cable upstream 1 minislot-size 4
 cable upstream 1 modulation-profile 21
 cable upstream 1 shutdown
 cable upstream 2 connector 6
```

```
 cable upstream 2 channel-width 1600000
 cable upstream 2 minislot-size 4
 cable upstream 2 modulation-profile 21
 cable upstream 2 shutdown
 cable upstream 3 connector 7
 cable upstream 3 channel-width 1600000
 cable upstream 3 minislot-size 4
 cable upstream 3 modulation-profile 21
 cable upstream 3 shutdown
 cable upstream 4 channel-width 1600000
 cable upstream 4 minislot-size 4
 cable upstream 4 modulation-profile 21
 cable upstream 4 shutdown
 cable upstream 5 channel-width 1600000
 cable upstream 5 minislot-size 4
 cable upstream 5 modulation-profile 21
 cable upstream 5 shutdown
 cable source-verify
 cable privacy kek life-time 300
 cable privacy tek life-time 180
 no keepalive
!
!
ip classless
ip http server
no ip http secure-server
!
!
no cdp run
snmp-server community public RW
snmp-server community private RW
snmp-server enable traps cable
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 exec-timeout 0 0
 password my-telnet-password
 login
 length 0
!
end
```

Additional References

For additional information related to DOCSIS 1.1 operations, refer to the following references:

Related Documents

Related Topic	Document Title
Commands on the Cisco CMTS routers	*Cisco IOS CMTS Cable Command Reference* http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html
HCCP N+1 Configuration	*N+1 Redundancy for the Cisco CMTS Routers* http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/cmts_nplus1_redun.html

Standards

Standards[1]	Title
SP-RFIv1.1-I08-020301	*Data-over-Cable Service Interface Specifications Radio Frequency Interface Specification*
SP-BPI+-I08-020301	*DOCSIS Baseline Privacy Interface Plus Specification*

1 Not all supported standards are listed.

MIBs

MIBs[2]	MIBs Link
• DOCS-BPI-PLUS-MIB • DOCS-CABLE-DEVICE-MIB (RFC 2669) • DOCS-CABLE-DEVICE-TRAP-MIB • DOCS-IF-EXT-MIB • DOCS-IF-MIB (RFC 2670) • DOCS-QOS-MIB • DOCS-SUBMGT-MIB • IGMP-STD-MIB (RFC 2933)	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

2 Not all supported MIBs are listed.

RFCs

RFCs[3]	Title
RFC 2669	DOCS-CABLE-DEVICE-MIB
RFC 2670	DOCS-IF-MIB
RFC 2933	IGMP-STD-MIB

3 Not all supported RFCs are listed.

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 DOCSIS 1.1 for the Cisco CMTS Routers

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

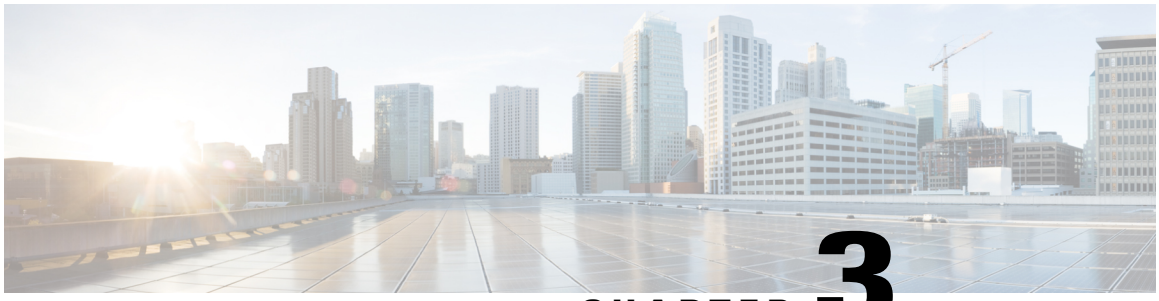
Note The table below lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 9: Feature Information for DOCSIS 1.1 for the Cisco CMTS Routers

Feature Name	Releases	Feature Information
DOCSIS 1.1 for the Cisco CMTS	12.1(4)CX	DOCSIS 1.1 support was introduced for Cisco uBR7200 series routers.
DOCSIS 1.1 for the Cisco CMTS	12.1(7)CX1	Several DOCSIS 1.1 MIBs were updated, reflecting changes in the DOCSIS 1.1 specification. The **cable submgmt default** command was also added, to set the default value of the attributes in DOCS-SUBMGT-MIB.
DOCSIS 1.1 for the Cisco CMTS	12.2(4)BC1	DOCSIS 1.1 support was introduced for the Cisco uBR7100 series, Cisco uBR7200 series, and Cisco uBR10012 routers on the Release 12.2 BC train.

Feature Name	Releases	Feature Information
N+1 redundancy	12.2(4)BC1b	N+1 redundancy during DOCSIS 1.1 operations was supported on the Cisco uBR10012 router.
N+1 redundancy	12.2(11)BC1	N+1 redundancy during DOCSIS 1.1 operations was supported on the Cisco uBR7200 series router.
UGS service flows	12.2(11)BC2	The **packetcable authorize vanilla-docsis-mta** command was supported to allow DOCSIS 1.1 cable modems to use UGS service flows when PacketCable operations have been enabled.
Enhanced Rate Bandwidth Allocation (ERBA)	12.3(13a)BC	Added support for Enhanced Rate Bandwidth Allocation (ERBA) for DOCSIS 1.0 cable modems, to include the following new configuration command and show command enhancement: • cable qos pro max-ds-burst • show cable qos profile Refer to the Enhanced Rate Bandwidth Allocation (ERBA) Support for DOCSIS 1.0 Cable Modems, on page 21.
Enhanced version of ERBA	12.3(21)BC	Added support for an enhanced version of ERBA on the Cisco uBR10012 router. Refer to the Enhanced Rate Bandwidth Allocation (ERBA) Support for DOCSIS 1.0 Cable Modems, on page 21.
DOCSIS 3.0 Downstream Peak Traffic Rate TLV Support for ERBA	12.2(33)SCB1	The ERBA feature was enhanced with the peak-rate keyword of the cable ds-max-burst command for the Cisco uBR10012 router.
DOCSIS 3.0 Downstream Peak Traffic Rate TLV Support for ERBA	12.2(33)SCD	Added support for Cisco uBR7246VXR and Cisco uBR7225VXR routers.

Feature Name	Releases	Feature Information
Suppressing Downstream and Upstream Peak Rate TLVs for pre DOCSIS 3.0 Cable Modems	12.2(33)SCB10	Support was added to restrict sending of the DOCSIS 3.0 TLVs to DOCSIS 1.X and DOCSIS 2.0 cable modems. A new command cable service attribute withhold-TLVs was introduced.
Downstream Classification Enhancement with MAC Addresses	12.2(33)SCH	New combinations of downstream classifiers with a destination MAC address are supported in Cisco IOS Release 12.2(33)SCH. For details about this feature, see Downstream Classification Enhancement with MAC Addresses, on page 24.



CHAPTER 3

DOCSIS WFQ Scheduler on the Cisco CMTS Routers

First Published: December 18, 2008 Last Updated: July 11, 2012

Cisco IOS Release 12.2(33)SCB introduces the Data-over-Cable Service Interface Specifications (DOCSIS) Weighted Fair Queuing (WFQ) Scheduler on the Cisco uBR10012 Universal Broadband Router. The DOCSIS WFQ Scheduler is an output packet scheduler that provides output scheduling services on both WAN uplink interfaces and DOCSIS downstream interfaces.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see 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 document.

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

Contents

Prerequisites for DOCSIS WFQ Scheduler

Table below shows the Cisco Cable Modem Termination System (CMTS) hardware compatibility prerequisites for this feature.

Table 10: DOCSIS 3.0 WFQ Scheduler QoS Support Hardware Compatibility Matrix

CMTS Platform	Processor Engine	Cable Interface Cards	SIP/SPA
Cisco uBR10012 Universal Broadband Router	**Cisco IOS Release 12.2(33)SCB and later releases** • PRE2 • PRE4 **Cisco IOS Release 12.2(33)SCH and later releases** • PRE5	**Cisco IOS Release 12.2(33)SCB and later releases** • Cisco uBR10-MC5X20S/U/H **Cisco IOS Release 12.2(33)SCC and later releases** • Cisco UBR-MC20X20V[4] Cisco IOS Release 12.2(33)SCE and later releases • Cisco uBR-MC3GX60V[5]	**Cisco IOS Release 12.2(33)SCB and later releases** • Cisco Wideband SIP and Cisco Wideband SPA • Cisco 10000 Series SIP-600 and Cisco Wideband SPA or Cisco 5-Port Gigabit Ethernet SPA or Cisco 1-Port 10-Gigabit Ethernet SPA **Cisco IOS Release 12.2(33)SCH and later releases** • Cisco Next Generation Wideband SPA
Cisco uBR7246VXR Universal Broadband Router	**Cisco IOS Release 12.2(33)SCD and later releases** • NPE-G2	**Cisco IOS Release 12.2(33)SCD and later releases** • Cisco uBR-MC88V[6]	–
Cisco uBR7225VXR Universal Broadband Router	**Cisco IOS Release 12.2(33)SCD and later releases** • NPE-G2	**Cisco IOS Release 12.2(33)SCD and later releases** • Cisco uBR-MC88V[7]	–

4 The Cisco UBR-MC20X20V cable interface line card has three variants: Cisco UBR-MC20X20V-0D, Cisco UBR-MC20X20V-5D, and Cisco UBR-MC20X20V-20D. The Cisco UBR-MC20X20V-0D line card supports 20 upstreams and 0 (no) downstreams. The Cisco UBR-MC20X20V-5D line card supports 20 upstreams and 5 downstreams, and the Cisco UBR-MC20X20V-20D line card supports 20 upstreams and 20 downstreams.

5 Cisco uBR3GX60V cable interface line card is not compatible with PRE2.

6 The Cisco uBR-MC88V cable interface line card is not compatible with NPE-G1. You must use NPE-G2 with the Cisco uBR-MC88V cable interface line card.

7 The Cisco uBR-MC88V cable interface line card is not compatible with NPE-G1. You must use NPE-G2 with the Cisco uBR-MC88V cable interface line card.

Note SPA interface processors (SIPs) and shared port adapters (SPAs) are required to only use DOCSIS 3.0 downstream channel bonding. Similarly, the Dynamic Bandwidth Sharing (DBS) feature is only applicable with DOCSIS 3.0 downstream channel bonding and is not a prerequisite for using the WFQ scheduler.

Restrictions for DOCSIS WFQ Scheduler

- The DBS feature is only applicable to DOCSIS 3.0 downstream channel bonding.

Information About DOCSIS WFQ Scheduler

The DOCSIS WFQ scheduling engine is used to provide output packet scheduling services, including absolute priority queueing, weighted fair queueing, minimum rate guarantee, traffic shaping, and DOCSIS bonding group dynamic bandwidth sharing on the Cisco uBR10012 universal broadband router. It replaces the existing Versatile Traffic Management System (VTMS) scheduler.

The DOCSIS WFQ Scheduler provides services on both WAN uplink interfaces and DOCSIS downstream interfaces. The scheduling parameters on WAN uplink interfaces are configured through the Modular QoS CLI (MQC). On cable downstream interfaces, queues are created for DOCSIS service flows with parameters configured by DOCSIS downstream QoS type, length, values (TLVs).

Starting with Cisco IOS Release 12.2(33)SCG, the default queue size for the DOCSIS service flows (with bandwidth greater than 150 Mbps) is increased from 255 to higher values based on the bandwidth on the cable downstream interfaces (see Table below). Additionally, the queue limit for all service flows can also be adjusted using the **cable queue-limit** command. For more information, see the Cisco IOS CMTS Cable Command Reference .

Note The default queue size change, and the **cable queue-limit** command do not affect the DOCSIS high priority queues.

Table below is an example of the queue size based on Annex B 256 QAM channels.

Table 11: Bandwidth, Queue Sizes, and Queue Limits

Channel	Bandwidth (Mbps)	Default Queue Size	Queue Size				
			1 ms	20 ms	30 ms	40 ms	200 ms
1	37.5	63	63	63	92	123	617
2	75	255	63	123	185	247	1235
3	112.5	255	63	185	277	370	1852
4	150	255	63	247	370	494	2470
5	187.5	319	63	308	463	617	3087
6	225	383	63	370	555	741	3705
7	262.5	447	63	432	648	864	4323
8	300	511	63	494	741	988	4940

Channel	Bandwidth (Mbps)	Default Queue Size	Queue Size				
			1 ms	20 ms	30 ms	40 ms	200 ms
12	450	767	63	741	1111	1482	7411
14	525	895	63	864	1296	1729	8646
16	600	1023	63	988	1482	1976	9881

For DOCSIS downstream interfaces, the DOCSIS WFQ Scheduler implements traffic shaping and physical link scheduling at two separate layers, which allows it to account for traffic overhead differently. This allows the scheduler to schedule accurately at the physical layer while conforming to DOCSIS specifications.

The DOCSIS WFQ Scheduler also allows significant enhancement to the queue scaling limits compared to the VTMS scheduler.

Table below shows the queue scaling number comparisons.

Table 12: Queue Scaling Limits

Queue Criteria	PRE4	PRE2	PRE2, Cisco IOS Release 12.2(33)SCA or earlier	NPE-G2/MC88V
Total Number of Queues Per System[8]	384,000	384,000	65,534	64,000
Total Number of CIR Queues	120,000	120,000	65,534	64,000
Number of Queues Per GE Link	16[9]	16	32[10]	N/A
Maximum Number of Packets in PXF	Small 1,703,936 Large 245,760	Small 52,428 Large 32,768	Small 52,428 Large 32,768	Small 150,000 Large 50,000
Queue Size on WAN Uplink	16,00-32,00	16,00-32,00	32,000-16,000	N/A
Queue Size on DOCSIS Downstream[11]	255	255	64	128

8 Includes network-control and default queues.

9 14 user-configurable queues, 1 class-default queue, and 1 system queue.

10 30 user-configurable queues, 1 class-default queue, and 1 system queue.

11 Starting Cisco IOS Release 12.2(33)SCG, the Queue Size on the PRE4 and PRE2 modules varies from 255 to 1023 with bandwidth 150 Mbps to 600 Mbps. See Table 2 .

The following sections explain the DOCSIS WFQ Scheduler features:

Queue Types

The DOCSIS WFQ Scheduler feature supports the following types of queues:

- Priority queues
- CIR queues
- Best Effort queues

Priority Queues

Priority queues are serviced with absolute priority over all the other queues. On DOCSIS downstream interfaces, the priority queues are configured by DOCSIS applications that request a priority service flow, for example, a packet cable voice service flow. On WAN uplink interfaces, the priority queues are configured by the MQC policy maps.

The following restrictions apply to priority queues:

- Only one priority queue is allowed per WAN uplink interface.
- Only one priority queue is allowed for low latency service flows created for each DOCSIS downstream interface.

CIR Queues

A CIR queue is guaranteed to be serviced with at least the Committed Information Rate (CIR). CIR queues are used to service DOCSIS service flows with non-zero minimum reserved rates. If the offered load to a CIR queue exceeds its CIR value, the excess traffic is serviced as best effort traffic.

The following conditions apply to CIR queues:

- CIR queues are supported only on DOCSIS downstream interfaces. They are not supported on WAN uplink interfaces.
- Each DOCSIS flow with a non-zero minimum reserved rate uses its own CIR queue.

Best Effort Queues

The Best Effort (BE) queues share the interface bandwidth not used by the priority queue and the CIR queues. The sharing is in proportion to each queue's quantum value.

The following conditions apply to BE queues:

- On DOCSIS downstream interfaces, BE queues are created by DOCSIS service flows that do not request a minimum reserved rate.
- Each DOCSIS flow without a minimum reserved rate uses its own BE queue.

DOCSIS QoS Support

DOCSIS defines a set of quality of service (QoS) parameters, including traffic priority, maximum sustained traffic rate, minimum reserved traffic rate, maximum traffic burst, maximum downstream latency, and peak traffic rate.

The downstream service flows use the QoS parameters to specify the desired QoS. The downstream policer and scheduler provides services such as traffic shaping, bandwidth provisioning, traffic prioritization, and bandwidth guarantee.

The DOCSIS service flow parameters are mapped to the packet queue parameters and provided with appropriate QoS support for the packet queues to support the DOCSIS parameters

The following DOCSIS QoS parameters are supported:

- Traffic priority
- Maximum sustained traffic rate
- Minimum reserved traffic rate

Note The maximum traffic burst size and the peak traffic rate are supported as described in the http://www.cisco.com/c/en/us/td/docs/cable/cbr/configuration/guide/b_cmts_quality_of_services/docsis_wfq_scheduler.html#con_1085732.

Traffic Priority

The downstream channel bandwidth available to the best effort traffic, namely the channel bandwidth minus the amount consumed by the priority traffic and the CIR traffic, is allocated to the best effort service flows in proportion to their DOCSIS traffic priorities. For example, if there are three service flows sending packets at a particular moment over the same downstream channel, and their DOCSIS traffic priorities are 0, 1 and 3, respectively, their share of the channel bandwidth will be 1:2:4. To achieve this bandwidth allocation, each service flow is assigned a value known as its excess ratio which is derived from its DOCSIS priority. Table below shows the default mappings of DOCSIS priority to excess ratio.

Note When traffic priority for a flow is not explicitly specified, a default priority value of 0 is used as per the DOCSIS specification.

Table 13: DOCSIS Priority to Excess Ratio Mapping

DOCSIS Traffic Priority	Excess Ratio
0	4
1	8
2	12

DOCSIS Traffic Priority	Excess Ratio
3	16
4	20
5	24
6	28
7	32

Custom DOCSIS Priority to Excess Ratio Mappings

Cisco IOS Release 12.2(33)SCC introduces the option to configure custom priority to excess ratio mappings for downstream service flows that override the default mappings listed in the above Table.

Note The configured values are used only for new service flows that are created after the configuration has been applied. All the existing service flows maintain their previous excess ratio values.

The option to configure priority to excess ratio mappings is available on a per downstream forwarding interface basis and is applicable to legacy cable, wideband and modular cable, and integrated cable interfaces.

Note Modular cable interfaces are not supported on Cisco uBR7200 series routers.

The cable downstream qos wfq weights command is used to configure the mappings. For more details on this command, refer to Cisco IOS CMTS Cable Command Reference Guide .

Maximum Sustained Traffic Rate

The maximum sustained traffic rate (MSR) specifies the peak information rate of a service flow. The MSR of a service flow is mapped to the shape rate of the packet queue. When the maximum sustained traffic rate is not specified or set to zero, its traffic rate becomes limited only by the physical channel capacity set by DOCSIS specifications.

Minimum Reserved Traffic Rate

The minimum reserved traffic rate (MRR) specifies the minimum rate reserved for a service flow. The MRR of a service flow is mapped to the CIR of the packet queue, which ensures the minimum amount of bandwidth a queue gets under congestion. When the MRR is not specified, the CIR is set to zero as per DOCSIS specifications.

High Priority Traffic

High priority traffic flows are mapped to a Low Latency Queue (LLQ) on the data forwarding interface. The packets in LLQ are serviced with absolute priority over other queues on the same interface.

The following service flows require high priority service:

- Service flows with DOCSIS downstream latency TLV set to a value above zero. For example, PacketCable Multimedia Specification (PCMM) voice calls.
- PacketCable downstream service flows.
- Service flows with Unsolicited Grant Service (UGS) type—non-PacketCable voice calls—upstream flows.

Enhanced Rate Bandwidth Allocation

The DOCSIS WFQ Scheduler supports the Enhanced Rate Bandwidth Allocation (ERBA) feature for service flows. The ERBA feature allows cable modems (CMs) to burst their temporary transmission rates up to the full line rate for short durations of time. This capability provides higher bandwidth for instantaneous bandwidth requests without having to make changes to existing service levels in the QoS profile.

The DOCSIS WFQ Scheduler allows each service flow to have one dedicated queue. When ERBA is enabled for the service flow, the peak rate is implemented as the queue shape rate within the scheduler, while the maximum sustained rate is set as the token bucket refill rate. The ERBA feature restricts the transmission rate to a value which is the lowest between the maximum sustained rate value and the peak rate value. When ERBA is turned off, the burst size and the peak rate value are not used.

The maximum traffic burst parameter is used to control a service flow burst duration, to burst up to the channel line rate or a configured peak rate, when it is within its maximum burst size allowance. On the Cisco uBR10012 Universal Broadband Router, the **cable ds-max-burst** command is used to control this behavior explicitly.

Note To enable ERBA, the **cable ds-max-burst burst-threshold** value must be less than or equal to **max-burst** value in the cable modem's configuration file.

For more details on this behavior and the CLI, refer to Cisco IOS CMTS Cable Command Reference Guide .

Note The ERBA feature is not applicable for high priority service flows and multicast service flows.

Table below summarizes the ERBA support for the Cisco uBR10012 router.

Table 14: Enhanced Rate Bandwidth Allocation Support for the Cisco uBR10012 Router

	Policer Rate	Policer Exceed Action	Policer Token Bucket Size	Queue Shape Rate
Traditional Service Flow	Maximum Sustained Traffic Rate (unused)	Transmit	A value computed internally by CMTS (unused)	Maximum Sustained Traffic Rate
ERBA-Enabled Service Flow	Maximum Sustained Traffic Rate	Drop	Maximum Traffic Burst TLV	Peak Traffic Rate

In Cisco uBR7246VXR and Cisco uBR7225VXR routers, the dual token bucket-based shaper is used to support ERBA on the Cisco uBR-MC88V line card (the ERBA feature is always enabled on the Cisco uBR-MC88V line card). The dual token bucket shaper has two independent token buckets for each service flow. The maximum rate of one bucket is configured to MSR and the maximum tokens are set to maximum traffic burst. The other bucket is configured with the refilling rate of the *peak-rate* and the maximum tokens are set to the default level, of 4 milliseconds. Packets are shaped if any of the two buckets are exhausted.

Table below summarizes the ERBA dual token bucket configuration for the Cisco uBR7246VXR and Cisco uBR7225VXR routers.

Table 15: ERBA Dual Token Bucket Configuration

	Token Bucket Rate (One)	Token Bucket Size (One)	Token Bucket Rate (Two)	Token Bucket Size (Two)
Traditional Service Flow	Maximum Sustained Traffic Rate	4ms * MSR	N/A	N/A
ERBA-enabled Service Flow	Maximum Sustained Traffic Rate	Maximum Traffic Burst or 4ms * MSR	Peak Rate	4ms * Peak Rate

For information about ERBA support on the Cisco CMTS routers, refer to Using Enhanced Bandwidth Rate Allocation (ERBA) Support for DOCSIS 1.0 Cable Modems at the following location: DOCSIS 1.1 for the Cisco CMTS Routers

Peak Traffic Rate

Note The **cable ds-max-burst** command is not supported on the Cisco uBR7246VXR and Cisco uBR7225VXR routers.

The *peak-rate* option of the **cable ds-max-burst** command allows you to specify the peak rate an ERBA-enabled service flow can use. The *peak-rate* value is a global value and is applied to all service flows created after the configuration of the **cable ds-max-burst** command. The default value of the *peak-rate* is zero.

If the DOCSIS 3.0 TLV 25.27 is specified for a service flow, the *peak-rate* value is set as the TLV value. However, if ERBA is not turned on for a service flow, the *peak-rate* value is ignored.

The *peak-rate* value can also be configured through cable service class command which forms part of the service class template. During modem registration or Dynamic Service Addition (DSA) operation, the service class name TLV 25.4 is sent to create the static or dynamic downstream service flow that matches the service class template. These downstream service flows are created with a specific *peak-rate* . If the *peak-rate* is not specified in he cable modem's configuration file, then the peak rate specified by the **cable ds-max-burst burst-threshold** *threshold* **peak-rate** *peak rate* command is used.

Note The option to specify peak rate in the **cable ds-max-burst** command is not available on the Cisco cBR Series Converged Broadband routers.

If a service flow has both service class and TLV 25.27 defined *peak-rate* , then the *peak-rate* value specified in the TLV is used.

Some of the DOCSIS 1.x and DOCSIS 2.0 cable modems, which are not fully DOCSIS 1.x or DOCSIS 2.0 compliant, may fail to come online when they receive TLV 25.27 from the Cisco CMTS during registration. In order to overcome this you can configure the **cable service attribute withhold-TLVs command with the peak-rate** keyword to restrict sending of this TLV to non-DOCSIS 3.0 cable modems.

For more details on the cable service class and **cable service attribute withhold-TLVs** commands, see Cisco IOS CMTS Cable Command Reference Guide .

DOCSIS 3.0 Downstream Bonding Support with Bonding Group Dynamic Bandwidth Sharing

DOCSIS 3.0 introduces the concept of downstream channel bonding. Each Bonding Group (BG) is made up of a collection of downstream channels, which can be used by one or more bonding groups. Each downstream channel can also serve as a primary channel in a MAC domain and carry non-bonded traffic, while being part of a BG.

Prior to DOCSIS 3.0 standards, the downstream service flows were associated with a single downstream interface, which in turn corresponded to a physical downstream on an RF channel. In DOCSIS 3.0, the downstream service flows are associated with the downstream bonding groups. These bonding groups can use multiple downstream RF channels.

On the Cisco uBR10012 universal broadband router, the DOCSIS 3.0 downstream channel bonding is supported on the SPA RF channels. To efficiently utilize the underlying RF channel bandwidth and to provide QoS to the downstream service flows, dynamic bandwidth sharing (DBS) is supported on the interfaces using SPA RF channels.

DBS is the dynamic allocation of bandwidth for wideband (WB), integrated cable (IC), and modular-cable (MC) interfaces sharing the same downstream channel. Due to the channel sharing nature of the bonding groups, the bandwidth available to bonding groups or non-bonded channels is not fixed. The bandwidth depends on the configuration and the traffic load on the WB, IC, or MC.

Note Bonding groups are implemented as WB interfaces and non-bonded channels as MC interfaces.

In the DBS mode, the bandwidth of the shared RF channels is dynamically allocated among the WB, IC, and MC interfaces. The DBS enables efficient use of the underlying RF channel bandwidth even in the presence of high burst traffic. The DBS is configured at the WB, IC, or MC interface level. By default, bandwidth for a WB, IC, or MC channel is statically allocated (non-DBS).

DBS does not prevent static bandwidth configuration. If a static portion of the bandwidth is configured on any RF channel that one or more DBS-enabled channel utilizes, that portion is subtracted from the RF channel bandwidth. This portion of bandwidth is dedicated to the non-DBS interface and becomes unavailable to the DBS WB, IC, or MC interfaces.

For information about DBS support on the Cisco CMTS routers, refer to the Dynamic Bandwidth Sharing on the Cisco CMTS Router feature.

How to Configure DOCSIS WFQ Scheduler

You cannot configure the DOCSIS WFQ Scheduler feature as it is automatically loaded into the Parallel Express Forwarding (PXF) engine. The parameters that the schedule uses include the interface bandwidth and queue parameters.

This section describes the following required and optional procedures:

Mapping DOCSIS Priority to Excess Ratio

This section describes how to map DOCSIS priorities to custom excess ratios for downstream service flows. These custom mappings will override the default mappings.

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	**interface cable** {*slot*/*port*|*slot*/*subslot*/*port* } **Example:** `Router(config)# interface cable 3/0/0`	Enters interface configuration mode for the indicated cable downstream interface. • On the Cisco uBR7246VXR router, the valid values are: ◦ *slot*—3 to 6 ◦ *port*—0 or 1 (depending on the cable interface) • On the Cisco uBR7225VXR router, the valid values are: ◦ *slot*—1 and 2 ◦ *port*—0 or 1 (depending on the cable interface) • On the Cisco uBR10012 router, the valid values are:

	Command or Action	Purpose
		◦ *slot* —5 to 8 ◦ *subslot* —0 or 1 ◦ *port*—0 to 4 (depending on the cable interface)
Step 4	**cable downstream qos wfq weigthts {weight1...weight8}** **Example:** `Router(config-if)# cable downstream qos wfq weights 10 20 30 40 50 60 70 80`	Configures the custom excess ratios for 8 priorities: • *weight1...weight8* —Custom weight. Valid values range from 1 to 100. **Note** The custom values are used only for new service flows and not existing ones.
Step 5	**end** **Example:** `Router(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Verifying the Service Flows and Queues

Cisco uBR10012 Router

To verify the downstream (DS) service flows and parameters for a modem, use the **show cable modem** [**mac-address** |**ip-address**]**qos** command on the Cisco uBR10012 router as shown in the following example:

```
Router# show cable modem 0018.f826.3453 qos
Sfid  Dir Curr  Sid   Sched  Prio MaxSusRate  MaxBrst   MinRsvRate  Throughput
          State       Type
7     US  act   1     BE     7    0           3044      0           0
8     DS  act   N/A   BE     7    0           2000000   100000      7429769
29    DS  act   N/A   BE     0    0           3044      0           0
```

To verify the detailed service flow configuration, use the **show interfaces cable-interface service-flow sfid qos** command on the Cisco uBR10012 router as shown in the following example:

```
Router# show interfaces c7/0/0 service-flow 8 qos
Sfid  Dir Curr  Sid   Sched  Prio MaxSusRate  MaxBrst   MinRsvRate  Throughput
          State       Type
8     DS  act   N/A   BE     7    0           2000000   100000      7430397
```

To verify the detailed service flow statistics, use the **show interfaces cable-interface service-flow sfid counters** command on the Cisco uBR10012 router as shown in the following example:

```
Router# show interfaces c7/0/0 service-flow 8 counters
Sfid  Packets             Bytes               PacketDrop Bits/Sec   Packet/Sec
8     100913              121095600           374337     7431599    773
```

To verify the service flow ID to queue ID (queue index) association, use the **show cr10k-rp cable-interface sfid queue** command on the Cisco uBR10012 router as shown in the following example:

```
Router# show cr10k-rp mod 1/2/0:0 queue
Docsis queues on the interface: 0
Total DOCSIS Queues Allocated: 45
Available/Maximal reservable rate(kbps): 3750/3750

HQF BLT Info (LBLT Group 36):
LBLT 36: wt/qntm 1/10000; PBLT 1236: BW 3750Kbps, flowbit prd/ofst 512/0, rsrc/flrsrc 3/3

BE Queues:

CIR Queues:

LL Queues:
```

To verify the service flow queue information, use the **show pxf cpu queue interface-name** command on the Cisco uBR10012 router as shown in the following example:

```
Router# show pxf cpu queue modular-cable 1/2/0:0
Cable Interface Queues:
QID     Len/Max  Dequeues   TailDrops   MinRt  Wt/Quantum  ShapeRt FlowId
                                        (Kbps)             (Kbps)
131147    0/255  190        0           0         1/240    0       58
131148    0/255  33820      0           0         1/10000  0       32824
Cable Service Flow Queues:
* Best Effort Queues
QID     Len/Max  Dequeues   TailDrops   MinRt  Wt/Quantum  ShapeRt FlowId
                                        (Kbps)             (Kbps)
131241    0/255  0          0           0         1/240    0       32881
* CIR Queues
QID     Len/Max  Dequeues   TailDrops   MinRt  Wt/Quantum  ShapeRt FlowId
                                        (Kbps)             (Kbps)
2049    254/255  131018     485751      99        1/1920   0       32880
* Low Latency Queues
QID     Len/Max  Dequeues   TailDrops
```

Cisco uBR7246VXR and Cisco uBR7225VXR Routers

To verify the downstream hierarchical queueing framework (HQF) queue information for a modem, use the **show cable modem [mac-address | ip-address] queue** command on the Cisco uBR7246VXR and Cisco uBR7225VXR routers as shown in the following example:

```
Router# show cable modem 41.3.190.2 queue
* idx/gqid Len/Limit Deqs      Drops     CIR       MIR/PR     ForwInt  SFID
            pkts    pkts      pkts      kbps       kbps
BE Queues:
    3/43     0/128   103       0         0           0/0      In5/1:1 Ca5/1:22
CIR Queues:
Low Latency Queues:
```

To verify the downstream HQF queue information for the interface, use the **show interfaces cable-interface service-flow sfid queue** command on the Cisco uBR7246VXR and Cisco uBR7225VXR routers as shown in the following example:

```
Router# show interfaces c3/0 service-flow 8 queue
*   idx/gqid   Len/Limit Deqs      Drops    CIR         MIR/PR
                 pkts    pkts      pkts     kbps         kbps
      0/53       0/128   0         0        100       15000/0
 I: Cable Interface Queue
 $: Low Latency Queue
 ~: Low Latency Policing Queue
```

To verify the detailed downstream HQF information for all queues under this interface, use the **show interfaces cable-interface service-flow sfid queue verbose** command on the Cisco uBR7246VXR and Cisco uBR7225VXR routers as shown in the following example:

```
Router# show interfaces c3/0 service-flow 8 queue verbose
   blt (0x19FA93C0, index 6, qid 53, fast_if_number 20) layer CLASS_HIER0
   scheduling policy: FIFO (110)
   classification policy: NONE (120)
   drop policy: TAIL (141)
   packet size fixup policy: NONE (0)   no of global policers: 0
   D/Traffic Shaping enabled
   blt flags: 0x22A208C    scheduler: 0x1A015D80
   total guarantee percent 0 total remaining perc 0 total bandwidth guarantee 9500 total
active 1
   D/Traffic Shaping enabled
   txcount 0 txqbytes 0 drops 0 qdrops 0 nobuffers 0 flowdrops 0
   qsize 0 aggregate limit/bytes 128/375000 availbuffers 128
   holdqueue_out 0 perc 0.00 remaining_ratio/perc 20
   visible_bw 100 max_rate 15000 allocated_bw 100 vc_encap 0 ecn_threshold NONE
   weight A 1 quantum A 1500 credit A 1500
   weight B 1 quantum B 1500 credit B 1500
   min-rate tokens: 1500, credit: 0, depth: 1500
   backpressure_policy 0 scheduler_flags C03F
   last_sortq[A/B] 0/0, remaining pak/particles 0/0
   leaf_blt[P1] 0x1A015D80 burst packets/bytes[P1] 0/0
   leaf_blt[P2] 0x1A015D80 burst packets/bytes[P2] 0/0
   leaf_blt[NOTP] 0x1A015D80 burst packets/bytes[NOTP] 0/0

   OUTPUT Shaping
     Bc internal 0 Be internal 0 Time interval 4
     increment 15000 increment_lower 0 increment_limit 15000
     last visit 0 credit 0 outstanding_tokens 0 maxtokens 32000000
     system timer delayed 0 restart timer 0
     timer set 0 hqf_shape_running 562
     nextexpire_system_time 0 nextexpire_time_qindex -1
```

Verifying the DOCSIS Priority to Excess Ratio Mapping

Cisco uBR10012 Router

To verify the DOCSIS priority to excess ratio mapping configuration on the Cisco uBR10012 router, use the **show running-config interface** command as shown in the following example:

```
Router# show running-config interface cable 8/0/0 | i qos
cable downstream qos wfq weights 10 20 30 40 50 60 70 80
```

To verify the excess ratio for each queue on an interface, use the show cr10k-rp interface queue be command on the Cisco uBR10012 router as shown in the following example:

```
Router# show cr10k cable8/1/0 queue be
Forwarding Interface: Cable8/1/0
Docsis queues on the interface: 8
Total DOCSIS Queues Allocated: 25
Available/Maximal reservable rate(kbps): 25232/26000
HQF BLT Info (LBLT Group 86):
LBLT 110: wt/qntm 1/10000; PBLT 1286: BW 26000Kbps, flowbit prd/ofst 32/3, rsrc/flrsrc 17/17

BE Queues:
Queue Index: 131268, GlobalQID 83, CBLT ID 131268
       MinRate(Kbps) 0, ExcessRatio 4, ShapeRate(bps) 10000000, QLimit 255 Service Flow(s):
 rp_sf_index 32880, lc_sfid 3, min_rate(bps) 0, max_rate(bps) 10000000 peak_rate(bps) 0
Queue Index: 131376, GlobalQID 81, CBLT ID 131376
        MinRate(Kbps) 0, ExcessRatio 32, ShapeRate(bps) 0, QLimit 255 Service Flow(s):
rp_sf_index 33115, lc_sfid 39, min_rate(bps) 0, max_rate(bps) 0 peak_rate(bps) 0
Queue Index: 131377, GlobalQID 82, CBLT ID 131377
```

```
       MinRate(Kbps) 0, ExcessRatio 24, ShapeRate(bps) 5000000, QLimit 255 Service Flow(s):
 rp_sf_index 33116, lc_sfid 40, min_rate(bps) 0, max_rate(bps) 5000000 peak_rate(bps) 0
Queue Index: 131378, GlobalQID 85, CBLT ID 131378
        MinRate(Kbps) 0, ExcessRatio 32, ShapeRate(bps) 0, QLimit 255 Service Flow(s):
rp_sf_index 33120, lc_sfid 35, min_rate(bps) 0, max_rate(bps) 0 peak_rate(bps) 0
Queue Index: 131379, GlobalQID 88, CBLT ID 131379
       MinRate(Kbps) 0, ExcessRatio 24, ShapeRate(bps) 5000000, QLimit 255 Service Flow(s):
 rp_sf_index 33121, lc_sfid 43, min_rate(bps) 0, max_rate(bps) 5000000 peak_rate(bps) 0
Queue Index: 131398, GlobalQID 109, CBLT ID 131398
        MinRate(Kbps) 0, ExcessRatio 32, ShapeRate(bps) 0, QLimit 255 Service Flow(s):
rp_sf_index 33170, lc_sfid 37, min_rate(bps) 0, max_rate(bps) 0 peak_rate(bps) 0
Queue Index: 131399, GlobalQID 110, CBLT ID 131399
       MinRate(Kbps) 0, ExcessRatio 24, ShapeRate(bps) 5000000, QLimit 255 Service Flow(s):
 rp_sf_index 33171, lc_sfid 51, min_rate(bps) 0, max_rate(bps) 5000000 peak_rate(bps) 0
```

Cisco uBR7246VXR and Cisco uBR7225VXR Routers

To verify the DOCSIS priority to excess ratio mapping configuration on the Cisco uBR7246VXR and Cisco uBR7225VXR routers, use the **show interfaces cable-interface service-flow sfid queue verbose** command as shown in the following example:

```
Router# show interfaces c3/0 service-flow 8 queue verbose
   blt (0x19FA93C0, index 6, qid 53, fast_if_number 20) layer CLASS_HIER0
   scheduling policy: FIFO (110)
   classification policy: NONE (120)
   drop policy: TAIL (141)
   packet size fixup policy: NONE (0)   no of global policers: 0
   D/Traffic Shaping enabled
   blt flags: 0x22A208C    scheduler: 0x1A015D80
   total guarantee percent 0 total remaining perc 0 total bandwidth guarantee 9500 total
active 1
   D/Traffic Shaping enabled
   txcount 0 txqbytes 0 drops 0 qdrops 0 nobuffers 0 flowdrops 0
   qsize 0 aggregate limit/bytes 128/375000 availbuffers 128
   holdqueue_out 0 perc 0.00 remaining_ratio/perc 20
   visible_bw 100 max_rate 15000 allocated_bw 100 vc_encap 0 ecn_threshold NONE
   weight A 1 quantum A 1500 credit A 1500
   weight B 1 quantum B 1500 credit B 1500
   min-rate tokens: 1500, credit: 0, depth: 1500
   backpressure_policy 0 scheduler_flags C03F
   last_sortq[A/B] 0/0, remaining pak/particles 0/0
   leaf_blt[P1] 0x1A015D80 burst packets/bytes[P1] 0/0
   leaf_blt[P2] 0x1A015D80 burst packets/bytes[P2] 0/0
   leaf_blt[NOTP] 0x1A015D80 burst packets/bytes[NOTP] 0/0

   OUTPUT Shaping
     Bc internal 0 Be internal 0 Time interval 4
     increment 15000 increment_lower 0 increment_limit 15000
     last visit 0 credit 0 outstanding_tokens 0 maxtokens 32000000
     system timer delayed 0 restart timer 0
     timer set 0 hqf_shape_running 562
     nextexpire_system_time 0 nextexpire_time_qindex -1
```

Verifying the HQF Queue Detail Information

Cisco uBR7246VXR and Cisco uBR7225VXR Routers

To verify the downstream HQF queue information for all the queues under an interface, use the **show interfaces {integrated-cable | wideband-cable} slot/port: sub-interface queue** command on the Cisco uBR7246VXR and Cisco uBR7225VXR routers as shown in the following example:

```
Router# show interfaces integrated-cable 3/0:0 queue
* idx/gqid Len/Limit Deqs      Drops     CIR       MIR/PR     SFID
             pkts    pkts      pkts      kbps       kbps
```

```
BE Queues:
I   0/1      0/128   0         0         0           0/0          -
    1/42     0/128   16        0         0           0/0      Ca4/0:116
    2/44     0/128   4         0         0        1000/0      Ca4/0:3890
CIR Queues:
Low Latency Queues:
 I: Cable Interface Queue
 $: Low Latency Queue
```

To verify the detailed downstream HQF queue information for all the queues under an interface, use the **show interfaces {integrated-cable | wideband-cable} slot/port: sub-interface queue [verbose]** command on the Cisco uBR7246VXR and Cisco uBR7225VXR routers as shown in the following example:

```
Router# show interfaces integrated-cable 4/0:0 queue verbose
   blt (0x20265E60, index 0, qid 0, fast_if_number 20) layer PHYSICAL
   scheduling policy: WFQ (111)
   classification policy: CLASS_BASED (122)
   drop policy: TAIL (141)
   packet size fixup policy: NONE (0)   no of global policers: 0
   D/Traffic Shaping enabled
   blt flags: 0x222000    scheduler: 0x202D2D80
   total guarantee percent 0 total remaining perc 0 total bandwidth guarantee 0
total active 0
   D/Traffic Shaping enabled
   txcount 13 txqbytes 746 drops 0 qdrops 0 nobuffers 0 flowdrops 0
   qsize 0 aggregate limit/bytes 8000/0 availbuffers 8000
   holdqueue_out 1000 perc 0.00 remaining_ratio/perc 0
   visible_bw 2600 max_rate 2600 allocated_bw 2080 vc_encap 0 ecn_threshold NONE
   weight A 1 quantum A 1500 credit A 0
   weight B 1 quantum B 1500 credit B 0
   min-rate tokens: 13000, credit: 0, depth: 13000
   backpressure_policy 1 scheduler_flags C03F
   last_sortq[A/B] 0/0, remaining pak/particles 0/0
   leaf_blt[P1] 0x202D2D80 burst packets/bytes[P1] 0/0
   leaf_blt[P2] 0x202D2D80 burst packets/bytes[P2] 0/0
   leaf_blt[NOTP] 0x202D2D80 burst packets/bytes[NOTP] 0/0
   OUTPUT Shaping
     Bc internal 0 Be internal 0 Time interval 4
     increment 2600 increment_lower 0 increment_limit 2600
     last visit 145532 credit 0 outstanding_tokens 20192 maxtokens 20800
     system timer delayed 0 restart timer 0
     timer set 0 hqf_shape_running 21
     nextexpire_system_time 0 nextexpire_time_qindex -1
   next layer HQFLAYER_CLASS (max entries 2000)
BE Queues:
    blt (0x20265DA0, index 0, qid 1, fast_if_number 20) layer CLASS_HIER0
    scheduling policy: FIFO (110)
    classification policy: NONE (120)
    drop policy: TAIL (141)
    packet size fixup policy: NONE (0)   no of global policers: 0
    blt flags: 0x220000    scheduler: 0x202D2CC0
    total guarantee percent 0 total remaining perc 0 total bandwidth guarantee 0
 total active 1
    txcount 13 txqbytes 746 drops 0 qdrops 0 nobuffers 0 flowdrops 0
    qsize 0 aggregate limit/bytes 128/0 availbuffers 128
    holdqueue_out 0 perc 0.00 remaining_ratio/perc 0
    visible_bw 0 max_rate 26000 allocated_bw 26000 vc_encap 0 ecn_threshold NONE
    weight A 1 quantum A 1600 credit A 0
    weight B 1 quantum B 1600 credit B 46
    min-rate tokens: 13000, credit: 0, depth: 13000
    backpressure_policy 0 scheduler_flags C03F
    last_sortq[A/B] 0/0, remaining pak/particles 0/0
    leaf_blt[P1] 0x202D2CC0 burst packets/bytes[P1] 0/0
    leaf_blt[P2] 0x202D2CC0 burst packets/bytes[P2] 0/0
    leaf_blt[NOTP] 0x202D2CC0 burst packets/bytes[NOTP] 1/46
CIR Queues:
Low Latency Queues:
```

To verify the normal downstream HQF queue information for all the class layer bandwidth limited traffic (CBLT) queues under an interface, use the **show interfaces {integrated-cable | wideband-cable} slot/port:**

sub-interface queue cblt [index | priority] command on the Cisco uBR7246VXR and Cisco uBR7225VXR routers as shown in the following example:

```
Router# show interfaces integrated-cable 3/0:0 queue cblt 1
    blt (0x65CE3EA0, index 1, qid 45, fast_if_number 19) layer CLASS_HIER0
    scheduling policy: FIFO (110)
    classification policy: NONE (120)
    drop policy: TAIL (141)
    packet size fixup policy: NONE (0)   no of global policers: 0
    D/Traffic Shaping enabled
    blt flags: 0x22A208C    scheduler: 0x65D504C0
    total guarantee percent 0 total remaining perc 0 total bandwidth guarantee 1000 total
active 1
    D/Traffic Shaping enabled
    txcount 890 txqbytes 63900 drops 0 qdrops 0 nobuffers 0 flowdrops 0
    qsize 0 aggregate limit/bytes 128/100000 availbuffers 128
    holdqueue_out 0 perc 0.00 remaining_ratio/perc 11
    visible_bw 0 max_rate 4000 allocated_bw 0 vc_encap 0 ecn_threshold NONE
    weight A 1 quantum A 1500 credit A 1500
    weight B 1 quantum B 1500 credit B 1500
    min-rate tokens: 1500, credit: 0, depth: 1500
    backpressure_policy 0 scheduler_flags C03F
    last_sortq[A/B] 0/0, remaining pak/particles 0/0
    leaf_blt[P1] 0x65D504C0 burst packets/bytes[P1] 0/0
    leaf_blt[P2] 0x65D504C0 burst packets/bytes[P2] 0/0
    leaf_blt[NOTP] 0x65D504C0 burst packets/bytes[NOTP] 0/0
    OUTPUT Shaping
      Bc internal 0 Be internal 0 Time interval 4
      increment 4000 increment_lower 0 increment_limit 4000
      last visit 87456736 credit 0 outstanding_tokens 23760 maxtokens 24352
      peak_rate_credit 0 peak_rate_tokens 0 peak_rate_increment 0
      system timer delayed 0 restart timer 0
      timer set 0 hqf_shape_running 17254
      nextexpire_system_time 0 nextexpire_time_qindex -1
```

To verify the normal and priority downstream HQF queue information for all the CBLT queues under an interface, use the **show interfaces {integrated-cable | wideband-cable} slot/port: sub-interface queue cblt [index | priority]** command on the Cisco uBR7246VXR and Cisco uBR7225VXR routers as shown in the following example:

```
Router# show interfaces integrated-cable 3/0:0 queue cblt priority
    blt (0x19FA9300, index 0, qid 52, fast_if_number 20) layer CLASS_HIER0
    scheduling policy: FIFO (110)
    classification policy: NONE (120)
    drop policy: TAIL (141)
    packet size fixup policy: NONE (0)   no of global policers: 0
    blt flags: 0x200800    scheduler: 0x1A015CC0
    total guarantee percent 0 total remaining perc 0 total bandwidth guarantee 9500 total
active 1

    txcount 114 txqbytes 12864 drops 0 qdrops 0 nobuffers 0 flowdrops 0
    qsize 0 aggregate limit/bytes 128/0 availbuffers 128
    holdqueue_out 0 perc 0.00 remaining_ratio/perc 0
    visible_bw 0 max_rate 37500 allocated_bw 0 vc_encap 0 ecn_threshold NONE
    weight A 1 quantum A 1500 credit A 1500
    weight B 1 quantum B 1500 credit B 1500
    min-rate tokens: 1500, credit: 0, depth: 1500
    backpressure_policy 0 scheduler_flags C83F
    last_sortq[A/B] 0/0, remaining pak/particles 0/0
    leaf_blt[P1] 0x1A015CC0 burst packets/bytes[P1] 0/0
    leaf_blt[P2] 0x1A015CC0 burst packets/bytes[P2] 0/0
    leaf_blt[NOTP] 0x1A015CC0 burst packets/bytes[NOTP] 0/0
PRIORITY LEVEL 1: total bandwidth 500 kbps, total percent 0%
```

To verify the downstream HQF queue information for all the physical layer bandwidth limited traffic (PBLT) queues under an interface, use the **show interfaces {integrated-cable | wideband-cable} slot/port:**

sub-interface queue pblt command on the Cisco uBR7246VXR and Cisco uBR7225VXR routers as shown in the following example:

```
Router# show interfaces integrated-cable 3/0:0 queue pblt
   blt (0x19FB4700, index 0, qid 0, fast_if_number 20) layer PHYSICAL
   scheduling policy: WFQ (111)
   classification policy: CLASS_BASED (122)
   drop policy: TAIL (141)
   packet size fixup policy: NONE (0)   no of global policers: 0
   blt flags: 0x220000    scheduler: 0x1A0210C0
  total guarantee percent 0 total remaining perc 0 total bandwidth guarantee 0 total active
 0
   txcount 67743 txqbytes 6281007 drops 2 qdrops 0 nobuffers 0 flowdrops 0
   qsize 0 aggregate limit/bytes 8000/0 availbuffers 8000
   holdqueue_out 1000 perc 0.00 remaining_ratio/perc 0
   visible_bw 37500 max_rate 37500 allocated_bw 18000 vc_encap 0 ecn_threshold NONE
   weight A 1 quantum A 1500 credit A 1500
   weight B 1 quantum B 1500 credit B 1500
   min-rate tokens: 13000, credit: 0, depth: 13000
   backpressure_policy 1 scheduler_flags C03F
   last_sortq[A/B] 0/0, remaining pak/particles 0/0
   leaf_blt[P1] 0x1A0210C0 burst packets/bytes[P1] 0/0
   leaf_blt[P2] 0x1A0210C0 burst packets/bytes[P2] 0/0
   leaf_blt[NOTP] 0x1A0210C0 burst packets/bytes[NOTP] 0/0
```

Additional References

The following sections provide references related to the DOCSIS WFQ Scheduler feature.

Related Documents

Related Topic	Document Title
CMTS cable commands	Cisco IOS CMTS Cable Command Reference
Modular Quality of Service	MQC QoS on the Cisco CMTS Routers
Enhanced Bandwidth Rate Allocation	DOCSIS 1.1 for the Cisco CMTS Routers
Dynamic Bandwidth Sharing	Dynamic Bandwidth Sharing on the Cisco CMTS Router

Standards

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

MIBs

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

RFCs

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

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature Information for DOCSIS WFQ Scheduler

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

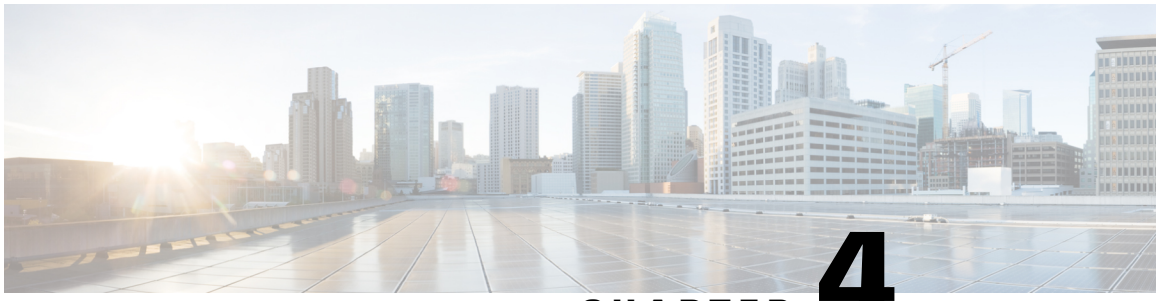
Note The table below lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table below lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Release 12.2(33)SCB or a later releases release appear in the table.

Table 16: Feature Information for DOCSIS WFQ Scheduler

Feature Name	Releases	Feature Information
DOCSIS WFQ Scheduler	12.2(33)SCB	The DOCSIS WFQ Scheduler provides output scheduling services on DOCSIS downstream interfaces. Cisco IOS Release 12.2(33)SCB introduces this feature on the Cisco uBR10012 Universal Broadband Router.
DOCSIS WFQ Scheduler	12.2(33)SCC	Cisco IOS Release 12.2(33)SCC introduces the option to configure user-defined priorities to map DOCSIS priority value to an excess ratio value. Using this feature, you can configure priorities in the downstream direction rather than using the default rates. The following command was introduced: cable downstream qos wfq weights
Enhanced Rate Bandwidth Allocation	12.2(33)SCD	Support was added for the Cisco uBR7246VXR and Cisco uBR7225VXR routers. Dual token bucket based shaper is used to support ERBA on the uBR-MC88V line card for the Cisco uBR7246VXR and Cisco uBR7225VXR routers. The following section provides information about this feature:

Feature Name	Releases	Feature Information
DOCSIS 3.0 Downstream Bonding Support with Bonding Group Dynamic Bandwidth Sharing	12.2(33)SCD	Support was added for the Cisco uBR7246VXR and Cisco uBR7225VXR routers. The following commands were introduced or modified: • **show cable modem** • **show interface cable service-flow** • **show interface integrated-cable** • **show interface wideband-cable queue**
Suppressing Downstream and Upstream Peak Rate TLVs for pre DOCSIS 3.0 Cable Modems	12.2(33)SCB10	Support was added to restrict sending of the DOCSIS 3.0 TLVs to DOCSIS 1.X and DOCSIS 2.0 cable modems. A new command cable service attribute withhold-TLVs was introduced.
Optimization of queue size	12.2(33)SCG	Default queue size for the DOCSIS service flows (with bandwidth greater than 150 Mbps) is increased. A new command **cable queue-limit** was introduced



CHAPTER 4

Dynamic Bandwidth Sharing on the Cisco CMTS Router

First Published: February 25, 2008

Last Updated: November 29, 2010

The Cable Modem Termination System (CMTS) enables dynamic bandwidth sharing (DBS) on modular cable (MC), integrated cable (IC), and wideband (WB) cable interfaces.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see 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 document.

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

Contents

Prerequisites for Dynamic Bandwidth Sharing

Table below shows the hardware compatibility prerequisites for the Dynamic Bandwidth Sharing on the Cisco CMTS Router feature.

Table 17: Cable Hardware Compatibility Matrix for Dynamic Bandwidth Sharing

CMTS Platform	Processor Engine	Cable Interface Line Cards
Cisco uBR10012 Universal Broadband Router	Cisco IOS Release 12.3(23)BC1 and later releases • PRE2 Cisco IOS Release 12.2(33)SCB and later releases • PRE4 Cisco IOS Release 12.2(33)SCH and later releases • PRE5	Cisco IOS Release 12.2(33)SCB and later releases • Cisco uBR10-MC5X20S/U/H Cisco IOS Release 12.2(33)SCC and later releases • Cisco UBR-MC20X20V Cisco IOS Release 12.2(33)SCE and later releases • Cisco uBR-MC3GX60V[12]
Cisco uBR7225VXR Universal Broadband Router	Cisco IOS Release 12.2(33)SCD and later releases • NPE-G2	Cisco IOS Release 12.2(33)SCD and later releases • Cisco uBR-MC88V
Cisco uBR7246VXR Universal Broadband Routers	Cisco IOS Release 12.2(33)SCD and later releases • NPE-G2	Cisco IOS Release 12.2(33)SCD and later releases • Cisco uBR-MC88V

12 Cisco uBR-MC3GX60V cable interface line card is not compatible with PRE2.

Restrictions for Dynamic Bandwidth Sharing

- The bandwidth sharing state of a modular, integrated, or wideband cable interface can be changed only when the interface is administratively shutdown.

Information About Dynamic Bandwidth Sharing

The following sections provide information on DBS:

DBS for Modular, Integrated, and Wideband Cable Interfaces

Prior to DOCSIS 3.0 standards, cable service flows were associated with a single cable interface, which in turn corresponded to a physical downstream on a line card. Under DOCSIS 3.0 standards, cable service flows can be associated with more than one downstream channel.

DBS is the dynamic allocation of bandwidth for MC, IC, and WB cable interfaces sharing the same downstream channel. The bandwidth available to each MC, IC, WB cable, or narrowband channel is not a fixed value—it depends on the configuration and the traffic load on the MC, IC, or WB cable.

The available bandwidth for data traffic is calculated using the following formula: Actual Line Rate – (Bandwidth used by MAC Management Messages [MMM] + Bandwidth loss due to DOCSIS header)

The bandwidth required by MMM depends on the CMTS configuration. The maximum bandwidth reserved for MMM is 4 percent (if the MMM uses less than 4 percent of bandwidth, the remaining unused bandwidth is available for the data traffic).

DBS enables high burst rates with DOCSIS 2.0 cable modems as well as DOCSIS 3.0 cable modems. The DBS feature continues working across line card and performance routing engine (PRE) switchovers with no loss of functionality.

DBS Configuration

Dynamic bandwidth sharing and static bandwidth allocations are configured at the MC, IC, or WB cable interface level. By default, bandwidth for an MC, IC, or WB cable channel is statically allocated. When DBS is enabled on an interface, the static bandwidth percentage is converted to a committed information rate (CIR) value for the corresponding interface. The interface CIR value represents the guaranteed portion of the interface bandwidth and is used for admission control of the service flows with minimum reserved rate. When DBS is enabled, you can also specify the remaining ratio value of the excess bandwidth for the interface. If DBS is enabled and no bandwidth percentage is specified, no bandwidth is reserved for the MC, IC, or WB cable interface and the interface is effectively in protocol down state.

Dynamic bandwidth sharing does not preclude static bandwidth configuration. If a static portion of bandwidth is configured on any RF channel that one or more DBS-enabled channel utilizes, that portion is subtracted from the CIR value of the RF link. Therefore, such a portion is always reserved and is not available to dynamic MC, IC, or WB cable interfaces.

Note Starting with Cisco IOS Release 12.2(33)SCE, the DBS mode is enabled by default, on the WB/MC/IC interfaces. To disable the DBS mode, configure the no cable dynamic-bw-sharing command.

How to Configure Dynamic Bandwidth Sharing

This section contains the following procedures:

Configuring DBS for a Modular Cable Interface

To configure DBS for an MC interface on the Cisco uBR10012 router, use the **cable dynamic-bw-sharing** command in interface configuration mode.

Note The interface must be administratively shutdown before DBS can be configured on the MC interface.

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	**interface modular-cable** *slot* /*subslot* /*port* :*nb-channel-number* **Example:** `Router(config)# interface modular-cable 1/0/0:1`	Configures a modular cable interface. • *slot* —Chassis slot number of the cable interface line card. Cisco uBR10012 router: The valid range for line card is from 5 to 8 and slots 1 and 3 can be used for SIPs. • *subslot* —(Cisco uBR10012 only) Secondary slot number of the cable interface line card. Valid subslots are 0 or 1. • *port* —Downstream port number. Cisco uBR10012 router: The valid range is from 0 to 4 (depending on the cable interface). • *nb-channel-number*—Narrowband channel number.
Step 4	**shutdown** **Example:** `Router(config-if)# shutdown`	Shuts down the interface selected in Step 3 prior to configuring dynamic bandwidth sharing.
Step 5	[**no**] **cable dynamic-bw-sharing** **Example:** `Router(config-if)# cable dynamic-bw-sharing`	Enables dynamic bandwidth sharing (DBS) on the modular cable interface. Use the **no** form of this command to enable static bandwidth sharing (SBS) on the interface.

	Command or Action	Purpose
		Note Starting with Cisco IOS Release 12.2(33)SCE, the DBS mode is enabled by default, on the WB, MC, and IC interfaces. To disable the DBS mode, configure the no cable dynamic-bw-sharing command.
Step 6	**no shutdown** **Example:** `Router(config-if)# no shutdown`	Enables the interface on which dynamic bandwidth sharing is configured.
Step 7	**cable rf-bandwidth-percent***percent-value* [**remaining ratio** *excess-value*] **Example:** `Router(config-if)# cable rf-bandwidth-percent 45 remaining ratio 22`	Enables either static or dynamic bandwidth sharing for modular cable interfaces. The default *percent-value* is 0. The *percent-value* range is 1–96. • If dynamic bandwidth sharing is enabled, the **remaining ratio** option is available. The bandwidth percentage is converted to a committed information rate (CIR) value for the corresponding interface. • The *excess value* - argument specifies the ratio of the excess bandwidth that can be allocated to the modular cable channel. The default *excess value* - is 1. The *excess value* - range is 1–100.

Configuring DBS for a Wideband Cable Interface

To configure DBS for a wideband cable interface, use the **cable dynamic-bw-sharing** command in interface configuration mode for WB cable.

Note The interface must be administratively shutdown before DBS can be configured on the wideband cable interface.

DETAILED STEPS

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

	Command or Action	Purpose
Step 3	**interface wideband-cable** {*slot*/*port* | *slot*/*subslot*/*port* }:*wideband-channel* **Example:** `Router(config)# interface wideband-cable 1/0/0:0`	Configures a wideband cable interface. • *slot* —Chassis slot number of the cable interface line card. Cisco uBR7246VXR router: The valid range is from 3 to 6. Cisco uBR7225VXR router: The valid range is from 1 to 2. Cisco uBR10012 router: The valid range is from 5 to 8. • *subslot* —(Cisco uBR10012 only) Secondary slot number of the cable interface line card. Valid subslots are 0 or 1. • *port* —Downstream port number. Cisco uBR7246VXR and Cisco uBR7225VXR routers: The valid port value is 0 or 1. Cisco uBR10012 router: The valid range is from 0 to 4 (depending on the cable interface). • *wideband-channel*—Wideband channel number. Cisco uBR7246VXR and Cisco uBR7225VXR routers: The valid values are from 0 to 5. Cisco uBR10012 router: The valid range is from 0 to 11.
Step 4	**shutdown** **Example:** `Router(config-if)# shutdown`	Shuts down the interface selected in Step 3 prior to configuring dynamic bandwidth sharing.
Step 5	**cable dynamic-bw-sharing** **Example:** `Router(config-if)# cable dynamic-bw-sharing`	Enables dynamic bandwidth sharing (DBS) on the wideband cable interface. Use the **no** form of this command to enable static bandwidth sharing (SBS) on the interface. **Note** Starting with Cisco IOS Release 12.2(33)SCE, the DBS mode is enabled by default, on the WB, MC, and IC interfaces. To disable the DBS mode, configure the **no cable dynamic-bw-sharing** command.
Step 6	**no shutdown** **Example:** `Router(config-if)# no shutdown`	Enables the interface on which dynamic bandwidth sharing is configured.
Step 7	**cable rf-channel***rf-port* [**bandwidth-percent** *bw-percent*] [**remaining ratio***excess-value*] **Example:** `Router(config-if)# cable rf-channel`	Associates an RF channel on a Wideband SPA with a wideband channel and allocates bandwidth. The range for **bandwidth-percent** is 1–100. If **bandwidth-percent** is not used, the default bandwidth value is 100 percent. The **remaining-ratio** option is only available if DBS is enabled. The default *excess-value* is 1. The range for *excess-value* is 1–100.

	Command or Action	Purpose
	`10 bandwidth-percent 50 remaining-ratio 5`	

Configuring DBS for an Integrated Cable Interface

To configure DBS for an integrated cable interface, use the **cable dynamic-bw-sharing** command in interface configuration mode.

Note The interface must be administratively shutdown before DBS can be configured on the integrated cable interface.

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	**interface integrated-cable** {*slot*/*port* | *slot*/*subslot*/*port* }:*rf-channel* **Example:** `Router(config)# interface integrated-cable 1/0/0:0`	Enters the cable interface mode. • *slot* —Chassis slot number of the cable interface line card. Cisco uBR7246VXR router: The valid range is from 3 to 6. Cisco uBR7225VXR router: The valid range is from 1 to 2. Cisco uBR10012 router: The valid range is from 5 to 8. • *subslot*—(Cisco uBR10012 only) Secondary slot number of the cable interface line card. Valid subslots are 0 or 1. • *port*—Downstream port number. Cisco uBR7246VXR and Cisco uBR7225VXR routers: The valid port value is 0 or 1. Cisco uBR10012 router: The valid range is from 0 to 4 (depending on the cable interface). • *rf-channel*—RF channel number with a range of 0 to 3.

	Command or Action	Purpose
Step 4	**shutdown** **Example:** `Router(config-if)# shutdown`	Shuts down the interface selected in Step 3 prior to configuring dynamic bandwidth sharing.
Step 5	**cable dynamic-bw-sharing** **Example:** `Router(config-if)# cable dynamic-bw-sharing`	Enables dynamic bandwidth sharing on the wideband cable interface. Use the **no** form of this command to enable static bandwidth sharing (SBS) on the interface. **Note** Starting with Cisco IOS Release 12.2(33)SCE, the DBS mode is enabled by default, on the WB, MC, and IC interfaces. To disable the DBS mode, configure the no cable dynamic-bw-sharing command.
Step 6	**no shutdown** **Example:** `Router(config-if)# no shutdown`	Enables the interface where dynamic bandwidth sharing is configured.
Step 7	**cable rf-channel** *rf-port* [**bandwidth-percent** *bw-percent*] [**remaining ratio** *excess-value*] **Example:** `Router(config-if)# cable rf-channel 10 bandwidth-percent 50 remaining-ratio 5`	Enables either static or dynamic bandwidth percentage sharing for an IC interface in interface configuration mode. • *bw-percent*—Static bandwidth allocation of a downstream RF channel. The range is 1 to 100%. The default is 0. • **remaining ratio**—(Optional) Indicates the ratio of the remaining or excess bandwidth that can be allocated to the modular cable channel. This option is available only when dynamic bandwidth sharing is enabled. Run the **cable dynamic-bw-sharing** command to enable DBS. • *excess-value*—Value of excess bandwidth that can be allocated to the cable channel. The range is from 1 to 100. The default value is 1.

Verifying Configuration of DBS

To verify the configuration of the CMTS DBS, use the **show** commands described below.

Cisco uBR10012 Universal Broadband Router

To view the parallel express forwarding (PXF) queueing and link queue statistics, use the **show pxf cpu queue** command for either modular cable or wideband cable interfaces.

Modular cable interface

```
Router(config)# interface modular-cable 1/0/0:1
...
Router(config-if)# cable dynamic-bw-sharing
...
Router# show pxf cpu queue modular-cable 1/0/0:1
```

```
Link Queues :
QID   CIR(act/conf)       EIR            MIR       RF Chan.   Status
  420   19661/19661        1/1        65535/65535      0       Inactive
```

Wideband cable interface

```
Router(config)# interface wideband-cable 1/0/0:0
...
Router(config-if)# cable dynamic-bw-sharing
...
Router# show pxf cpu queue wideband-cable 1/0/0:0
Link Queues :
QID   CIR(act/conf)       EIR            MIR       RF Chan.   Status
  419   32768/32768        1/1        65535/65535      0       Inactive
  566   19661/19661        1/1        65535/65535      1       Inactive
```

Cisco uBR7200 Series Universal Broadband Router

To view the DBS configuration on the Cisco uBR7200 series universal broadband router, use show interface wideband-cable slot/port:wideband-channel dbs and show interface integrated-cable slot/port:rf-channel dbs commands as shown below:

Wideband cable interface

```
Router(config)# interface wideband-cable 5/1:0
...
Router(config-if)# cable dynamic-bw-sharing
...
Router# show
interface wideband-cable 5/1:0 dbs
        Dynamic Bandwidth Sharing is enabled
        bg_rf_channel_bitmap_local 70, active 0
        RF 4: tokens 32500, active 0, policer 3250 KB/s, max_tokens 32500
                deficit counter 0, quantum 10000
                ticks_limit: 62500, max_ticks:687500, policer(ticks): 212
                dbs_pct: 100, remain_bytes: 0, if range: 7-7
        RF 5: tokens 32500, active 0, policer 3250 KB/s, max_tokens 32500
                deficit counter 0, quantum 10000
                ticks_limit: 62500, max_ticks:687500, policer(ticks): 212
                dbs_pct: 100, remain_bytes: 0, if range: 7-7
        RF 6: tokens 32500, active 0, policer 3250 KB/s, max_tokens 32500
                deficit counter 0, quantum 10000
                ticks_limit: 62500, max_ticks:687500, policer(ticks): 212
                dbs_pct: 100, remain_bytes: 0, if range: 7-7
                dbs state: start:4, end:6
```

Integrated cable interface

```
Router(config)# interface integrated-cable 5/1:0
...
Router(config-if)# cable dynamic-bw-sharing
...
Router# show
interface integrated 5/1:0 dbs
        Dynamic Bandwidth Sharing is enabled
        active 0
        RF 4: tokens 32500, active 0, policer 3250 KB/s, max_tokens 32500
              deficit counter 0, quantum 0
              ticks_limit: 62500, max_ticks:687500, policer(ticks): 212
              dbs_pct: 100, remain_bytes: 0, if range: 7-7
```

Enabling DBS Debug

To enable specific DBS debug output, use the **debug cr10k-rp dbs-queue** command on the Cisco uBR10012 router and the debug cable dbs command on the Cisco uBR7200 series routers as shown in the following examples:

```
Router# debug cr10k-rp dbs-queue
CR10K RP debug dynamic BG link queue setup debugging is on
Router# debug cable dbs
DBS for cable 8x8 LC debugging is on
```

Note Routine use of the **debug cr10k-rp dbs-queue** and debug cable dbs commands is not recommended.

Configuration Examples for Dynamic Bandwidth Sharing

This section provides the following configuration examples:

Example: Configuring DBS on a Modular Cable Interface

In the following example, DBS is enabled on modular cable interface 1. Because DBS is enabled, the percent value is converted to a committed information rate (CIR) of 45, which means the modular cable channel is guaranteed 45 percent of the bandwidth. The ratio of excess bandwidth is assigned a value of 22, which means that if there is excess bandwidth available, a remaining ratio of 22 can be assigned to the MC channel.

Cisco uBR10012 Universal Broadband Routers

```
configure terminal
interface modular-cable 1/0/0:1
shutdown
cable dynamic-bw-sharing
no shutdown
cable rf-bandwidth-percent 45 remaining ratio 22
```

Example: Configuring DBS on a Wideband Cable Interface

In the following example, DBS is enabled on wideband channel 0. Because DBS is enabled, the percent value is converted to a CIR value of 50, which means the wideband cable channel is guaranteed 50 percent of the bandwidth. The *excess-value* is assigned a value of 5, which means that if there is excess bandwidth available, a remaining ratio of 5 can be assigned to the wideband channel.

Cisco uBR10012 Universal Broadband Routers

```
configure terminal
interface wideband-cable 1/0/0:0
shutdown
cable dynamic-bw-sharing
no shutdown
cable rf-channel 10 bandwidth-percent 50 remaining ratio 5
```

Cisco uBR7200 Series Universal Broadband Routers

```
configure terminal
interface wideband-cable 1/0:0
shutdown
cable dynamic-bw-sharing
no shutdown
cable rf-channel 10 bandwidth-percent 50 remaining ratio 5
```

Example: Configuring DBS on an Integrated Cable Interface

In the following example, DBS is enabled on integrated channel 0. Because DBS is enabled, the percent value is converted to a CIR value of 50, which means the integrated cable channel is guaranteed 50 percent of the bandwidth. The *excess-value* is assigned a value of 5, which means that if there is excess bandwidth available, a remaining ratio of 5 can be assigned to the integrated channel.

Cisco uBR10012 Universal Broadband Routers

```
configure terminal
interface integrated-cable 1/0/0:0
shutdown
cable dynamic-bw-sharing
no shutdown
cable rf-channel 10 bandwidth-percent 50 remaining ratio 5
```

Cisco uBR7200 Series Universal Broadband Routers

```
configure terminal
interface integrated-cable 1/0:0
shutdown
cable dynamic-bw-sharing
no shutdown
```
cable rf-channel 10 bandwidth-percent 50 remaining ratio 5

Where to Go Next

For further information on the commands required to configure, maintain, and troubleshoot Cisco uBR10012 universal broadband router or Cisco uBR7200 series universal broadband router and Cisco cable modems, see the *Cisco IOS CMTS Cable Command Reference* at:

http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html .

Additional References

The following sections provide references related to the dynamic bandwidth sharing (DBS) on the Cisco CMTS.

Related Documents

Related Topic	Document Title
Cisco IOS CMTS cable commands	See the *Cisco IOS CMTS Cable Command Reference* at: http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html

Standards

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

MIBs

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

RFCs

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

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Dynamic Bandwidth Sharing

Table below lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation

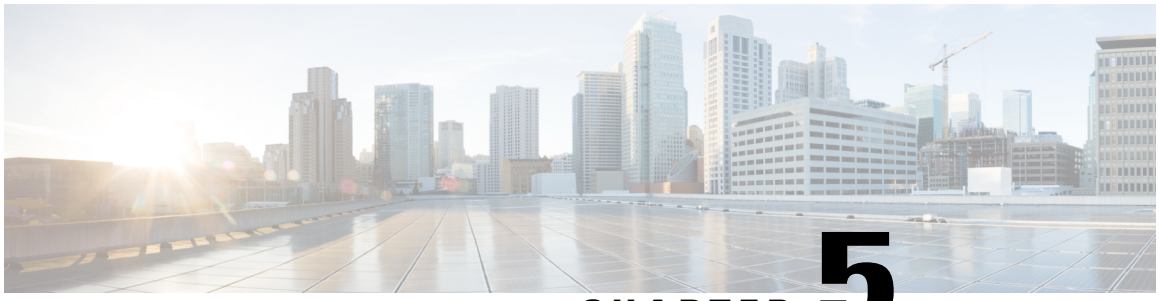
.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note The table below 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.

Table 18: Feature Information for Dynamic Bandwidth Sharing

Feature Name	Releases	Feature Information
CMTS Dynamic Bandwidth Sharing	12.3(23)BC1	The Cisco CMTS new feature enables dynamic bandwidth sharing on a modular cable or wideband cable interface. The following commands were introduced or modified by this feature: • **cable dynamic-bw-sharing** • **cable rf-bandwidth-percent** • **cable rf-channel** • **debug cr10k-rp dbs-queue** • **show pxf cable controller** • **show pxf cpu queue**
CMTS Dynamic Bandwidth Sharing	12.2(33)SCD	Support on the Cisco uBR7225VXR and Cisco uBR7246VXR routers was added. The following commands were introduced or modified: • **debug cable dbs** • **interface integrated-cable** • **interface wideband-cable** • **show interface integrated-cable** • **show interface wideband-cable**



CHAPTER 5

Fairness Across DOCSIS Interfaces

First Published: June 20, 2011

The Fairness Across DOCSIS Interfaces feature introduces an adaptive mechanism to effectively distribute reservable bandwidth for committed information rate (CIR) flows and fair bandwidth for best-effort (BE) service flows across adjacent bonding groups (BGs).

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see 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 document.

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

Contents

Prerequisites for Fairness Across DOCSIS Interfaces

Table below shows the hardware compatibility prerequisites for this feature.

Note The hardware components introduced in a given Cisco IOS Release will be supported in all subsequent releases unless otherwise specified.

Table 19: Fairness Across DOCSIS Interfaces for the Cisco CMTS Routers Hardware Compatibility Matrix

CMTS Platform	Processor Engine	Cable Interface Cards	SIP/SPA
Cisco uBR10012 Universal Broadband Router	Cisco IOS Release 12.2(33)SCF and later releases • PRE2 • PRE4 Cisco IOS Release 12.2(33)SCH and later releases • PRE5	Cisco IOS Release 12.2(33)SCF and later releases • Cisco uBR-MC5X20H[13] • Cisco UBR-MC20X20V • Cisco uBR-MC3GX60V[14]	Cisco IOS Release 12.2(33)SCF and later releases • Cisco Wideband SIP and Cisco Wideband SPA • Cisco 10000 Series SIP-600 and Cisco Wideband SPA Cisco IOS Release 12.2(33)SCH and later releases • Cisco Next Generation Wideband SPA

13 When Fairness Across DOCSIS Interfaces feature is enabled, the Cisco uBR-5X20H cable interface line card can only act as a Guardian or MAC domain host as bonding is not supported on the card.

14 The Cisco uBR-3GX60V cable interface line card is not compatible with PRE2.

Note The term 'Bonding Group (BG)' is used in this document to refer to all the integrated-cable (IC), modular-cable (MC), and wideband-cable (WC) interfaces in the context of Fairness Across DOCSIS Interfaces feature context. The IC and MC interfaces are considered as a single-channel BG.

Restrictions for Fairness Across DOCSIS Interfaces

- The CIR flows cannot reserve all the RF bandwidth. The CIR flows can only reserve 90 percent[15] of the RF bandwidth that is not statically reserved by the "bandwidth-percent", in addition to the legacy CIR bandwidth.
- It is recommended that the CIR reservation be cleared before disabling Fairness Across DOCSIS Interfaces feature to ensure that the CIR reservation is not more than the static reservable bandwidth specified by

15 The reservable bandwidth for CIR flows consists of static and dynamic portions. By default, the static portion of bandwidth is assigned from the legacy configuration. The dynamic portion of bandwidth comes from the headroom left on each RF channel for BE traffic.

the “bandwidth-percent” in legacy configuration. This is to prevent CIR over-subscription after disabling Fairness Across DOCSIS Interfaces feature.

- The effect of Fairness Across DOCSIS Interfaces feature depends on topology and flow distribution. In certain cases, Fairness Across DOCSIS Interfaces feature may not achieve BE fairness or maximum CIR utilization.
- Fairness Across DOCSIS Interfaces feature applies only to dynamic bandwidth sharing (DBS) enabled IC and WB interfaces.

Information About Fairness Across DOCSIS Interfaces

The Fairness Across DOCSIS Interfaces feature is an enhancement over the DOCSIS WFQ scheduler. It enables downstream CIR service flows to be admitted on the interfaces over the thresholds defined in the legacy configuration (that is, “bandwidth-percent” or “max-reserved-bandwidth”). For example, the feature enables large CIR flows (like multicast service flows) to be admitted when the current parameters cannot guarantee enough bandwidth. However, its success rate depends on the allocation and reservation of the bandwidth for cable interfaces within common RF channels.

This feature also ensures fair bandwidth for downstream BE service flows across cable interfaces with common RF channels. The per-flow bandwidth of all active service flows on the adjacent BGs are balanced periodically in proportion to their DOCSIS traffic priority (traffic priority + 1) for downstream BE service flows. This bandwidth, available for BE traffic, can also be used to admit additional CIR flows.

Note For information about DOCSIS traffic priority, see DOCSIS WFQ Scheduler on the Cisco CMTS Routers guide.

How to Configure Fairness Across DOCSIS Interfaces

This section describes the following tasks that are required to implement Fairness Across DOCSIS Interfaces feature:

Configuring Fairness Across DOCSIS Interfaces

This section describes how to enable Fairness Across DOCSIS Interfaces feature on the cable interfaces. The configuration is applied to all WB, MC or IC interfaces on the router.

Restriction We recommend that you clear the CIR reservation before disabling the Fairness Across DOCSIS Interfaces feature to ensure that CIR reservation is not more than the static reservable bandwidth specified by the “bandwidth-percent” in the legacy configuration.

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	**cable acfe enable** **Example:** `Router(config)# cable acfe enable`	Enables Fairness Across DOCSIS Interfaces feature on the cable interfaces.
Step 4	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.

Configuring Maximum Excess Information Rate Ratio

This section describes how to configure the maximum Excess Information Rate (EIR) ratio between the BE bandwidth among adjacent BGs.

The EIR ratio is used to maintain the maximum EIR bandwidth difference between BGs. It helps to prevent BGs (which has only a few active BE service flows) from getting very low or zero EIR bandwidth. Otherwise, these BGs will not be able to admit CIR flows as they get only very low EIR bandwidth.

For example, there are two BGs sharing the same RF channel, with BG1 having 1000 active BE service flows and BG2 having none. If “max-eir-ratio” is not used, BG1 gets all the bandwidth leaving no bandwidth for BG2. When a voice CIR tries for bandwidth at BG2, it will get rejected. If “max-eir-ratio” is set at 10, BG2 gets about 10 percent of the QAM that is sufficient to admit the voice CIR. The ‘max-eir-ratio’ is a trade-off between perfect fairness and CIR utilization. It means, compromising 'flow fairness' to prevent some BGs from getting all the bandwidth leaving the other BGs with none.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable acfe max-eir-ratio** *eir-ratio* **Example:** `Router(config)# cable acfe max-eir-ratio 20`	Configures the maximum EIR ratio between the BE bandwidth among adjacent BGs.
Step 4	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.

Configuring Constant Excess Information Rate Demand

This section describes how to configure the constant excess information rate (EIR) demand for a bonding group (BG). EIR demand is a unitless value that is used to determine relative bandwidth ratio between BGs.

An active EIR flow with DOCSIS priority-0 is given 1000 units of demand in ACFE module. Therefore a BG with constant-eir-demand set to 1 will get no more than 1/1000 of the bandwidth of a single service flow.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cable acfe constant-eir-demand** *value*
4. **exit**

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable acfe constant-eir-demand** *value* **Example:** `Router(config)# cable acfe constant-eir-demand 20`	Configures the constant EIR demand as 20 for a BG.
Step 4	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.

Configuring Maximum Bonus Bandwidth

This section describes how to configure the maximum usable bonus bandwidth for a BG.

Bonus bandwidth is the additional bandwidth provided by the Fairness Across DOCSIS Interfaces feature to each BG for CIR reservation. In the default maximum bonus bandwidth configuration, a single BG can reserve all the underlying RF bandwidth. When the maximum bonus is set, the AC module will not admit CIR flows above that setting even if the scheduler has guaranteed more bandwidth. This will effectively prevent BGs from being starved for CIR flows.

Note The **cable acfe max-bonus-bandwidth** command configuration is applicable only for the new incoming CIR flows. It will not terminate the existing CIR flows that exceeds the **max-bonus-bandwidth** .

Restriction If the maximum bonus bandwidth is less than the current CIR reservation on an interface, no new CIR flows are admitted until the CIR reservation drops below the maximum bonus bandwidth configuration.

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** {**wideband-cable** | **modular-cable** | **interface-cable** }*slot*/*subslot* /*port* :*interface-num* **Example:** `Router(config)# interface wideband-cable 1/0/0:0`	Specifies the interface to be configured. **Note** The valid values for the arguments depend on CMTS router and cable interface line card. See the hardware documentation for your router chassis and cable interface line card for supported values.
Step 4	**cable acfe max-bonus-bandwidth** *bonus-bandwidth* **Example:** `Router(config-if)# cable acfe max-bonus-bandwidth 1000000`	Configures the maximum usable bonus bandwidth for a BG.
Step 5	**end** **Example:** `Router(config)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Verifying the Fairness Across DOCSIS Interfaces

To monitor the Fairness Across DOCSIS Interfaces feature, use the following procedures:

Verifying Reservable Bandwidth

To display the reserved and reservable bandwidth for a particular interface, use the **show interface {wideband-cable | modular-cable | integrated-cable}** command as shown in the example:

```
Router# show interfaces wideband-cable 1/0/0:1 downstream
Total downstream bandwidth 3235 Kbps
Total downstream reserved/reservable bandwidth 0/200 Kbps
Total downstream guaranteed/non-guaranteed bonus bandwidth 66618/9972 Kbps
!
```

The “reservable bandwidth” is a part of the guaranteed bandwidth from the legacy configuration. When the Fairness Across DOCSIS Interfaces feature is disabled, values of both the “guaranteed bonus bandwidth” and “non-guaranteed bonus bandwidth” are zero. When the feature is enabled, the “reservable bandwidth” and “guaranteed bonus bandwidth” represents the maximum CIR that can be reserved on the interface. Unicast CIR flows exceeding this limit are rejected. The additional “non-guaranteed bonus bandwidth” allows the multicast CIR flows to pass the AC module. However, the service flow may not be created successful because the bandwidth comes from the shared pool.

Note The “guaranteed bonus bandwidth” and “non-guaranteed bonus bandwidth” are part of the bandwidth provided by the maximum bonus bandwidth configuration. The “non-guaranteed bonus bandwidth” is expected to be used only by multicast service flows in Cisco IOS Release 12.2(33)SCF.

To display the reserved and reservable bandwidth for a particular interface, use the **show cable admission-control interface** command as shown in the example:

```
Router# show cable admission-control interface wideband-cable 1/0/0:1 verbose
Interface Wideband-Cable1/0/0:1
Configured AC Max Reservable Bandwidth = 6000000 bps
 Resource - Downstream Bandwidth
 -------------------------------
Bkt    Name   Minor # of  Major # of  Excls # of  Non-Ex Curr. Curr. Conf  # of
No            Level Times Level Times Level Times Level  Resv  Ovrsb Level Rej
1             0     0     0     0     0     0     0  *    0.0   0.0  G       0
2             0     0     0     0     0     0     0  *    0.0   0.0  G       0
3             0     0     0     0     0     0     0  *    0.0   0.0  G       0
4             0     0     0     0     0     0     0  *    0.0   0.0  G       0
5             0     0     0     0     0     0     0  *    0.0   0.0  G       0
6             0     0     0     0     0     0     0  *    0.0   0.0  G       0
7             0     0     0     0     0     0     0  *    0.0   0.0  G       0
8             0     0     0     0     0     0     100*   50.0   0.0  G       0
 Note: * indicates that the thresholds are implicit
WB-NB CIR for Wideband-Cable1/0/0:1
CIR Values for Cable8/1/4
Bkt SFAC BW    Rsvd CIR   Reject #
0   0          0          0
1   0          0          0
2   0          0          0
3   0          0          0
4   0          0          0
5   0          0          0
6   0          0          0
7   4500000    3000000    0
Available Guaranteed Bonus BW (bps): 30375000
Available Non-guaranteed Bonus BW (bps): 0
WB Multicast CIR Utilization
Bkt SFAC BW    Rsvd CIR   Reject #
0   0          0          0
1   0          0          0
2   0          0          0
3   0          0          0
4   0          0          0
5   0          0          0
6   0          0          0
7   1500000    0          0
Available Guaranteed Bonus BW (bps): 30375000
Available Non-guaranteed Bonus BW (bps): 0
```

Verifying Global Fairness Across DOCSIS Interfaces Status and Statistics

To display the global status and statistics of the Fairness Across DOCSIS Interfaces feature, use the **show cable acfe summary** command as shown in the example:

```
Router# show cable acfe summary
ACFE state: Enabled
EIR Rebalance period (secs): 5
EIR Rebalance invocations:   254
CIR Acquire rate/limit:      100/100
CIR Acquire invocations:     0
CIR Acquire throttled:       0
CIR Oversubscriptions:       0
```

```
Maximal EIR ratio:           10
Constant EIR demand:         2
```

Verifying Per-Controller Fairness Across DOCSIS Interfaces Status and Statistics

To display the status and statistics for each controller interface, use the **show cable acfe controller** command as shown in the following example:

```
Router# show cable acfe controller modular-cable 1/0/0
EIR Rebalance invoked: 301832
Adaptive CIR granted:  0
Adaptive CIR rejected: 0
Total clusters: 2
!
```

The BG clusters span across multiple channels and are used as a means to share the underlying RF channel bandwidth dynamically.

```
RF      FlexBW
0       30375
1       30375
RF      FlexBW
2       30375
3       30375
```

Verifying Per-Interface Fairness Across DOCSIS Interfaces Status and Statistics

To display the status and statistics for each interface, use the **show cable acfe interface** command as shown in the following example:

```
Router# show cable acfe interface wideband-cable 1/0/0:1
EIR Demand (raw/scale):   0/1
Per-Flow EIR BW (kbps):   19125
Guar Bonus BW (kbps):     19125
Non-guar Bonus BW (kbps): 38250
Reserved Bonus BW (kbps): 0
!
```

The EIR demand is the number of active BE service flows for each BG within a specific time period weighted by DOCSIS priority. The EIR portion is adjusted periodically in proportion to the EIR demand for each BG within the same BG cluster.

```
AC Max Reserved Bandwidth: 200 kbps
Bucket Reservations (kbps):
!
```

For information on Bucket Reservations, see the Service Flow Admission Control for the Cisco CMTS Routers guide.

Troubleshooting

The following **debug** commands help you troubleshoot an improper configuration:

- **debug cable acfe —**Enables debug operation for the Fairness Across DOCSIS Interfaces feature. You should run the debug cable acfe command first to enable other debug options listed below.
- **debug cable acfe algorithm —**Provides debugging information on internal operations of algorithms.

- **debug cable acfe all** —Provides debugging information of all cable events.
- **debug cable acfe filter** —Provides debugging information after applying the filter to limit the debug output.
- **debug cable acfe filter controller** —Provides debugging information on specific controllers.
- **debug cable acfe cluster** —Provides debugging information on specific clusters.
- **debug cable acfe hccp** —Provides debugging information on high availability and Hot Standby Connection-to-Connection Protocol (HCCP) activities.
- **debug cable acfe process** —Provides debugging information on process activities.
- **debug cable acfe read**—Provides debugging information from the system.
- **debug cable acfe topology** —Provides debugging information on cluster topology.
- **debug cable acfe verbose** —Provides debugging information on all internal data.
- **debug cable acfe write** —Provides debugging output to the router.

For detailed information on these and other debug commands, see the Cisco IOS CMTS Cable Command Reference guide.

Configuration Examples for Fairness Across DOCSIS Interfaces

This section lists the following sample configurations for the Fairness Across DOCSIS Interfaces feature on a Cisco CMTS router:

Example: Fairness Across DOCSIS Interfaces

The following sample configuration shows Fairness Across DOCSIS Interfaces feature enabled on the router:

```
Current configuration : 39682 bytes
!
! Last configuration change at 04:30:02 UTC Wed Jan 19 2
! NVRAM config last updated at 04:23:17 UTC Wed Jan 19 2
!
version 12.2
!
cable clock dti
cable acfe enable
!
.
.
.
```

Example: Maximum EIR Demand Ratio

The following sample configuration shows maximum EIR demand ratio configured on the router:

```
Building configuration...
Current configuration : 54253 bytes
!
version 12.2
!
```

```
cable clock dti
cable acfe enable
cable acfe max-eir-ratio 20
!
```

The effect of the **cable acfe max-eir-ratio** command is demonstrated using a simple BG cluster, a 37.5 Mbps RF bandwidth shared by an MC and WB interface. The interfaces are configured as given in the following configuration example:

```
!
interface Modular-Cable1/0/0:0
cable bundle 1
 cable rf-bandwidth-percent 10
!
interface Wideband-Cable1/0/0:0
cable bundle 1
 cable rf-channel 0 bandwidth-percent 10
end
!
```

On this RF channel, 20 percent of the bandwidth is reserved by the 'bandwidth-percent' allowing Fairness Across DOCSIS Interfaces feature to use 27 Mbps, that is: (100 - 20) * 90 * 37.5). If the 'max-eir-ratio' is above 100 and the WB interface has 99 active BE flows and the MC interface has only 1 BE flow, then MC interface gets only 270 kbps, that is 1/(1+99)*27 of the bonus bandwidth. The BE traffic enjoys perfect fairness here. However, it is not possible to admit a unicast CIR flow beyond 270 kbps on the MC interface, as it would exceed the bonus bandwidth. If the 'max-eir-ratio' is set to 10, then the MC interface is treated to have 99/10 flows on it, resulting in a higher bonus bandwidth allocation. The 'max-eir-ratio' is a trade-off between perfect fairness and CIR utilization.

Example: Constant EIR Demand

The following sample configuration shows constant EIR demand on the router:

```
Building configuration...
Current configuration : 54253 bytes
!
version 12.2
!
cable clock dti
cable acfe enable
cable acfe max-eir-ratio 20
cable acfe constant-eir-demand 2
!

!
interface Modular-Cable1/0/0:0
cable bundle 1
 cable rf-bandwidth-percent 10
 cable acfe constant-eir-demand 2

!
interface Wideband-Cable1/0/0:0
cable bundle 1
 cable rf-channel 0 bandwidth-percent 10
 cable acfe constant-eir-demand 2

end
!
```

Example: Maximum Bonus Bandwidth

The following sample configuration shows the maximum bonus bandwidth enabled on the router:

```
Building configuration...
Current configuration : 274 bytes
!
interface Wideband-Cable1/0/0:0
cable bundle 1
cable rf-channel 0 bandwidth-percent 10
cable acfe max-bonus-bandwidth 10000
end
!
```

In this per-interface configuration, even if the Fairness Across DOCSIS Interfaces feature guarantees more than 10 Mbps for a WB interface, the AC module will not pass more than 10 Mbps bandwidth above the legacy reservable bandwidth.

```
!
.
.
.
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Cisco IOS CMTS Cable Command Reference	Cisco IOS CMTS Command Reference
Dynamic Bandwidth Sharing	Dynamic Bandwidth Sharing on the Cisco CMTS Router
DOCSIS WFQ Scheduler	DOCSIS WFQ Scheduler on the Cisco CMTS Routers
Service Flow Admission Control for the Cisco CMTS Routers	Service Flow Admission Control for the Cisco CMTS Routers

Standards

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

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco software 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 by this feature, and support for existing RFCs has not been modified by this feature.	—

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 Fairness Across DOCSIS Interfaces

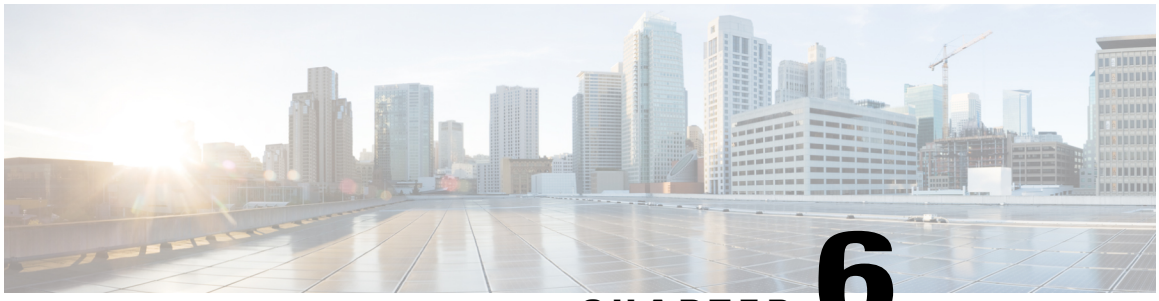
Table below lists the release history for this feature.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note The table below 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.

Table 20: Feature Information for Fairness Across DOCSIS Interfaces

Feature Name	Releases	Feature Information
Fairness Across DOCSIS Interfaces	12.2(33)SCF	The Fairness Across DOCSIS Interfaces feature introduces an adaptive mechanism to effectively distribute reservable bandwidth for CIR flows and fair bandwidth for BE service flows across adjacent BGs. The following commands were introduced or modified: • **cable acfe enable** • **cable acfe max-eir-ratio** • **cable acfe max-bonus-bandwidth** • **debug cable acfe** • **debug cable acfe filter** • **show cable acfe controller** • **show cable acfe interface** • **show cable acfe summary** • **show cable admission-control** • **show cr10k-rp controller** • **show interface integrated-cable** • **show interface modular-cable** • **show interface wideband-cable**



CHAPTER 6

Modular Quality of Service Command-Line Interface QoS on the Cisco CMTS Routers

First Published: December 18, 2008 Last Updated: July 11, 2012

The Modular Quality of Service Command-Line Interface (MQC) is designed to simplify the configuration of Quality of Service (QoS) on the Cisco CMTS routers by defining a common command syntax and resulting set of QoS behaviors across platforms.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see 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 document.

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

Contents

Prerequisites for MQC QoS

Table below shows the Cisco cable modem termination system (CMTS) hardware compatibility prerequisites for this feature.

Note The hardware components introduced in a given Cisco IOS Release will be supported in all subsequent releases unless otherwise specified.

Table 21: MQC QoS Support Hardware Compatibility Matrix

CMTS Platform	Processor Engine	Cable Interface Cards
Cisco uBR10012 Universal Broadband Router	**Cisco IOS Release 12.2(33)SCA and later releases releases** • PRE2 **Cisco IOS Release 12.2(33)SCB and later releases releases** • PRE4 **Cisco IOS Release 12.2(33)SCH and later releases** • PRE5	**Cisco IOS Release 12.2(33)SCB and later releases releases** • Cisco uBR10-MC5X20U/H **Cisco IOS Release 12.2(33)SCC and later releases releases** • Cisco UBR-MC20X20V **Cisco IOS Release 12.2(33)SCE and later releases releases** • Cisco uBR-MC3GX60V [16]
Cisco uBR7246VXR Universal Broadband Router	**Cisco IOS Release 12.2(33)SCA and later releases** • NPE-G1 • NPE-G2	**Cisco IOS Release 12.2(33)SCA and later releases** • Cisco uBR-MC28U/X **Cisco IOS Release 12.2(33)SCD and later releases** • Cisco uBR-MC88V [17]

CMTS Platform	Processor Engine	Cable Interface Cards
Cisco uBR7225VXR Universal Broadband Router	**Cisco IOS Release 12.2(33)SCA and later releases** • NPE-G1 **Cisco IOS Release 12.2(33)SCB and later releases** • NPE-G2	**Cisco IOS Release 12.2(33)SCA and later releases** • Cisco uBR-E-28U • Cisco uBR-E-16U • Cisco uBR-MC28U/X **Cisco IOS Release 12.2(33)SCD and later releases** • Cisco uBR-MC88V

16 The Cisco uBR-3GX60V cable interface line card is not compatible with PRE2.
17 The Cisco uBR-MC88V cable interface line card is compatible only with NPE-G2.

Note The combination of PRE4 and Cisco Half-Height Gigabit Ethernet (HHGE) is not supported in the same chassis.

Restrictions for MQC QoS

- The sum of all priority traffic running on a given port must be less than or equal to 90 percent of the port bandwidth.
- The 802.1p and Multiprotocol Label Switching (MPLS) Matching and Marking feature is currently supported only on Cisco uBR10012 routers.
- The MPLS Pseudowire for Cable L2VPN (Any Transport Over MPLS [AToM]) feature does not support matching and marking based on IP header fields. AToM supports only the matching and marking of experimental (EXP) bits.
- The Transport Layer Security (TLS) and cable dot1q L2VPN do not support the Input service policy and IPv6 service policy.
- PRE2 does not support IPv6 class of service (CoS) policy.
- MQC must be configured on the logical interface of a tunnel for the Cisco uBR10012 router.

Information About MQC QoS

Quality of Service (QoS) is supported on WAN interfaces using the standard MQC. The MQC CLI structure allows you to create traffic policies and attach these policies to interfaces. A traffic policy contains a traffic class and QoS features. A traffic class is used to select traffic, while the QoS features in the traffic policy determine how to treat the classified traffic.

Classifying Traffic

The Cisco uBR10012 Universal Broadband Router must differentiate traffic before it can apply appropriate QoS actions to the traffic. You can use an MQC CLI element called a *class map* to define traffic classification rules or criteria.

Class maps organize data packets into specific categories called classes that can receive user-defined QoS policies. The traffic class defines the classification rules for packets received on an interface.

Configuring QoS Policy Actions and Rules

After classifying the traffic, the Cisco uBR10012 Universal Broadband Router must be configured to handle the traffic that meets the matching criteria. The MQC CLI element *policy map* is used to create QoS policies and configure QoS actions and rules to apply to packets that match a particular traffic class.

A policy map associates a traffic class with one or more QoS actions. While configuring a policy map, you can specify a class map name and configure the actions you want the router to take on the matching traffic. However, before creating class policies in a policy map, the class classification criteria must be configured in a class map.

Whenever you modify a class policy of a policy map, class-based weighted fair queuing (CBWFQ) is notified and new classes are installed as part of the policy map in the CBWFQ system.

Attaching Service Policies to an Interface

After creating and configuring a traffic policy, you should attach the policy to an interface. A policy can be applied to packets in either direction, inbound or outbound. An interface can have different service policies for incoming and outgoing packets.

802.1p CoS

The 802.1p CoS feature introduces QoS-based matching and marking to VLAN user priority bits to provide QoS service on the Gigabit Ethernet WAN interface for 802.1q packets.

The 802.1p CoS marking is a QoS action like the “set ip precedence” that sets the user priority bits for traffic prioritization. CoS refers to the three bits in the VLAN header that is used to indicate the IEEE 802.1p priority of the Ethernet frame as it passes through a switched network.

Marking is a way to identify packet flows to differentiate them. Packet marking enables partitioning of the network into multiple priority levels, or classes of service. During network congestion, the priority marked packets are offered a higher priority than normal packets.

The 802.1p input packets are classified at eight different QoS levels (0 to 7) based on the VLAN user priority bits. The packet classification is specified through the MQC using ‘match’ statements within the class-map command.

On the Cisco CMTS router, 802.1p CoS matching is provided only for the input VLAN tagged frames. The user priority bits matching is not available for TLS and dot1q L2VPN packets.

For 802.1q output packets, QoS marking is done at the VLAN header to modify VLAN user priority bits. QoS services use these priority bit settings to gain traffic priority during times of congestion. For upstream TLS and dot1q L2VPN packets, user priority bits marking is done on the WAN interface.

Note For information on QoS, see Cisco IOS Release 12.0 Quality of Service Solutions Configuration Guide .

MPLS Short-Pipe

The MPLS Short-Pipe Mode feature introduces QoS-based matching and marking of MPLS EXP bits to provide QoS service on the WAN interface for MPLS packets. The three bit EXP define QoS treatment for a packet. The EXP bits support up to eight classes of traffic.

When an IP packet is sent from one site to another, the IP precedence field specifies QoS. Based on the IP precedence marking, the packet is given the treatment configured for that QoS. In an MPLS network, IP precedence value is copied to the MPLS EXP field during label imposition by default.

MPLS marking is a QoS action like the “set ip precedence”. Marking sets different values for the MPLS EXP field. This enables service providers to set the priority for packets transported through their networks. The packet classification criteria is specified through the MQC using ‘match’ statements within the class-map command.

MPLS CoS matching provides the QoS classification function based on the EXP bits of the label entry. For MPLS input packets, QoS classification is done to provide different levels of QoS based on the MPLS EXP bits. For MPLS output packets, the QoS marking is done at the MPLS label header to modify EXP bits.

Note IP ToS will be inactive when the MPLS EXP classification is active as both MPLS EXP and IP ToS shares the same field.

MPLS CoS treats AToM packets as general MPLS packets. For upstream AToM packets, marking is done for EXP bits on the imposition label. For downstream AToM packets, classification is done based on the EXP bits.

MPLS Tunneling

Tunneling is the ability of QoS to be transparent from one edge to the other edge of the network. A tunnel starts on label imposition, and ends at label disposition. When the label is stripped off, the packet goes out as an MPLS packet with a different Per-Hop Behavior (PHB) layer underneath or as an IP packet with and IP PHB layer.

MPLS QoS supports the following tunneling modes:

Uniform Mode

In this mode, packets are treated uniformly across the network. All the customers of the MPLS network use the same IP precedence settings. The IP precedence value and the MPLS EXP bits always correspond to the same PHB.

Short Pipe Mode

This mode provides a distinct MPLS PHB layer (on top of the IP PHB layer) across the entire MPLS network, allowing customers of a service provider to implement their own IP PHB marking scheme on the MPLS network.

For more information on tunneling, see DiffServ Tunneling Modes for MPLS Networks at http://www.cisco.com/en/US/tech/tk436/tk428/tech_tech_notes_list.html .

Input MQC Support on the Cable Bundle Interfaces

The Input MQC Support on the Cable Bundle Interfaces feature introduced on the Cisco CMTS from Cisco IOS Release 12.2(33)SCG onwards enables you to differentiate upstream traffic on the cable bundle or sub-bundle interface and set a corresponding 'qos-group'. This 'qos-group' is used at the output WAN interface to classify and set MPLS EXP bits that are different from the ToS and DSCP value of IP packets.

Note The term cable bundle is used to refer to both the cable bundle and sub-bundle interface in this document.

Table below lists the MQC match statements supported by the Input MQC Support on the Cable Bundle Interfaces feature on a cable bundle interface of the Cisco uBR10012 router.

Table 22: MQC Match Statements Supported on a Cable Bundle Interface of the Cisco uBR10012 Router

Match Statement	Purpose
access-group	Matches access group name or number.
any	Matches any packet.
dscp	Matches differentiated services code point (DSCP) for IPv4.
precedence	Matches precedence for IPv4.
input-interface	Matches interface specification. **Note** This option supports only bundle interface.
ip dcsp	Matches DSCP for IPv4.
ip precedence	Matches precedence for IPv4.
ip rtp	Matches Real-Time Transport Protocol (RTP) port numbers for IPv4.
not	Negates match result.

Match Statement	Purpose
qos-group	Matches QoS group. **Note** The 'qos-group' is internal to the router and should not be used to classify upstream traffic from external world.

Table below lists the MQC action statements supported by the Input MQC Support on the Cable Bundle Interfaces feature on a cable bundle interface of the Cisco uBR10012 router.

Table 23: MQC Action Statements Supported on a Cable Bundle Interface of the Cisco uBR10012 Router

Action Statement	Purpose
set dcsp	Sets DCSP value.
set ip dscp	Sets IP DSCP.
set ip precedence	Sets IP precedence.
set precedence	Sets precedence value.
set qos-group	Sets value from 0 to 99.

Table below lists the MQC match statements supported by the Input MQC Support on the Cable Bundle Interfaces feature on a cable bundle interface of the Cisco uBR7200 series routers.

Table 24: MQC Match Statements Supported on a Cable Bundle Interface of the Cisco uBR7200 Series Routers

Match Statement	Purpose
access-group	Matches access group name.
any	Matches any packet.
class-map	Matches class map name.
discard-class	Discards class identifier.
dscp	Matches DSCP in IPv4 and IPv6 packets.
input-interface	Matches an input interface. **Note** This option supports only the bundle interface.
ip dscp	Matches IP DSCP.
ip precedence	Matches IP precedence.

Match Statement	Purpose
ip rtp	Matches RTP port numbers.
mpls experimental	Matches MPLS experimental bits.
not	Negates match result.
packet length	Matches layer 3 packet length.
precedence	Matches precedence in IPv4 and IPv6 packets.
protocol	Matches protocol.
qos-group	Matches QoS group. **Note** The 'qos-group' is internal to the router and should not be used to classify upstream traffic from external world.
source-address	Matches source address.

Table below lists the MQC action statements supported by the Input MQC Support on the Cable Bundle Interfaces feature on a cable bundle interface of the Cisco uBR7200 series routers.

Table 25: MQC Action Statements Supported on a Cable Bundle Interface of the Cisco uBR7200 Series Routers

Action Statement	Purpose
set dscp	Sets DSCP value.
set ip dscp	Sets IP DSCP.
set ip precedence	Sets IP precedence value.
set precedence	Sets precedence value.
set qos-group	Sets value from 0 to 99.

How to Configure MQC QoS on the Cisco CMTS Routers

Note MQC support is applicable only to WAN interfaces as DOCSIS has its own QoS mechanism. However, DOCSIS QoS extends limited MQC support for cable interfaces to limit peer-to-peer (P2P) traffic.

This section describes the following required and optional procedures:

Configuring QoS Features Using MQC

To configure QoS features using the Modular QoS CLI, complete the following basic steps:

Step 1 Define a traffic class using the **class-map** command.

Step 2 Create a traffic policy by associating the traffic class with QoS features using the **policy-map** command.

Step 3 Attach the traffic policy to the interface using the **service-policy** command and specify whether the policy has to be applied to inbound or outbound traffic.

What to Do Next

Each of the above-mentioned steps is accomplished using a user interface command. Specifically, the three steps are accomplished through the use of three abstractions, class map, policy map, and service policy.

Note Service policies are applied to Gigabit Ethernet, Ten Gigabit Ethernet, 802.1Q VLAN subinterfaces, and tunnel interfaces. Tunnel interfaces are virtual interfaces without queues, and service policies applied to tunnels cannot contain queuing actions. The Cisco uBR10012 Universal Broadband Router does not support per-subinterface queues for VLAN subinterfaces. However, the VLANs share the main interface queues.

For more information about MQC, see the "Configuring the Modular Quality of Service Command-Line Interface" chapter of the http://www.cisco.com/en/US/docs/ios/12_2/qos/configuration/guide/qcfmcli2.html Cisco IOS Quality of Service Solutions Configuration Guide, Release 12.2 document.

Note Though MQC is not broadly supported on cable interfaces as most subscriber queue configuration is controlled by parameters in the cable modem configuration file, a subset of MQC is supported on cable interfaces. This allows multiple service operators (MSOs) to classify P2P traffic based on type of service (ToS) bits and send it to a shaped queue. The P2P traffic control feature can configure shape and queue-limit actions on the P2P traffic control policy map. The ToS P2P is supported only on legacy cable interfaces and not on Wideband or modular cable (MC) interfaces.

Configuring QoS Traffic Classes

The **class-map** command is used to create a traffic class. A traffic class contains three major elements: a name, a series of **match** commands, and, if more than one **match** command exists in the traffic class, an instruction on how to evaluate these **match** commands.

The **match** commands are used to specify various criteria for classifying packets. Packets are checked to determine whether they match the criteria specified in the **match** commands; if a packet matches the specified criteria, that packet is considered a member of the class and is forwarded according to the QoS specifications set in the traffic policy. Packets that fail to meet any of the matching criteria are classified as members of the default traffic class.

For more information about the default traffic class, refer to the "Configuring the Modular Quality of Service Command-Line Interface" chapter of the http://www.cisco.com/en/US/docs/ios/12_2/qos/configuration/guide/qcfmdcli.html Cisco IOS Quality of Service Solutions Configuration Guide, Release 12.2 document.

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	**class-map** [**match-all** | **match-any**] *class-name* **Example:** `Router(config)# class-map class1`	Creates a class to be used with a class map, and enters class-map configuration mode. The class map is used for matching packets to the specified class. • **match-all—**(Optional) Specifies that all match criteria in the class map must be matched, using a logical AND of all matching statements defined under the class. This is the default. • **match-any—**(Optional) Specifies that one or more match criteria must match, using a logical OR of all matching statements defined under the class. • *class-name* —User-defined name of the class.
Step 4	**match** *type* **Example:** `Router(config-cmap)# match access-group 101`	Specifies the matching criterion to be applied to the traffic, where *type* represents one of the forms of the **match** command.
Step 5	end **Example:** `Router(config-cmap)# end`	Exits the class-map configuration mode and returns to privileged EXEC mode.

What to Do Next

Table below lists the match options supported on the class-map command.

Table 26: Match Options Supported on the MQC QoS

Command	Purpose
match access-group {*number* | *name*}	Specifies that the packet must be permitted by the specified access control list (ACL). • *number*—ACL identifier applied to an interface. Valid values are from 1 to 2699. • *name*—Packet with the indicated name must be permitted by the access list. The name can be a maximum of 40 alphanumeric characters.
match-all	Specifies that the packet must match all of the matching criteria defined for a class map.
match-any	Specifies that the packet must match at least one of the matching criteria defined for a class map.
match cos *cos-value* [*cos-value* [*cos-value* [*cos-value*]]]	Specifies that the packet must match on the basis of a Layer 2 CoS/Inter-Switch Link (ISL) marking. • *cos-value*— IEEE 802.1Q/ISL CoS value. The cos-value can range from 0 to 7; up to four CoS values, separated by a space, can be specified in one match cos statement.
match input-interface *name*	Specifies that the packet input interface must match the interface name. **Note** Matching is supported for cable bundles but not for physical cable interfaces.

Command	Purpose
match ip dscp {*ip-dscp-value* | **afxy** | **csx** | **ef** | **default**}	Specifies that the packet IP differentiated service code point (DSCP) value must match one or more of the specified attributes. • *ip-dscp-value*—*DSCP* value to match. Valid values are from 0 to 63. You can specify up to 8 code point values, using a space to separate consecutive values. Instead of specifying a numeric ip-dscp-value, you can specify one of the following reserved keywords: • **afxy**—Indicates assured forwarding points. The first number (x) indicates the AF class. Valid values are from 1 to 4. The second number (y) indicates the level of drop preference within each class. Valid values are from 1 (low drop) to 3 (high drop). • **csx**—Indicates class selector code points that are backward-compatible with IP precedence. Valid values for x are from 1 to 7. The CS code points (CS1 through CS7) are identical to IP precedence values from 1 to 7. • **ef**—Indicates expedited forwarding. • **default**—Indicates best effort or DSCP 0.
match ip precedence {*ip-precedence-value* | *precedence-name*}	Specifies that the packet IP precedence value must match one or more precedence values or the name of the precedence. • *ip-precedence-value* —IP precedence value to match. Valid values are from 0 to 7. You can specify up to 8 precedence values, using a space to separate consecutive values. • *precedence-name*—Name of the IP precedence value.

Command	Purpose
match ip rtp {*lowest-udp-port range* }	Specifies that the packet with even-numbered UDP port value must be within the specified range of port numbers. Only even-numbered ports are matched because they carry the real-time data streams. Odd-numbered ports are not matched because they only carry control information. • *lowest-udp-port*—Number specified from 0 to 65535 and is the lowest number in the range. • *range*—Number specified from 0 to 65535 and is the highest number in the range.
match mpls experimental topmost *value*	Matches the experimental (EXP) value in the topmost label. • *value*—Value to which you want to set the MPLS EXP bits in the topmost label header. Valid values are from 0 to 7.
match not *criteria*	Specifies that the packet must not match this particular matching criterion value. • *criteria*—Match criterion value that should be an unsuccessful match criteria. All other values of the specified match criterion are considered successful match criteria.
match qos-group *number*	Specifies that the packet QoS group number value must match the specified QoS group number. • *number*—Group number specified from 0 to 99.

Configuring Traffic Policies

After creating traffic classes, you can configure traffic policies to configure marking features to apply certain actions to the selected traffic in those classes.

The **policy-map** command is used to create a traffic policy. The purpose of a traffic policy is to configure the QoS features that should be associated with the traffic that has been classified in a user-specified traffic class.

Note A packet can match only one traffic class within a traffic policy. If a packet matches more than one traffic class in the traffic policy, the first traffic class defined in the policy will be used.

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 policy9`	Creates or modifies a traffic policy and enters policy map configuration mode, where: • *policy-map-name*—Name of the traffic policy to configure. Names can be a maximum of 40 alphanumeric characters.
Step 4	**class** {*class-name* | **class-default**} **Example:** `Router(config-pmap)# class class1`	Specifies the name of the traffic class to which this policy applies and enters policy-map class configuration mode: • *class-name*—Policy applied to a user-defined class name previously configured. • **class-default**—Specifies that the policy applies to the default traffic class.
Step 5	end **Example:** `Router(config-pmap)# end`	Exits the policy-map class configuration mode and returns to privileged EXEC mode.

Defining QoS Actions in a Policy Map

Action commands can be added from within class mode on a policy map. Action commands fall into three general categories as given below:

Set Actions

Set commands allow traffic to be marked such that other network devices along the forwarding path can quickly determine the proper class of service to apply to a traffic flow. Set commands can be applied to both input and output policy maps.

Table below lists the set options supported on the Cisco uBR10012 Universal Broadband Router.

Table 27: Set Options Supported on the MQC QoS

Command	Purpose
set cos {*cos-value* | *from-field* [**table** *table-map-name*]}	Sets the Layer 2 CoS value of an outgoing packet. • *cos-value*—IEEE 802.1Q CoS value. The valid range is from 0 to 7. • *from-field*—Packet-marking category used to set packet CoS value. If a table map is used for mapping and converting packet-marking values, this establishes the "map from" packet-marking category. Packet-marking category keywords are precedence and dscp. • **table**—(Optional) Sets the values specified in a table that is used to set the CoS value. • *table-map-name*—(Optional) Name of the table map used to specify the CoS value. Maximum of 64 alphanumeric characters.
set ip dscp {*ip-dscp-value* | **afxy** | **csx** | **ef** | **default**}	Marks a packet with the differentiated services code point (DSCP) you specify. Valid values are from 0 to 63. Instead of specifying a numeric ip-dscp-value, you can specify one of the following reserved keywords: • **afxy**—Indicates assured forwarding points. The first number (x) indicates the AF class. Valid values are from 1 to 4. The second number (y) indicates the level of drop preference within each class. Valid values are from 1 (low drop) to 3 (high drop). • **csx**—Indicates class selector code points that are backward-compatible with IP precedence. Valid values for x are from 1 to 7. The CS code points (CS1 through CS7) are identical to IP precedence values from 1 to 7. • **ef**—Indicates expedited forwarding. • **default**—Indicates best effort or DSCP 0.
set ip precedence {*precedence-value* }	Marks a packet with the IP precedence level you specify. Valid values are from 0 to 7.

Command	Purpose
set mpls experimental topmost {*mpls-exp-value* | **qos-group** [**table** *table-map-name*]}	Set the MPLS EXP field value in the topmost label on either an input or an output interface. • *mpls-exp-value*—Value used to set the MPLS EXP bits defined by the policy map. The valid values range from 0 to 7. • **qos-group**—Specifies that the qos-group packet-marking category is used to set the MPLS EXP imposition value. If you are using a table map for mapping and converting packet-marking values, this establishes the "map from" packet-marking category. • **table**—(Optional) Used in conjunction with the **qos-group** keyword. Indicates that the values set in a specified table map will be used to set the MPLS EXP value. • *table-map-name* —(Optional) Name of the table map used to specify the MPLS EXP value. Used in conjunction with the table keyword. The name can be a maximum of 64 alphanumeric characters.
set qos group *group-id*	Marks a packet with the QoS group identifier you specify. The valid values range from 0 to 99.

Police Actions

Traffic policing is a traffic regulation mechanism that is used to limit the rate of traffic streams. Policing allows you to control the maximum rate of traffic sent or received on an interface. Policing propagates bursts of traffic and is applied to the inbound or outbound traffic on an interface. When the traffic rate exceeds the configured maximum rate, policing drops or remarks the excess traffic. Although policing does not buffer excess traffic, in the output direction, a configured queuing mechanism applies to conforming packets that might need to be queued while waiting to be serialized at the physical interface.

Traffic policing uses a token bucket algorithm to manage the maximum rate of traffic. This algorithm is used to define the maximum rate of traffic allowed on an interface at a given moment in time. The algorithm puts tokens into the bucket at a certain rate. Each token is permission for the source to send a specific number of bits into the network. With policing, the token bucket determines whether a packet exceeds or conforms to the applied rate. In either case, policing implements the action you configure such as setting the IP precedence or differentiated services code point (DSCP).

To configure traffic policing based on bits per second, use the **police** command in policy-map class configuration mode.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configureterminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**policy-map** [**name**] **Example:** `Router(config)# policy-map policy9`	Specifies the traffic policy and enters policy-map configuration mode.
Step 4	**class** [**name**] **Example:** `Router(config-pmap)# class class1`	Specifies the name of the traffic class to which this policy applies and enters policy-map class configuration mode.
Step 5	police [bps] [burst-normal] [burst-excess] conform [conform-action] exceed [exceed-action] **Example:** `Router(config-pmap-c)# police 10000000 15000 20000 conform transmit exceed drop`	Configures traffic policing based on bits per second. • *bps*—(Optional) Average rate in bits per second (bps). Valid values are from 8,000 to 2,488,320,000 bps. If you only specify police bps, the router transmits the traffic that conforms to the bps value and drops the traffic that exceeds the bps value. • *burst-normal*—(Optional) Normal or committed burst size used by the first token bucket for policing. The burst-normal option specifies the committed burst in bytes. Valid values are from 1 to 512,000,000. The default is 9,216 bytes. • *burst-excess*—(Optional) Excess burst size used by the second token bucket for policing. The burst-excess option specifies the excess burst in bytes. Valid values are from 0 to 1,024,000,000 bytes. The default is 0. You must specify burst-normal before you specify burst-excess. **Note** When the burst-excess value equals 0, we recommend that you set the egress burst-normal value to be greater than or equal to the ingress burst-normal value plus 1. Otherwise, packet loss can occur. For example: burst-excess = 0; egress burst-normal >= ingress burst-normal + 1. • *conform-action*—Action to take on packets that conform to the rate limit. The default action is transmit. You must specify burst-excess before you specify conform. • *exceed-action* —Action to take on packets that exceed the rate limit. The default action is drop. You must specify conform before you specify exceed.

	Command or Action	Purpose
Step 6	**end** **Example:** `Router(config-pmap-c)# end`	Exits the policy-map class configuration mode and returns to privileged EXEC mode.

Queuing Actions

When queuing actions are applied to a given class within a policy map, they either cause queues to be created for that particular class of traffic or control how the queues are managed. Queuing commands are valid only in the output direction.

The Cisco uBR10012 Universal Broadband Router supports the MQC policy maps for class queue creation on WAN interfaces.

The following two types of queues are supported through MQC:

- Priority queues—Used mainly for voice traffic. They are policed at their individual committed information rate (CIR) to limit their bandwidth to the subscribed level. Only one priority queue is allowed per logical interface.
- Class queues—Implemented as best effort queues. They are based on a specified bandwidth in Kbps and shaped using the "bandwidth" policy map action. Generally, the specified bandwidth is not guaranteed.

Weighted random early detection (WRED) is a mechanism for controlling congestion of queues. WRED combines the capabilities of the random early detection (RED) mechanism with IP precedence, DSCP, and discard class to provide preferential handling of higher priority packets. For additional information on WRED, refer to the Cisco IOS Quality of Service Solutions Configuration Guide, Release 12.2 .

Note Cisco IOS Release 12.2(33)SCB does not support random-detect for type of service (ToS) peer-to-peer (P2P) policy maps.

Table below lists the **queuing actions** supported on the Cisco uBR10012 Universal Broadband Router.

Table 28: Queuing Actions Supported on the MQC QoS

Command	Purpose
priority	Assigns priority to the class you specified and reserves a priority queue for class-based weighted fair queuing (CBWFQ) traffic. The **priority** command does not have any arguments. You must use the **police** command to specify a guaranteed bandwidth.

Command	Purpose
queue-limit number-of-packets	Specifies or modifies the maximum number of packets that a particular class queue can hold.
random-detect dscp-based	Configures WRED to drop packets based on a DSCP value.
random-detect precedence-based	Configures WRED to drop packets based on an IP precedence value.
random-detect dscp dscp-values sub-class-val1 [...[sub-class-val8]]minimum-thresh *min-thresh-value* **maximum-thresh** *max-thresh-value* **mark-prob** *mark-prob-value*	Configures the minimum and maximum packet thresholds for the differentiated services code point (DSCP) value. • dscp-values—DSCP value. The DSCP value can be a number from 0 to 63. • **min-thresh-value**—Minimum threshold in number of packets. The value range of this argument is from 1 to 4096. • **max-thresh-value**—Maximum threshold in number of packets. The value range of this argument is from the value of the **min-thresh-value** argument to 4096. • **max-prob-value**—Specifies the fraction of packets dropped when the average queue depth is at the maximum threshold.
random-detect precedence values *sub-class-val1* [...[*sub-class-val8*]] **minimum-thresh** *min-thresh-value* **maximum-thresh** *max-thresh-value* **mark-prob** *mark-prob-value*	Configures WRED and distributed WRED (DWRED) parameters for a particular IP Precedence. Valid values are from 0 to 7. Typically, 0 represents low priority traffic that can be aggressively managed (dropped) and 7 represents high priority traffic. • *min-thresh-value*—Minimum threshold in number of packets. The value range of this argument is from 1 to 4096. • *max-thresh-value*—Maximum threshold in number of packets. The value range of this argument is from the value of the min-thresh-value argument to 4096. • *mark-prob-value* —Fraction of packets dropped when the average queue depth is at the maximum threshold.

Command	Purpose
shape [**average**]*cir*	Shapes traffic to the rate you specify, or shapes traffic based on the percentage of available bandwidth you specify. • **average—**Specifies the committed burst (Bc) that specifies the maximum number of bits sent out in each interval. • *cir***—**Committed information rate (CIR), in bits per second (bps).
bandwidth {*bandwidth-kbps* | **percent** *percentage* | **remaining percent** *percentage*}	Specifies or modifies the minimum bandwidth allocated for a traffic class in a policy map. • *bandwidth-kbps***—**Minimum bandwidth allocated for a class belonging to a policy map. Accepted input values are from 8 to 10,000,000,000 although the maximum value entered should not be larger than the link bandwidth of the slowest interface to which the policy will be applied. • **percent** *percentage* **—**Specifies or modifies the minimum percentage of the link bandwidth allocated for a class belonging to a policy map. Valid values are from 1 to 100. • **remaining percent** *percentage***—**Specifies or modifies the minimum percentage of unused link bandwidth allocated for a class belonging to a policy map. Valid values are from 1 to 100. **Note** Configure the amount of bandwidth large enough to also accommodate Layer 2 overhead.

Attaching Service Policies

The **service-policy** command is used to attach the traffic policy, as specified with the **policy-map** command, to an interface. Because the elements of the traffic policy can be applied to packets entering and leaving the interface, it is essential to specify whether the traffic policy characteristics should be applied to incoming or outgoing packets.

To attach a policy map that the router can use to apply QoS policies to inbound and outbound packets, use the **service-policy** command in interface or map class configuration mode.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configureterminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *interface-name* **Example:** `Router(config)# interface GigabitEthernet 3/0/0`	Specifies the interface and enters interface configuration mode.
Step 4	Router(config-if)# service-**policy** {*input* | *output*} *policy-map-name* **Example:** `Router(config-if)# service-policy output policy1`	Specifies a policy map that the router can use to apply QoS policies to inbound or outbound packets. • *input* —Applies the QoS policy to inbound packets. • *output*—Applies the QoS policy to outbound packets. • *policy-map-name*—Name of the policy map (created using the policy-map command) you want to attach. The policy-map-name can be a maximum of 40 alphanumeric characters.

Configuring Output Rate

To restrict the WAN interface bandwidth output rate to a smaller value than that of the physical link bandwidth, use the output-rate command in interface configuration mode.

Note The output-rate command is valid only for Gigabit Ethernet interfaces.

Note Starting with Cisco IOS Release 12.2(33)SCG, the **output-rate** command is not supported and the value 10,000 is used for the output line rate on a Cisco uBR10012 router.

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	**interface interface-name** **Example:** `Router(config)# interface GigabitEthernet 3/0/0`	Specifies the interface and enters interface configuration mode.
Step 4	**output-rate** *rate* **Example:** `Router(config-if)# output-rate 100`	Specifies a custom-defined output rate to a WAN interface instead of the default line rate. • *rate* —Output rate defined for the WAN interface, in kilobits per second. Valid values range from 1 to 1,000,000.
Step 5	exit **Example:** `Router(config-if)# exit`	Exits the interface configuration mode and returns to privileged EXEC mode.

Configuring Input MQC Support on the Cable Bundle Interfaces

To configure input MQC on a cable bundle interface to differentiate upstream traffic and set corresponding "qos-group" features, follow the steps given below.

Restriction

- QoS actions like policing, shaping, WRED, and queuing are not supported.
- Input MQC cannot be configured on cable physical interfaces.

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	**class-map match-all** *class-name* **Example:** `Router(config)# class-map match-all class-ip-prec-6`	Creates a class to be used with a class map, and enters class-map configuration mode. The class map is used for matching packets to the specified class. • **match-all—**Specifies that all match criteria in the class map must be matched, using a logical AND of all matching statements defined under the class. This is the default option. • *class-name***—**User-defined name of the class.
Step 4	**match ip precedence** *ip-precedence-value* **Example:** `Router(config-cmap)# match ip precedence 6`	Specifies the IP precedence values as match criteria. • *ip-precedence-value* **—**IP precedence value. The valid values range from 0 to 7.
Step 5	exit **Example:** `Router(config-cmap)# exit`	Exits the class-map configuration mode and returns to global configuration mode.
Step 6	Repeat Step 3, on page 141 and Step 4, on page 141 to define the second class map.	
Step 7	**policy-map** *policy-map-name* **Example:** `Router(config)# policy-map policy-input`	Creates a policy map that can be attached to one or more interfaces to specify a service policy and enters policy map configuration mode. • *policy-map-name* **—**Name of the policy map. The name can be up to 40 alphanumeric characters.
Step 8	**class** *class-name* **Example:** `Router(config-pmap-c)# class`	Specifies the name of the class for which to create a policy and enters the policy-map class configuration mode. • *class-name***—**Name of the class to configure.

	Command or Action	Purpose
	`class-ip-prec-6`	
Step 9	**set qos-group** *group-id* **Example:** `Router(config-pmap-c)# set qos-group 6`	Sets a group ID that can be used later releases to classify packets. • *group-id*—Group identifier number. The valid range is from 0 to 99.
Step 10	exit **Example:** `Router(config-pmap-c)# exit`	Exits the policy-map class configuration mode and returns to global configuration mode.
Step 11	**interface bundle** *bundle-number* **Example:** `Router(config)# interface bundle 1`	Configures a cable bundle interface and enters interface configuration mode. • *bundle-number* —Cable bundle interface identification number.
Step 12	**service-policy input** *policy-map-name* **Example:** `Router(config-if)# service-policy input policy-input`	Attaches a policy map to an input interface that is used as the service policy for the interface • *input* —Attaches the specified policy map to the input interface. • *policy-map-name* —Name of the service policy map (created using the **policy-map** command) to be attached. The name can be up to 40 alphanumeric characters
Step 13	end **Example:** `Router(config-pmap-c)# end`	Exits the interface configuration mode and returns to privileged EXEC mode.

Configuration Examples for MQC QoS

This section provides the following configuration examples:

Example: Configuring the Traffic Class

The following example shows how to create two traffic classes and specify their match criteria. For the first traffic class called class1, access control list (ACL) 101 is used as the match criteria. For the second traffic

class called class2, ACL 102 is used as the match criteria. Packets are checked against the contents of these ACLs to determine if they belong to the class.

```
Router(config)# class-map class1

Router(config-cmap)# match access-group 101
Router(config-cmap)# exit

Router(config)# class-map class2

Router(config-cmap)# match access-group 102

Router(config-cmap)# exit
```

Example: Configuring the Traffic Policy

The following example shows how to define a traffic policy called policy1 that contains policy specifications for class1.

```
Router(config)# policy-map policy1
Router(config-pmap)# class class1
Router(config-pmap-c)# bandwidth 3000

Router(config-pmap-c)# queue-limit 30

Router(config-pmap)# exit
```

Example: Attaching the Service Policy

The following example shows how to attach an existing traffic policy to an interface. After you define a traffic policy with the **policy-map** command, you can attach it to one or more interfaces by using the **service-policy** command in interface configuration mode. Although you can assign the same traffic policy to multiple interfaces, each interface can have only one traffic policy attached at the input and only one traffic policy attached at the output.

```
Router(config)# interface GigabitEthernet 3/0/0
Router(config-if)# service-policy output policy1

Router(config-if)# exit
```

Example: Verifying QoS Policy

The following example shows how to verify a policy map configuration by entering any of the following commands in privileged EXEC mode.

```
Router# show policy-map policy-map-name class class-name
Class foobar
      bandwidth percent 20
       packet-based wred, exponential weight 9
      random-detect aggregate
      random-detect precedence values 2 minimum-thresh 1024 maximum-thresh 20481
```

Example: Configuring Input MQC Support on the Cable Bundle Interfaces

The following example shows how to differentiate upstream traffic on the cable bundle interfaces and set corresponding “qos-group” features.

```
!Define two different class maps.
class-map match-all class-ip-prec-6
  match ip precedence 6
class-map match-all class-ip-prec-7
  match ip precedence 7
!Define a policy map.
policy-map policy-input
  class class-ip-prec-6
   set qos-group 6
  class class-ip-prec-7
   set qos-group 7
!Attach the policy map to the cable bundle interface in the input direction.
configure terminal
 interface bundle 1
  service-policy input policy-input
```

How to Configure 802.1p CoS and MPLS EXP on the Cisco CMTS Routers

This section describes the following required procedures:

Configuring 802.1p CoS Matching

Use the following procedure to specify a class-map and match a packet based on the CoS marking.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configureterminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**class-map** *class-map-name*— **Example:** `Router(config)# class-map cos1`	Specifies the class name used for the class in the policy map. • *class-map-name*— Name of the class for the class map.

	Command or Action	Purpose
Step 4	**match cos***cos-value* **Example:** `Router(config-cmap)# match cos 0`	Enters the class-map configuration mode and specifies the class of service that needs to match the class map. • *cos-value*— Packet CoS bit value. The valid values range from 0 to 7. You can specify up to four CoS values in one **match cos** statement.
Step 5	end **Example:** `Router(config-cmap)# end`	Exits the class-map configuration mode and returns to privileged EXEC mode.

Configuring 802.1p CoS Marking

Use the following procedure to specify a policy-map and associate a map class with it to set the CoS value for an outgoing packet.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configureterminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**policy-map policy-map-name** **Example:** `Router(config)# policy-map cos0`	Specifies a policy map name. • *policy-map-name*—Policy map name.
Step 4	**class name** **Example:** `Router(config-pmap)# class cos1`	Enters the policy-map configuration mode and specifies the map class to which the packets has to be matched. • *name* —Map class name.

	Command or Action	Purpose
Step 5	set cos *cos-value* **Example:** `Router(config-pmap-c)# set cos 2`	Enters the policy-map class configuration mode and specifies a CoS value to associate with the packet. • *cos-value*—Class of service value. The valid values range from 0 to 7.
Step 6	**end** **Example:** `Router(config-pmap-c)# end`	Exits the policy-map class configuration mode and returns to privileged EXEC mode.

Configuring MPLS EXP Matching

Use the following procedure to specify a class-map and match a packet based on the EXP marking.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configureterminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**class-map** *class-map-name* **Example:** `Router(config)# class-map exp7`	Specifies the class name used for the class in the policy map. • *class-map-name*—Name of the class for the class map.
Step 4	**match mpls experimental topmost** *number* **Example:** `Router(config-cmap)# match mpls experimental topmost 2`	Enters the class-map configuration mode and specifies the MPLS EXP field in the topmost label header. • *number*—MPLS EXP field number. The valid values range from 0 to 7.

	Command or Action	Purpose
Step 5	end **Example:** `Router(config-cmap)# end`	Exits the class-map configuration mode and returns to privileged EXEC mode.

Configuring MPLS EXP Marking

Use the following procedure to specify a policy-map and associate a map class set to the EXP value for an outgoing packet.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configureterminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**policy-map** *policy-map-name* **Example:** `Router(config)# policy-map exp5`	Specifies a policy map name. • *policy-map-name*—Policy map name.
Step 4	**class name** **Example:** `Router(config-pmap)# class exp7`	Enters the policy-map configuration mode and specifies the map class to which the packets has to be matched. • *name*— Map class name.
Step 5	t **set mpls experimental topmos***number* **Example:** `Router(config-pmap-c)# set mpls experimental topmost 2`	Enters the policy-map class configuration mode and sets the MPLS EXP field in the topmost label header. • *number* —MPLS EXP field number. The valid values range from 0 to 7.

	Command or Action	Purpose
Step 6	**end** **Example:** `Router(config-pmap-c)# end`	Exits the policy-map class configuration mode and returns to privileged EXEC mode.

Configuration Examples for 802.1p CoS and MPLS EXP Matching and Marking

This section provides the following configuration examples:

Example: Configuring 802.1p CoS Matching

The following example shows how to match traffic classes within the 802.1p domain using packet CoS values.

```
Router> enable
Router# configure terminal
Router(config)# class-map cos1
Router(config-cmap)# match cos 0
Router(config-cmap)# end
```

Example: Configuring 802.1p CoS Marking

The following example shows how to define traffic classes within the 802.1p domain using packet CoS values.

```
Router> enable
Router# configure terminal
Router(config)# policy-map cos2
Router(config-pmap)# class cos1
Router(config-pmap)# set cos 2
Router(config-pmap)# end
```

Example: Configuring MPLS EXP Matching

The following example shows how to match traffic classes within the MPLS domain using packet EXP values.

```
Router> enable
Router# configure terminal
Router(config)# class-map exp1
Router(config-cmap)# match mpls experimental topmost 2
Router(config-cmap)# end
```

Example: Configuring MPLS EXP Marking

The following example shows how to define traffic classes within the MPLS domain using packet EXP values.

```
Router> enable
Router# configure terminal
Router(config)# policy-map exp2
Router(config-pmap)# class exp1
Router(config-pmap)# set mpls experimental topmost 2
Router(config-pmap)# end
```

Verifying 802.1p CoS and MPLS EXP Matching and Marking

This section explains how to verify 802.1p CoS and MPLS EXP configurations on the Cisco CMTS router:

Example: Verifying Matching and Marking

The following example shows how to verify the matching and marking configuration by entering the following command in privileged EXEC mode:

```
Router# ping vrf vrfa 1.3.99.98
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.3.99.98, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/10/20 ms
```

Example: Verifying QoS and Service Flow

The following example shows how to verify the QoS and service flow information for a particular cable modem (CM) by entering the following command in privileged EXEC mode:

```
Router# show cable modem 1.3.99.98 qos
Load for five secs: 1%/0%; one minute: 1%; five minutes: 1%
Time source is hardware calendar, *23:01:41.873 pst Thu Mar 3 2011
Sfid  Dir Curr  Sid   Sched  Prio MaxSusRate  MaxBrst     MinRsvRate  Throughput
          State       Type
49    US  act   31    BE     7    300000000   1000000     0           1968000
50    DS  act   N/A   BE     0    300000000   3044        0           1969253
```

Example: Verifying Input and Output Service Policies

The following example shows how to verify the statistics and the configurations of the input and output service policies that are attached to an interface by entering the following command in privileged EXEC mode:

```
Router# show policy-map interface gigabitEthernet 1/2/0
Load for five secs: 1%/0%; one minute: 1%; five minutes: 1%
Time source is hardware calendar, *23:02:40.857 pst Thu Mar 3 2011
 GigabitEthernet1/2/0
  Service-policy input: policy-in
    Class-map: class-exp-0 (match-all)
      6647740 packets, 9304674796 bytes
      30 second offered rate 3234000 bps, drop rate 0 bps
      Match: mpls experimental topmost 0
```

```
      QoS Set
        precedence 3
          Packets marked 6647740
    Class-map: class-default (match-any)
      1386487 packets, 1903797872 bytes
      30 second offered rate 658000 bps, drop rate 0 bps
      Match: any
  Service-policy output: policy-out
    Class-map: class-pre-1 (match-all)
      2041355 packets, 2857897000 bytes
      30 second offered rate 986000 bps, drop rate 0 bps
      Match: ip precedence 1
      QoS Set
        mpls experimental topmost 1
          Packets marked 2041355
    Class-map: class-default (match-any)
      6129975 packets, 8575183331 bytes
      30 second offered rate 2960000 bps, drop rate 0 bps
      Match: any
```

Example: Verifying PXF QoS

The following example shows how to verify the Parallel eXpress Forwarding (PXF) CPU statistics and QoS for a particular interface by entering the following command in privileged EXEC mode:

```
Router# show pxf cpu statistics qos gigabitEthernet 1/2/0
Load for five secs: 1%/0%; one minute: 1%; five minutes: 1%
Time source is hardware calendar, *23:04:11.893 pst Thu Mar 3 2011
   Classmap           Match         Pkts           Bytes
    Index             Number        Matched        Matched
-------------- --------------- --------------- -------------
 policy-in (Input) service-policy :
class-exp-0     (0)     0               6674330         751960948
class-default   (1)     0               1392134         1911548970
 policy-out (Output) service-policy :
class-pre-1     (0)     0               2049682         2869554800
class-default   (1)     0               6154976         20224030
```

Example: Verifying MPLS Virtual Circuits

The following example shows how to verify the state of all virtual circuits associated with an MPLS pseudowire by entering the following command in privileged EXEC mode:

```
Router# show cable l2-vpn xconnect mpls-vc-map state
Load for five secs: 2%/0%; one minute: 2%; five minutes: 1%
Time source is hardware calendar, *23:05:30.061 pst Thu Mar 3 2011
MAC Address    Peer IP Address  VCID  Type  Prio  State  Customer Name/VPNID  State
54d4.6f88.7362  10.8.8.8        97    Prim*        UP                          UP
```

Example: Verifying MPLS Mapping

The following example shows how to verify the details about the mapping between an MPLS pseudowire and its virtual circuits by entering the following command in privileged EXEC mode:

```
Router# show cable l2-vpn xconnect mpls-vc-map 54d4.6f88.7362 verbose
Load for five secs: 2%/0%; one minute: 1%; five minutes: 2%
Time source is hardware calendar, *16:46:29.139 pst Thu Mar 3 2011
MAC Address                    : 54d4.6f88.7362
Customer Name                  :
Prim Sid                       : 18
```

```
Cable Interface                    : Cable5/0/1
MPLS-EXP                           : 0
PW TYPE                            : Ethernet
Backup enable delay                : 0 seconds
Backup disable delay               : 0 seconds
Primary peer
Peer IP Address (Active)           : 10.8.8.8
XConnect VCID                      : 97
Circuit  ID                        : Bu254:97
Local State                        : UP
Remote State                       : UP
Total US pkts                      : 418756
Total US bytes                     : 586227332
Total US pkts   discards           : 0
Total US bytes  discards           : 0
Total DS pkts                      : 417347
Total DS bytes                     : 591773612
Total DS pkts   discards           : 0
Total DS bytes  discards           : 0
```

Additional References

The following sections provide references related to the MQC QoS feature.

Related Documents

Related Topic	Document Title
CMTS cable commands	Cisco IOS CMTS Cable Command Reference
Modular Quality of Service Command-Line Interface	Cisco IOS Quality of Service Solutions Configuration Guide, Release 12.2
IP Differentiated Services Code Point Marking	Cisco IOS Quality of Service Solutions Configuration Guide, Release 12.2
Weighted Random Early Detection	Cisco IOS Quality of Service Solutions Configuration Guide, Release 12.2
DiffServ Tunneling Modes for MPLS Networks	MPLS Design TechNotes

Standards

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

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco software 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 by this feature, and support for existing RFCs has not been modified by this feature.	—

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 MQC QoS on the Cisco CMTS Routers

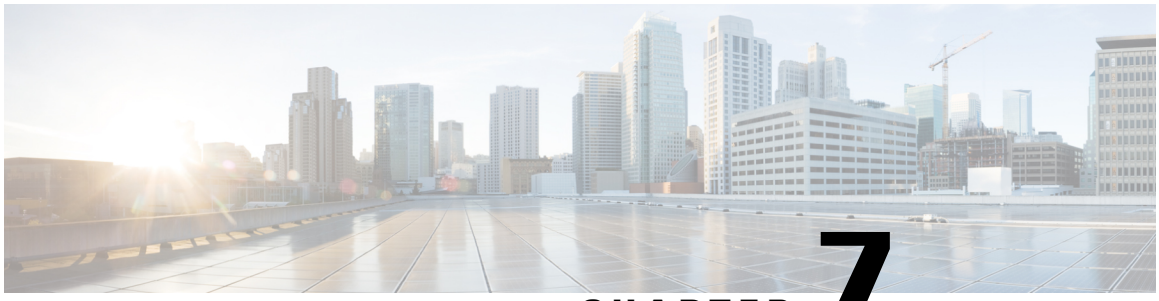
Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note The table below 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.

Table 29: Feature Information for MQC QoS on the Cisco CMTS Routers

Feature Name	Releases	Feature Information
MQC QoS on the Cisco CMTS Routers	12.2(33)SCB	MQC simplifies the configuration of QoS on the Cisco CMTS routers by defining a common command syntax and resulting set of QoS behaviors across platforms.
MQC QoS on the Cisco CMTS Routers	12.2(33)SCC	The output-rate command was introduced to limit the upstream bandwidth output rate to a smaller number than that of the physical link bandwidth.
802.1Q QoS Support on GiGE WAN	12.2(33)SCF	This feature introduces QoS service on the Gigabit Ethernet WAN interface for 802.1q packets, enabling the user to set priority bits for traffic prioritization. The following commands were introduced or modified: • **class** • **class-map** • **policy-map** • **match cos** • **set cos**
MPLS short-pipe mode	12.2(33)SCF	This feature introduces QoS service on the WAN interface for MPLS EXP bits, enabling the user to set priority bits for traffic prioritization. The following commands were introduced or modified: • **match mpls experimental topmost** • **set mpls experimental topmost** • **show policy-map interface** • **show cable l2-vpn xconnect**

Feature Name	Releases	Feature Information
Input MQC Support on the Cable Interfaces	12.2(33)SCG	This feature enables you to differentiate upstream traffic on cable bundle interface and set MPLS EXP bits without changing the ToS and DSCP value of IP packets. The following sections provide information about this feature: • Input MQC Support on the Cable Bundle Interfaces , on page 124 • Configuring Input MQC Support on the Cable Bundle Interfaces, on page 140 • Example: Configuring Input MQC Support on the Cable Bundle Interfaces, on page 144



CHAPTER 7

Service Flow Admission Control for the Cisco CMTS Routers

First Published: February 14, 2008

Last Updated: November 29, 2010

Note Cisco IOS Release 12.2(33)SCA integrates support for this feature on the Cisco CMTS routers. This feature is also supported in Cisco IOS Release 12.3BC, and this document contains information that references many legacy documents related to Cisco IOS 12.3BC. In general, any references to Cisco IOS Release 12.3BC also apply to Cisco IOS Release 12.2SC.

This document describes the topics, advantages, configuration, and monitoring capabilities of Service Flow Admission Control (SFAC) on the Cisco CMTS.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see 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 document.

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

Contents

- Feature Information for SFAC for the Cisco Cable Modem Termination System, page 196

Prerequisites for SFAC for the Cisco CMTS Routers

The Service Flow Admission Control (SFAC) feature is supported on the Cisco CMTS routers in Cisco IOS Release 12.3BC and 12.2SC. Table below shows the hardware compatibility prerequisites for this feature.

Table 30: SFAC Hardware Compatibility Matrix

CMTS Platform	Processor Engine	Cable Interface Cards
Cisco uBR10012 Universal Broadband Router	Cisco IOS Release 12.3(21)BC and later releases • PRE-1 • PRE-2 Cisco IOS Release 12.2(33)SCA and later releases • PRE-2 Cisco IOS Release 12.2(33)SCB and later releases • PRE-4 Cisco IOS Release 12.2(33)SCC and later releases • PRE-2 • PRE-4 Cisco IOS Release 12.2(33)SCH and later releases • PRE5	Cisco IOS Release 12.3(21)BC and later releases • Cisco uBR10-MC5X20S/U/H Cisco IOS Release 12.2(33)SCA and later releases • Cisco uBR10-MC5X20S/U/H Cisco IOS Release 12.2(33)SCC and later releases • Cisco uBR10-MC5X20S/U/H • Cisco uBR-MC20X20V Cisco IOS Release 12.2(33)SCE and later releases • Cisco uBR-MC3GX60V [18]

CMTS Platform	Processor Engine	Cable Interface Cards
Cisco uBR7246VXR Universal Broadband Router	Cisco IOS Release 12.3(21)BC and later releases • NPE-G1 Cisco IOS Release 12.2(33)SCA and later releases • Cisco uBR7246VXR Universal Broadband Router only • NPE-G1 • NPE-G2 Cisco IOS Release 12.2(33)SCD and later releases • NPE-G2	Cisco IOS Release 12.3(21)BC and later releases • Cisco uBR-MC28U/X • Cisco uBR-MC16U/X Cisco IOS Release 12.2(33)SCA and later releases • Cisco uBR-MC28U/X • Cisco uBR-MC16U/X Cisco IOS Release 12.2(33)SCD and later releases • Cisco uBR-MC88V[19] **Note** Cisco uBR-MC88V is supported only on Cisco IOS Release 12.2(33)SCD and later releases.
Cisco uBR7225VXR Universal Broadband Router	Cisco IOS Release 12.2(33)SCA and later releases • NPE-G1 Cisco IOS Release 12.2(33)SCD and later releases • NPE-G2	Cisco IOS Release 12.2(33)SCA and later releases • Cisco uBR-E-28U • Cisco uBR-E-16U • Cisco uBR-MC28U/X • Cisco uBR-MC16U/X Cisco IOS Release 12.2(33)SCD and later releases • Cisco uBR-MC88V

18 Cisco uBR3GX60V cable interface line card is not compatible with PRE2. You must use PRE4 with the Cisco uBR3GX60V cable interface line card.
19 Cisco uBR-MC88V cable interface line card is not compatible with NPE-G1. You must use NPE-G2 with the Cisco uBR-MC88V cable interface line card.

Restrictions for SFAC

SFAC in Cisco IOS Release 12.3(21)BC and 12.2(33)SC follows these general factors when implementing on the Cisco CMTS:

- Configure SFAC before admitting any static or dynamic service flows. The best option is to have the configuration in place during startup time, or before the interface is up.

- SFAC in Cisco IOS Release 12.3(21)BC and Cisco IOS Release 12.2(33)SC supports the following resource monitoring on the Cisco CMTS:
  - Upstream and downstream bandwidth on the Cisco CMTS
  - CPU utilization and memory resources on the Cisco uBR10012, Cisco uBR7246VXR, and Cisco uBR7225VXR router chassis (Cisco uBR10-MC5X20U and Cisco uBR-MC88V broadband processing engines)
- SFAC does not support WAN bandwidth monitoring for the Cisco uBR10012, Cisco uBR7246VXR, and Cisco uBR7225VXR routers.

Information About SFAC

This section describes DOCSIS topics and configuration options supported on the Cisco CMTS for SFAC.

Overview of SFAC for the Cisco CMTS

SFAC on the Cisco CMTS is a mechanism that gracefully manages service flow admission requests when one or more resources are not available to process and support the incoming service request. Lack of such a mechanism not only causes the new request to fail with unexpected behavior but could potentially cause the flows that are in progress to have quality related problems. SFAC monitors such resources constantly, and accepts or denies requests depending on the resource availability.

SFAC enables you to provide a reasonable guarantee about the Quality of Service (QoS) to subscribers at the time of call admission, and to enable graceful degradation of services when resource consumption approaches critical levels. SFAC reduces the impact of unpredictable traffic demands in circumstances that would otherwise produce degraded QoS for subscribers.

SFAC uses two event types for resource monitoring and management—cable modem registration and dynamic service (voice call) requests. When either of these two events occurs on the Cisco CMTS, SFAC verifies that the associated resources conform to the configured limits prior to admitting and supporting the service call request.

SFAC is not a mechanism to apply QoS to the traffic flows. Scheduling and queuing are some of the mechanisms used for implementing the QoS. The QoS is applied on per packet basis. SFAC checks are performed before the flow is admitted.

SFAC in Cisco IOS Release 12.3(21)BC monitors the following resources on the Cisco CMTS.

- *CPU utilization* —SFAC monitors CPU utilization on the Cisco CMTS, and preserves QoS for existing service flows when new traffic would otherwise compromise CPU resources on the Cisco CMTS.
- *Memory resource utilization (I/O, Processor, and combined total)* —SFAC monitors one or both memory resources and their consumption, and preserves QoS in the same way as with CPU utilization.
- *Bandwidth utilization for upstream and downstream* —SFAC monitors upstream and downstream bandwidth utilization, and associated service classes, whether for data or dynamic service traffic.

Note See also SFAC and Cisco CMTS Resources, on page 160.

Note SFAC begins graceful degradation of service when either a critical threshold is crossed, or when bandwidth is nearly consumed on the Cisco CMTS, depending on the resource being monitored.

SFAC enables you to configure major and minor thresholds for each resource on the Cisco CMTS. These thresholds are expressed in a percentage of maximum allowable resource utilization. Alarm traps may be sent each time a minor or major threshold is crossed for a given resource.

For system-level resources, such as CPU and memory utilization, you can configure critical thresholds in addition to the major and minor thresholds. When a critical threshold is crossed, further service requests are gracefully declined until the associated resource returns to a lower threshold level.

For upstream (US) and downstream (DS) channels, you can configure the bandwidth allocation with exclusive and non-exclusive thresholds. These thresholds can be configured for specified DOCSIS traffic types.

- Exclusive bandwidth indicates the percentage of bandwidth that is allocated exclusively for the specified traffic type. This bandwidth may not be shared with any other traffic type.
- Non-exclusive bandwidth indicates the percentage of bandwidth that is configured in addition to the exclusive bandwidth. Non-exclusive bandwidth is also configured for specific DOCSIS traffic types. Non-exclusive bandwidth is not guaranteed, and may be shared with other traffic types.
- The sum of exclusive and non-exclusive thresholds indicates the maximum bandwidth the specified traffic type may use.

SFAC and Cisco Universal Broadband Routers

SFAC on the Cisco uBR10012 Universal Broadband Router

Cisco IOS Release 12.3(21)BC and Cisco IOS Release 12.2(33)SC support SFAC on the Cisco uBR10012 router and all broadband processing engines.

Starting with Cisco IOS Release 12.2(33) SCC, the SFAC support is extended to bonded channels (wideband interface for downstream and upstream channel bonding), modular cable, and integrated cable interfaces.

SFAC on the Cisco uBR7246VXR and the Cisco uBR7225VXR Universal Broadband Routers

Cisco IOS release 12.3(21)BC and Cisco IOS release 12.2(33)SC support SFAC on the Cisco uBR7246VXRand uBR7225VXR routers.

Starting with Cisco IOS Release 12.2(33) SCC, the SFAC support is extended to bonded channels (wideband interface for downstream and upstream channel bonding), modular cable, and integrated cable interfaces.

interface for down stream and upstreamCB) as well as Modular cable and Integrated cable interfaces.

SFAC and Memory Requirements for the Cisco CMTS

SFAC for the Cisco CMTS is a powerful feature that maintains Quality of Service (QoS) on the Cisco CMTS and enforces graceful degradation in service when attempted consumption exceeds resource availability.

Additional memory is required in the Cisco universal broadband router to maintain and store information about various scheduling types, the distribution of upstream or downstream traffic, and associated resource

check processes. For complete information about memory requirements and Cisco IOS Release 12.3(21)BC, refer to the corresponding release notes for your product:

- *Release Notes for Cisco uBR10012 Universal Broadband Router for Cisco IOS Release 12.3 BC*

http://www.cisco.com/en/US/docs/cable/cmts/ubr10012/release/notes/12_3bc/ubr10k_123bc_rn.html

- *Release Notes for Cisco uBR7200 Series for Cisco IOS Release 12.3 BC*

http://www.cisco.com/en/US/docs/cable/cmts/ubr7200/release/notes/12_3bc/123BCu72.html

- *Release Notes for Cisco Universal Broadband Routers in Cisco IOS Release 12.2SC*

http://www.cisco.com/en/US/partner/products/hw/cable/ps2209/prod_release_notes_list.html

SFAC and Cisco CMTS Resources

SFAC with Cisco IOS Release 12.3(21)BC implements graceful QoS policies for the following resources of the Cisco CMTS:

System-Level Resources—Impact All Cisco CMTS Functions

- CPU utilization on route processor or broadband processing engine (BPE) modules
- I/O memory on route processor or broadband processing engine modules
- Processor memory

Bandwidth-Level Resources—Impact Traffic Per Interface or Per Port

- Downstream DOCSIS 1.1 bandwidth with QoS support on Cisco cable interface line cards or BPEs
- Upstream DOCSIS 1.1 bandwidth with QoS support on Cisco cable interface line cards or BPEs

Cisco IOS release 12.3(21)BC supports the following resources for the following Cisco CMTS routers:

Cisco uBR10012 Router Resources

- Cisco uBR Route Processor
  - CPU Utilization
  - Processor Memory
  - I/O Memory
- Cisco uBR Cable Interface Line Card
  - Downstream Bandwidth
  - Upstream Bandwidth

Cisco uBR7246VXR Router Resources with the Cisco MC28U Cable Interface Line Card

- Cisco uBR Route Processor
  - CPU Utilization
  - Processor Memory
  - I/O Memory
- Cisco uBR Cable Interface Line Card
  - Downstream Bandwidth
  - Upstream Bandwidth

Cisco uBR7246VXR Router Resources without the Cisco MC28U Cable Interface Line Card

- Network Processing Engine
  - CPU Utilization
  - Processor Memory
  - I/O Memory
  - Downstream Bandwidth
  - Upstream Bandwidth

Cisco uBR7246VXR Router Resources with the Cisco MC88V Cable Interface Line Card

- Cisco uBR Router Processor
  - CPU Utilization
  - Processor Memory
  - I/O Memory
- Cisco uBR Cable Interface Line Card
  - Downstream Bandwidth
  - Upstream Bandwidth

Cisco uBR7246VXR Router Resources without the Cisco MC88V Cable Interface Line Card

- Network Processing Engine
  - CPU Utilization
  - Processor Memory
  - I/O Memory
  - Downstream Bandwidth

- Upstream Bandwidth

Cisco uBR7225VXR Router Resources with the Cisco MC28U Cable Interface Line Card

- Cisco uBR Router Processor
  - CPU Utilization
  - Processor Memory
  - I/O Memory
- Cisco uBR Cable Interface Line Card
  - Downstream Bandwidth
  - Upstream Bandwidth

Cisco uBR7225VXR Router Resources without the Cisco MC28U Cable Interface Line Card

- Network Processing Engine
  - CPU Utilization
  - Processor Memory
  - I/O Memory
  - Downstream Bandwidth
  - Upstream Bandwidth

Cisco uBR7225VXR Router Resources with the Cisco MC88V Cable Interface Line Card

- Cisco uBR Router Processor
  - CPU Utilization
  - Processor Memory
  - I/O Memory
- Cisco uBR Cable Interface Line Card
  - Downstream Bandwidth
  - Upstream Bandwidth

Cisco uBR7225VXR Router Resources without the Cisco MC88V Cable Interface Line Card

- Network Processing Engine
  - CPU Utilization
  - Processor Memory

- I/O Memory
- Downstream Bandwidth
- Upstream Bandwidth

For more information, see the How to Configure, Monitor, and Troubleshoot Service Flow Admission Control, on page 165.

SFAC and CPU Utilization

CPU utilization is defined and monitored either as a five-second or a one-minute average. Both averages cannot be configured at the same time for any given resource. For CPU utilization, you can set minor, major, and critical threshold levels.

For additional information, refer to the Configuring SFAC Based on CPU Utilization, on page 167.

SFAC and Memory Utilization

SFAC can define up to three different memory options on the Cisco CMTS:

- IO memory - Current available (free) I/O memory
- Processor memory - Current available processor memory
- Both - Combined (IO and processor) memory that are available on the router

Memory resources are similar to CPU utilization, in that you can set minor, major, and critical threshold levels. Memory-based SFAC is supported for memory on the main CPU in Cisco IOS Release 12.3(21)BC, and not for the broadband processing engine line card memory.

For additional information, refer to the Configuring SFAC Based on Memory Resources, on page 169.

SFAC and Upstream or Downstream Bandwidth Utilization

SFAC allows you to control the bandwidth usage for various DOCSIS traffic types or application types. The application types are defined by the user using a CLI to categorize the service flow.

Categorization of Service Flows

The SFAC feature allows you to allocate the bandwidth based on the application types. Flow categorization allows you to partition bandwidth in up to eight application types or buckets. The composition of a bucket is defined by the command-line interface (CLI), as is the definition of rules to categorize service flows into one of these eight application buckets. Various attributes of the service flow may be used to define the rules.

For flows created by PacketCable, the following attributes may be used:

- The priority of the Packetcable gate associated with the flow (high or normal)

For flows created by PacketCable MultiMedia (PCMM), the following attributes may be used:

- Priority of the gate (0 to 7)

- Application type (0 to 65535)

The scheduling type for Upstream flows uses the following attribute type:

- Service class name

Before a service flow is admitted, it is passed through the categorization routine. Various attributes of the service flow are compared with the user-configured rules. Based on the match, the service flow is labeled with application type, from 1 to 8. The bandwidth allocation is then performed per application type.

Before a service flow is admitted, it is categorized based on its attributes. The flow attributes are compared against CLI-configured rules, one bucket at a time. If a match is found for any one of the rules, the service flow is labeled for that bucket, and no further check is performed.

Bucket 1 rules are scanned first and bucket 8 rules are scanned last. If two different rules match two different buckets for the same service flow, the flow gets categorized under the first match. If no match is found, the flow is categorized as Best Effort (BE) and the bucket with best effort rule is labelled to the flow. By default, the BE bucket is bucket 8.

Thresholds for Upstream or Downstream Bandwidth

SFAC monitors upstream or downstream bandwidth consumption with minor, major, and critical thresholds. SFAC generates alarm traps when bandwidth consumption crosses minor and major thresholds. For additional information, refer to the How to Configure, Monitor, and Troubleshoot Service Flow Admission Control, on page 165.

Exclusive and Non-Exclusive Bandwidth Thresholds

In addition to minor and major thresholds, SFAC also allows configuration of exclusive or non-exclusive thresholds.

- *Exclusive* bandwidth thresholds, for the upstream or downstream bandwidth, define a given percentage of the total (100%) bandwidth, and dedicate it to a specific traffic type.
- *Non-exclusive* bandwidth thresholds can be shared with multiple traffic types. Non-exclusive bandwidth is typically used by Best Effort traffic, yet remains available to other traffic types when required.

When the traffic usage exceeds the exclusive threshold, SFAC checks if there is any non-exclusive bandwidth available. Any new service request is permitted only if sufficient non-exclusive bandwidth is available.

Comparing SFAC with Prior Admission Control

The prior Admission Control feature on the Cisco CMTS was introduced in Cisco IOS Release 12.3(13a)BC. This prior version of Admission Control allows you to set minor, major, exclusive and non-exclusive thresholds. This topic lists changes introduced for SFAC in Cisco IOS Release 12.3(21)BC, and identifies which part of the functionality is changed and which functionality is preserved.

Note The configuration, monitoring, and debugging commands used for the original Admission Control feature are not supported for the SFAC bucket scheme.

- SFAC retains the prior Admission Control concept of thresholds. SFAC enables configuration of major, minor, exclusive and non-exclusive thresholds. However, SFAC is *distinct and unique in that the thresholds are applied per application bucket, numbered 1 to 8.*
- For downstream service flows, the prior Admission Control feature permitted bandwidth allocation for only data and voice traffic, and only PacketCable voice was recognized. SFAC uniquely allows bandwidth allocation per application bucket. As with Admission Control, however, SFAC allocates bandwidth for PacketCable voice by configuring the appropriate rules that apply to the application buckets.
- Upstream bandwidth allocation in SFAC is not based on the scheduling types, such as UGS, RTPS and so forth. SFAC newly handles upstream channels in fashion similar to downstream channels—the upstream channels also support eight application types. You may configure SFAC bandwidth allocation based on the scheduling types. You achieve the same result, however, by defining the appropriate rules to map each scheduling type into one of the eight buckets.
- SFAC monitors and manages Cisco CMTS resources according to the categorization of service flow, in which service flow policies, status and resource management are configured and processed in more categorical fashion, to include support for both PacketCable and PacketCable MultiMedia voice traffic.
- SFAC newly treats upstream and downstream traffic in the same manner and in more uniform fashion than the previous Admission Control feature.
- Exclusive and non-exclusive thresholds define resource management processes of the SFAC feature.
- SFAC introduces enhanced support for the CISCO-CABLE-ADMISSION-CTRL-MIB.

Overview of Bonding Group Admission Control

DOCSIS 3.0 introduced bonded channels or bonding groups that allow a single cable modem to send data over multiple RF channels achieving higher throughput. These bonding groups are defined for both upstream and downstream channels. Cisco IOS 12.2(33)SCC release extends the SFAC feature to support upstream and downstream bonding groups.

Bonding groups are created by combining multiple RF channels. A single RF channel may also be shared by multiple bonding groups.

Bonding group SFAC functionality allows to define the maximum reserved bandwidth for an application-type as a fraction of the available bandwidth. This fraction of the bandwidth is defined as a percentage value of the total bandwidth that can be reserved.

In order to support SFAC for bonding groups, Cisco IOS 12.2(33)SCC release introduced a new command to specify the reserve-able bandwidth available for a bonding group. Thus 100% threshold equals the bandwidth that can be reserved for a bonding group.

For additional information, refer to the Defining Maximum Reserved Bandwidth Limit, on page 173.

How to Configure, Monitor, and Troubleshoot Service Flow Admission Control

This section describes the following configuration, monitoring and troubleshooting procedures for the SFAC (SFAC) feature. Configuration procedures are optional, given default configurations are enabled in Cisco IOS

Release 12.3(21)BC. This section presents a sequence of procedures for non-default configurations, monitoring and debugging procedures that apply in default or non-default operations of SFAC.

Enabling SFAC for Event Types

SFAC can be enabled for one or more of the following events. At least one of these events must be configured for SFAC on the Cisco CMTS prior to the configuration of any additional settings:

- the registration of a cable modem
- the request for a dynamic service, such as a PacketCable or PCMM voice call

Perform these steps to configure either or both event types on the Cisco CMTS.

Note Starting from Cisco IOS Release 12.2(33)SCC, during a CM registration process, if a SFAC committed information rate (CIR) threshold value for a matching bucket is exceeded due to admission of a non-zero CIR service flow, the CM registration will be rejected by admission control with a minimum reserve rate failure. This functionality helps in avoiding CIR over-subscription that was observed in CM registration processes prior to Cisco IOS Release 12.2(33)SCC.

Before You Begin

SFAC requires that event types, traffic types and CMTS resource thresholds be configured and enabled on the Cisco CMTS.

DETAILED STEPS

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

Step 3	**cable admission-control event** { **cm-registration** | **dynamic-service** }
	
	Example:
	
	`Router(config)# cable admission-control event cm-registration`
	`Router(config)# cable admission-control event dynamic-service`
		Sets the event type on the Cisco CMTS when SFAC performs resource monitoring and management. At least one of the following keywords must be used, and both can be set:
		
		• **cm-registration—**Sets SFAC checks to be performed when a cable modem registers. If there are insufficient resources at the time of registration, the cable modem is not allowed to come online.
		
		• **dynamic-service—**Sets SFAC checks to be performed when a dynamic service, such as a voice call, is requested.

	Command or Action	Purpose
		Note The Cisco CMTS displays a warning message if any one of the event type is disabled.
Step 4	**Ctrl-Z** **Example:** `Router(config-if)# Ctrl^Z`	Returns to Privileged EXEC mode.

What to Do Next

Once configured, event types and SFAC event activity on the Cisco CMTS can be reviewed using the following two commands:

- **debug cable admission-control** *options*
- **show cable admission-control**

If the resources to be monitored and managed by SFAC are not yet configured on the Cisco CMTS, refer to the additional procedures in this document for information about their configuration.

Configuring SFAC Based on CPU Utilization

SFAC allows you to configure minor, major and critical thresholds for CPU utilization. The thresholds are specified as percentage of CPU utilization. When the an event such as cable modem registration or dynamic service takes place, and the CPU utilization is greater than the major or minor threshold, an alarm is generated. If it is greater than the critical threshold, the new service is gracefully declined.

SFAC enforces threshold levels in one of two ways. The Cisco CMTS supports both enforcement methods, but both cannot be configured at the same time.

- cpu-5sec—This finest-level setting configures the Cisco CMTS to reject new requests when the cpu-5sec utilization has exceeded the configured critical threshold. This protects any time-sensitive activities on the router. SFAC takes action on the router when a new request might otherwise exceed the configured CPU threshold level.

Note When CPU utilization exceeds the critical threshold, new requests for dynamic service flow creation for packetcable are rejected. However, new requests for CM registration will still be accepted as long as bandwidth thresholds are not crossed.

- cpu-avg—This normal-level setting is a CPU utilization average, enforced by sampling the CPU utilization at much lower frequency and calculating an exponentially weighted average. SFAC takes action on the router when a new service request might otherwise exceed the configured CPU peak threshold level.

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	[**no**] **cable admission-control** {**cpu-5sec** | **cpu-avg**} **minor** *num1* **major** *num2* **critical** *num3* **Example:** `Router# no cable admission-control cpu-avg minor 60 major 70 critical 80`	Configures CPU memory thresholds on the Cisco CMTS for SFAC. • **cpu-5sec—**average CPU utilization over a period of five seconds. • **cpu-avg—**average CPU utilization over a period of one minute. • **minor***num1* **—**Specifies the minor threshold level, where *num1* is a percentage and can be an integer between 1 and 100. • **major***num2* **—**Specifies the major threshold level, where *num2* is a percentage and can be an integer between 1 and 100. • **critical***num3* **—**Specifies the critical threshold level, where *num3* is a percentage and can be an integer between 1 and 100. There are no default values for this command. **Note** **cpu-5sec** and **cpu-avg** cannot be configured at the same time.
Step 4	**Ctrl-Z** **Example:** `Router(config-if)# Ctrl^Z`	Returns to Privileged EXEC mode.

What to Do Next

Note When the minor value (*num1*) is crossed, then an alarm (trap) is sent. When the major value (*num2*) is crossed, then another alarm (trap) is sent. When the critical value (*num3*) is crossed, then the request is gracefully declined.

Note The threshold counters are set to zero when the resource is re-configured.

Note The minor threshold should be less than the major threshold, and the major threshold must be less than the critical threshold.

Configuring SFAC Based on Memory Resources

Three different memory resource options can be configured on the Cisco CMTS:

- IO memory - Current available (free) I/O memory
- Processor memory - Current available processor memory
- Both - Combined (IO and processor) memory that are available on the router

Memory-based SFAC is supported for memory on the main CPU in Cisco IOS Release 12.3(21)BC, and not for the broadband processing engine line card memory. As with CPU utilization, you can set minor, major, and critical threshold levels.

Note When memory utilization exceeds the critical threshold, new requests for dynamic service flow creation for packetcable are rejected. However, new requests for CM registration will still be accepted as long as bandwidth thresholds are not crossed.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configureterminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	[**no**] **cable admission-control** { **io-mem** | **proc-mem** | **total-memory**} **minor** *num1* **major** *num2* **critical** *num3* **Example:** `Router# no cable admission-control io-mem minor 60 major 70 critical 80`	Configures CPU memory thresholds on the Cisco router. There are no default values for this command. **Note** All three memory threshold levels can and should be configured.
Step 4	Ctrl-Z **Example:** `Router(config-if)# Ctrl^Z`	Returns to Privileged EXEC mode.

What to Do Next

Note When the minor value (*num1*) is crossed, then an alarm (trap) is sent. When the major value (*num2*) is crossed, then another alarm (trap) is sent. When the critical value (*num3*) is crossed, then the request is gracefully declined.

Note The threshold counters are set to zero when the resource is re-configure.

Defining Rules for Service Flow Categorization

This procedure describes how to configure service flow categorization rules on the Cisco CMTS. This flexible procedure changes default global service flow rules with variations of the **cable application type include** command.

By default, Cisco IOS Release 12.3(21)BC enables the definition of service flows according to application or traffic type, with bucket assignments for a standard set of service flow applications.

Any one or several of these steps or commands may be used, in nearly any combination, to set or re-configure SFAC on the Cisco CMTS.

Note Application rules for SFAC are global configurations, and upstream and downstream bandwidth resources use the same sets of service flow rules.

DETAILED STEPS

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

	Command or Action	Purpose
Step 3	**cable application-type** *n* **include packetcable** { **normal** | **priority** } **Example:** `Router(config)# cable application-type 5 include packetcable priority`	For PacketCable, this command variation maps PacketCable service flow attributes to the specified bucket. PacketCable service flows are associated with PacketCable gates. The gate can be normal or high-priority.

Step 4	**cable application-type** *n* **include pcmm** {**priority** *gate-priority* / **app-id** *gate-app-id* }
	
	Example:
	
	`Router(config)# cable application-type 2 include pcmm priority 7`
	`Router(config)# cable application-type 2 include pcmm app-id 152`
		For PCMM, this command variation maps PCMM service flow priority or application to the specified bucket. The PCMM gates are characterized by a priority level and by an application identifier.

Step 5	**cable application-type** *n* **include scheduling-type** *type*
	
	Example:
	
	`Router(config)# cable application-type 1 include scheduling-type ugs`
	
	`Router(config)# cable application-type 1 include scheduling-type ugs-ad`
		For DOCSIS scheduling types, this command variation binds the DOCSIS scheduling types into the designated application bucket. DOCSIS 1.1 specifies the scheduling type to bind QoS parameters to the service flows for upstream traffic.

Step 6	**cable application-type** *n* **include service-class** *service-class-name* **Example:** `Router(config)# cable application-type 1 include service-class stream1`	For service class parameters, this command variation applies a service class name to the service flows, and applies corresponding QoS parameters. DOCSIS 1.1 introduced the concept of service classes. A service class is identified by a service class name. A service class name is a string that the Cisco CMTS associates with a QoS parameter set One of the objectives of using a service class is to allow the high level protocols to create service flows with the desired QoS parameter set. Using a service class is a convenient way to bind the application with the service flows. The rules provide a mechanism to implement such binding. Note the following factors when using the command in this step: • Service classes are separately configured using the **cable service class** command to define the service flow. • A named service class may be classified into any application type. • Up to ten service class names may be configured per application types. Attempting to configure more than ten service classes prints an error message. • Use the **no cable traffic-type** command to remove the configuration of a service class before adding a new class.

	Command or Action	Purpose
Step 7	**cable application-type** *n* **include BE** **Example:** `Router# cable application-type 3 include BE`	For Best Effort service flows, this command variation elaborates on Step 3, and changes the default bucket of 8 for Best Effort service flows with non-zero Committed Information Rate (CIR). These BE service flows are often created during cable modem registration. Note that there is an alternate rule that applies to the Best Effort scheduling type. This rule is applicable only for upstream service flows, as described in an earlier step of this procedure. The BE CIR service flow rule may be applicable to both upstream and downstream. However, in the case of upstream service flows, in most cases, the same service flow may map both the rules.
Step 8	Ctrl-Z **Example:** `Router(config)# Ctrl^Z`	Returns to Privileged EXEC mode.

The following example maps high-priority PacketCable service flows into application bucket 5.

```
Router(config)# cable application-type 5 include packetcable priority
```

The following example maps normal PacketCable service flows into application bucket 1.

```
Router(config)# cable application-type 1 include packetcable normal
```

The following example maps the specified bucket number with PCMM service flow with a priority of 7, then maps an application identifier of 152 for the same bucket number:

```
Router(config)# cable application-type 2 include pcmm priority 7
Router(config)# cable application-type 2 include pcmm app-id 152
```

The following example maps both UGS and UGS-AD into bucket number 1:

```
Router(config)# cable application-type 1 include scheduling-type ugs
Router(config)# cable application-type 1 include scheduling-type ugs-ad
```

The following example maps the Best Effort CIR flows to bucket 3:

```
Router(config)# cable application-type 3 include BE
```

Naming Application Buckets

This procedure enables you to assign alpha-numeric names to six of the eight application buckets that SFAC supports. The default bucket identifiers range from 1 to 8.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configureterminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable application-type** *n***name** *bucket-name* **Example:** `Router(config)# cable application-type 7 name besteffort`	Assigns an alpha-numeric name for the specified bucket. **Note** This bucket name appears in supporting **show** and **debug** commands along with the default bucket number.
Step 4	Ctrl-Z **Example:** `Router(config)# Ctrl^Z`	Returns to Privileged EXEC mode.

Defining Maximum Reserved Bandwidth Limit

This procedure enables you to define the maximum bandwidth available for CIR reservations per bonding group for all service flows that are allowed by the Cisco CMTS. The bandwidth limit depends on the RF bandwidth percent configuration for the specific bonding group.

The max-reserved-bandwidth for WB/MC/IC interfaces have lower threshold as 1% instead of 0%. For upstream and downstream bonding the lower threshold is 0%.

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface cable** {*slot*/*port* | *slot*/*subslot* /*port* } **Example:** `Router(config)# interface cable w1/0/0:0`	(Optional) Interface configuration mode implements this feature only for the specific WB, IC, or MC interface, and upstream bonding groups. Use global configuration mode in step 4 for global configurations. If downstream thresholds are configured for the interface, then that configuration supersedes the global configuration.
Step 4	**cable admission-control max-reserved-bandwidth** *bw-in-kbps* **Example:** `Router(config-if)# cable admission-control max-reserved-bandwidth 6344`	Defines the maximum reserved bandwidth for the specific WB, IC or MC interface.
Step 5	*Ctrl-Z* **Example:** `Router(config)# Ctrl^Z`	Returns to Privileged EXEC mode.

Setting Downstream and Upstream Application Thresholds

This procedure sets downstream and upstream applications thresholds for SFAC on the Cisco CMTS. This procedure extends the previous Admission Control commands from earlier Cisco IOS releases to support additional applications in SFAC. The settings in this procedure may be applied in either global or per-interface mode for downstream and upstream applications, and may also be applied in per-upstream fashion if desired.

Precedence of These Configuration Commands

SFAC based on bandwidth can be configured at the interface or global level. For upstream bandwidth, SFAC can be configured at the per-upstream level as well.

For downstream channels, the interface-level thresholds have higher precedence over the global thresholds configured. For upstream ports, the port-level thresholds have higher precedence over interface-level thresholds; and the interface-level thresholds have higher precedence over global thresholds.

As such, if you configure both global and interface-level downstream thresholds, the interface-level thresholds are effective for that interface. In similar fashion, if you configure port-level settings and the interface-level upstream thresholds, the port-level thresholds are effective on that port. The remaining ports, with no port-level thresholds in place, use the interface-level upstream thresholds.

DETAILED STEPS

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

Step 3	**interface cable** {*slot*/*port* | *slot*/*subslot* /*port* }
	
	Example:
	
	`Router(config)# interface c5/0/1`
	`Router(config-if)#`
		(Optional). Interface configuration mode implements this feature only for the specified interface. Use global configuration mode in step 4 for global configurations.
		If downstream thresholds are configured for the interface, then that configuration supersedes global configuration.
		• *slot* —Slot where the line card resides.
		◦ Cisco uBR7225VXR router—The valid range is from 1 to 2.
		◦ Cisco uBR7246VXR router—The valid range is from 3 to 6.
		• *port*—Downstream controller number on the line card. The valid *port* values are 0 or 1.
		• *slot*/*subslot* /*port* —Designates the cable interface on the Cisco uBR10012 router.
		◦ *slot*—Slot where the line card resides. The permitted range is from 5 to 8.
		◦ *subslot*—Subslot where the line card resides. The available slots are 0 or 1.
		◦ *port*—The downstream controller number on the line card. The permitted *port* range is from 0 to 4.

Step 4	**cable admission-control ds-bandwidth bucket-no** *n* **minor** *minor-threshold* **major** *major-threshold* **exclusive** *exclusive-percentage* [**non-exclusive** *non-exclusive-percentage*] **Example:** `Router(config)# cable admission-control ds-bandwidth bucket-no 1 minor 15 major 25 exclusive 30 non-exclusive 15`	Sets minor, major and exclusive thresholds for downstream voice or data bandwidth for each or all interfaces on the Cisco CMTS. Repeat this step when setting bandwidth for multiple buckets. Global configuration mode implements this feature across the entire Cisco CMTS. Otherwise, use this command in interface configuration mode as per step 3. Bandwidth values are as follows: • **ds-bandwidth**—Sets downstream throughput thresholds. • **bucket-no** *n* —Keyword and variable select the bucket number for which this configuration applies. • n—Selects the application bucket number for which this configuration applies.

	Command or Action	Purpose
		• **minor** *minor-threshold* —Sets the minor alarm threshold. The minor-threshold value is a percentage from 1 to 100. • **major** *major-threshold*—Sets the major alarm threshold. The major-threshold value is a percentage from 1 to 100. • **exclusive** *exclusive-percentage* —Specifies the percentage of throughput reserved exclusively for this class (voice or data). The *exclusive-percentage* value is an integer between 1 and 100. No other bucket can use this throughput. • **non-exclusive***non-exclusive-percentage* —(Optional) Specifies the percentage of throughput, over and above the exclusive share, that can be used by this class. The non-exclusive-percentage value is an integer between 1 and 100. Because this throughput is non-exclusive, it can be used by other buckets as specified. **Note** CMTS supports this command on modular cable and integrated cable interfaces. The no form of this command removes downstream bandwidth configuration from the Cisco CMTS: • **nocable admission-control ds-bandwidth**

Step 5	**interface cable** {*slot*/*port* | *slot*/*subslot* /*port* }
	Example:
	`Router(config)# interface c5/0/1`
	`Router(config-if)#`
		(Optional). Interface configuration mode implements this feature only for the specified interface. Use global configuration mode for global configurations.
		• *slot* —Slot where the line card resides.
		◦ Cisco uBR7225VXR router—The valid range is from 1 to 2.
		◦ Cisco uBR7246VXR router—The valid range is from 3 to 6.
		• *port*—Downstream controller number on the line card. The valid *port* values are 0 or 1.
		• *slot* /*subslot* /*port* —Designates the cable interface on the Cisco uBR10012 router.
		◦ *slot*—Slot where the line card resides. The permitted range is from 5 to 8.
		◦ *subslot*—Subslot where the line card resides. The available slots are 0 or 1.
		◦ *port*—The downstream controller number on the line card. The permitted *port* range is from 0 to 4.

Step 6	**cable admission-control us-bandwidth bucket-no** *n* **minor** *minor-threshold* **major** *major-threshold* **exclusive** *exclusive-percentage* [**non-exclusive** *non-exclusive-percentage*]	Configures global or interface-level upstream bandwidth thresholds and exclusive or non-exclusive resources on the Cisco CMTS. If upstream thresholds are configured for the interface, then that configuration supersedes global configuration. • **us-bandwidth**—Specifies that this command is to configure the upstream bandwidth thresholds.

	Command or Action	Purpose
	Example: `Router(config)# cable admission-control us-bandwidth bucket-no 1 minor 10 major 20 exclusive 30 non-exclusive 10`	• **bucket-no** *n* —Selects the application bucket for which this configuration applies.: • **minor** *minor-threshold*—Sets the minor alarm threshold. The minor-threshold value is a percentage from 1 to 100. • **major** *major-threshold*—Sets the major alarm threshold. The major-threshold value is a percentage from 1 to 100. • **exclusive** *exclusive-percentage*—Represents the critical threshold for the upstream throughput resource. Specifies the percentage of throughput reserved exclusively for this class. The exclusive-percentage value is a range from 1 to 100. No other class can use this bandwidth. • **non-exclusive** *non-exclusive-percentage*—(Optional) Specifies the percentage of bandwidth, over and above the exclusive share, that can be used by this class. The non-exclusive-percentage value is an integer between 1 and 100. Because this bandwidth is non-exclusive, it can be used by other classes as specified. **Note** CMTS supports this command on modular cable and integrated cable interfaces.
Step 7	**interface cable** {*slot*/*port* | *slot*/*subslot* /*port* }	(Optional). Interface configuration mode implements this feature only for the specified interface. Use global configuration mode for global configurations. If downstream thresholds are configured for the interface, then that configuration supersedes global configuration.

	Example:
	`Router(config)# interface c5/0/1`
	`Router(config-if)#`
		• *slot* /*port* —Designates the cable interface on the Cisco uBR7246VXR and Cisco uBR7225VXR routers.
		• *slot*/*subslot* /*port* —Designates the cable interface on the Cisco uBR10012 router.

Step 8	**cable upstream** *n* **admission-control us-bandwidth bucket-no** *n***minor** *minor-threshold* **major** *major-threshold* **exclusive** *exclusive-percentage* [**non-exclusive** *non-exclusive-percentage*]	Configures global or interface-level upstream bandwidth thresholds and exclusive or non-exclusive resources on the Cisco CMTS. If upstream thresholds are configured for the interface, then that configuration supersedes global configuration. • **upstream**—Specifies that this command applies on per-upstream channel basis. • *n* —Specifies the upstream channel number. The traffic type takes the same values as the downstream command. • **us-bandwidth**—Specifies that this command is to configure the upstream bandwidth thresholds. • **bucket-no***n* bucket-no *n* —Selects the application bucket for which this configuration applies. • **minor** *minor-threshold* —Sets the minor alarm threshold. The minor-threshold value is a percentage from 1 to 100. • **major** *major-threshold* —Sets the major alarm threshold. The major-threshold value is a percentage from 1 to 100.
	Example: `Router(config)# cable upstream 1 admission-control us-bandwidth bucket-no 1 minor 10 major 20 exclusive 30 non-exclusive 10`	

	Command or Action	Purpose
		• **exclusive** *exclusive-percentage* —Represents the critical threshold for the upstream throughput resource. Specifies the percentage of throughput reserved exclusively for this class. The exclusive-percentage value is a range from 1 to 100. No other class can use this bandwidth. • **non-exclusive** *non-exclusive-percentage* —(Optional) Specifies the percentage of bandwidth, over and above the exclusive share, that can be used by this class. The non-exclusive-percentage value is an integer between 1 and 100. Because this bandwidth is non-exclusive, it can be used by other classes as specified.
Step 9	**Ctrl-Z** **Example:** `Router(config)# Ctrl^Z`	Returns to Privileged EXEC mode.

Preempting High-Priority Emergency 911 Calls

You may configure SFAC rules and thresholds so that the high-priority voice (911) traffic receives an exclusive share of bandwidth. Because the average call volume for Emergency 911 traffic may not be very high, the fraction of bandwidth reserved for Emergency 911 calls may be small. In the case of regional emergency, the call volume of Emergency 911 calls may surge. In this case, it may be necessary to preempt some of the normal voice traffic to make room for surging Emergency 911 calls.

The Cisco CMTS software preempts one or more normal-priority voice flows to make room for the high-priority voice flows. SFAC provides the command-line interface (CLI) to enable or disable this preemption ability.

SFAC preemption logic follows the following steps:

1. When the first pass of admission control fails to admit a high priority PacketCable flow, it checks if it is possible to admit the flow in another bucket configured for normal PacketCable calls (applicable only if the PacketCable normal and high-priority rules are configured for different buckets). If the bandwidth is available, the call is admitted in the normal priority bucket.
2. If there is no room in normal priority bucket, it preempts a normal priority PacketCable flow and admits the high priority flow in the bucket where the low priority flow was preempted.
3. If there is no normal priority flow that it can preempt, it rejects the admission for high-priority flow. This usually happens when both normal and high-priority buckets are filled with 911 flows.

This preemption is effective only for PacketCable high-priority flows.

When an upstream or downstream low-priority service flow is chosen for preemption, the corresponding service flow for the same voice call in the opposite direction gets preempted as well.

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	[**no**] **cable admission-control preempt priority-voice** **Example:** `Router(config)# no cable admission-control preempt priority-voice`	Changes the default Emergency 911 call preemption functions on the Cisco CMTS, supporting throughput and bandwidth requirements for Emergency 911 calls above all other buckets on the Cisco CMTS. The **no** form of this command disables this preemption, and returns the bucket that supports Emergency 911 calls to default configuration and normal function on the Cisco CMTS.

Step 4	**Ctrl-Z**
	
	Example:
	
	`Router(config)# Ctrl^Z`
	`Router#`
		Returns to Privileged EXEC mode.

Calculating Bandwidth Utilization

The SFAC feature maintains a counter for every US and DS channel, and this counter stores the current bandwidth reservation. Whenever a service request is made to create a new service flow, SFAC estimates the bandwidth needed for the new flow, and adds it to the counter. The estimated bandwidth is computed as follows:

- For DS service flows, the required bandwidth is the minimum reservation rate, as specified in the DOCSIS service flow QoS parameters.
- For US flows, the required bandwidth is as follows:
  - For BE flows the required bandwidth is the minimum reservation rate as specified in the DOCSIS service flow QoS parameters.
  - For UGS flows the required bandwidth is grant size times number of grants per second, as per the DOCSIS specification.
  - For RTP and RTPS flows, the required bandwidth is sum of minimum reservation rate as specified in the DOCSIS service flow QoS parameters; and the bandwidth required to schedule the request slots.

- For UGSAD flows the required bandwidth is sum of bandwidth required for payload (same as UGS flows) and the bandwidth required to schedule to request slots.

In each of the above calculations, SFAC does not account for the PHY overhead. DOCSIS overhead is counted only in the UGS and UGS-AD flows. To estimate the fraction of bandwidth available, the calculation must account for the PHY and DOCSIS overhead, and also the overhead incurred to schedule DOCSIS maintenance messages. SFAC applies a correction factor of 80% to the raw data rate to calculate the total available bandwidth.

Note For the DS and US flow in bonded channels, the maximum reserved bandwidth is the bandwidth defined for the SFAC threshold values. This value is indicated in kbps.

Monitoring and Troubleshooting Commands for SFAC

This section describes the following monitoring and troubleshooting procedures for the SFAC (SFAC) feature.

Bandwidth Validity Checks for SFAC

SFAC is based on and monitors multiple resources on the Cisco CMTS. You can configure major, minor, exclusive and non-exclusive thresholds for various traffic types. To prevent circumstances in which some SFAC configurations are inconsistent, SFAC first validates the attempted configuration, and if an error is found, SFAC prints an error message and the configuration is not set.

Before setting the threshold limits for a given resource on the Cisco CMTS, SFAC configuration should follow these important guidelines to ensure a valid configuration:

1. For the given resource, the minor threshold should be less than the major threshold, and the major threshold should be less than the exclusive or critical threshold. For example, minor threshold at 45%, major threshold at 65%, and critical threshold at 85%.
2. For downstream and upstream bandwidth, the sum of the exclusive thresholds and the maximum configured non-exclusive threshold should be less than 100%. For example, consider US bandwidth configuration for various buckets. If exclusive thresholds for buckets 1-4 were configured at 15% each, this would mean a total of 60% bandwidth is reserved exclusively for these four buckets. This leaves only 40% for any non-exclusive bandwidth. Therefore, in this case, the maximum non-exclusive thresholds that any bucket can have is 40% (100% - 60%), and should be less than 40%.

Implicit Bandwidth

You may choose not to assign any explicit thresholds to certain buckets. In this case, these buckets assume implicit thresholds. In the previous example, if you do not configure any thresholds for buckets 5-8, then those buckets assume implicit thresholds. Because 60% bandwidth is already reserved by buckets 1-4, buckets 5-8 can share the remaining 40% bandwidth. This 40% bandwidth is treated in a non-exclusive manner. This information displays in supporting **show** commands. The implicit bucket bandwidth for WB interface is 0 unlike other cable interface types where the implicit bandwidth is 100%.

If cable application type includes any multicast application ID, then CMTS expects default bucket will not accommodate multicast service flows. If no multicast application type is configured, all the multicast service flows are admitted to the default bucket 8.

Once a bucket is configured for one multicast application ID, all the subsequent multicast application IDs should be mapped to buckets other than bucket 8.

Oversubscription

Oversubscription of a given resource on the Cisco CMTS may be encountered in one of the following ways:

- Consider a situation where voice and data are both given 50% exclusive bandwidth. If a large number of cable modems register with non-zero committed information rate (CIR) service flows, this results in consuming a large fraction of the bandwidth. This situation is called oversubscription.
- Cable modem registration with CM configuration files with CIR flows may result in oversubscription. As explained above, the admission of CIR flows, even though it violates the admission control policy, can result in oversubscription.
- Enabling SFAC events after the service flows are admitted may result in oversubscription. If the SFAC check is not enabled using the cable admission-control dynamic-service command, this can result in service flows being admitted. If the thresholds are configured, the bandwidth usage may exceed its allocated share.
- Dynamically changing the thresholds can result in oversubscription. You can make changes in dynamic fashion to the threshold levels while the flows are already admitted. If the new threshold is lower than the current reservation for a given bucket, that bucket will oversubscribe its share under the new and lower threshold.
- The service flow handling method may result in oversubscription. The amount of bandwidth exceeding the allocated bandwidth is measured as "oversubscribed bandwidth". The oversubscribed bandwidth is displayed in the show cable admission-control commands. While calculating the available bandwidth for the rest of the buckets, the oversubscribed bandwidth is not taken into consideration. We calculate effective bandwidth as follows:

Effective bandwidth = current reservation - oversubscribed bandwidth

For example, referring to the starting scenario with voice and data both given 50% bandwidth, if the data usage reaches 70%, the data bucket oversubscription totals 20%. That is, the effective bandwidth for the data bucket = 70 - 20 = 50%.

Therefore, while calculating the available bandwidth for voice, full 50% bandwidth is considered available. Note that in this example, if you allow voice utilization to reach 50%, the total reservation becomes 120%. At present the Cisco CMTS platforms do not allow total reservation to exceed 100% of the available bandwidth for downstream channels; only upstream channels may exceed 100% reservation.

Displaying Application Buckets for SFAC

Cisco IOS Release 12.3(21)BC introduces the **show application-buckets** command to display default or customized SFAC settings and status on the Cisco CMTS. This command displays the bucket number and bucket name, if the latter is configured, and the associated rules for each bucket. When multiple rules are applied to one bucket, the rules display in order of priority for that bucket.

Before You Begin

This procedure presumes that SFAC is configured and operational on the Cisco CMTS.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show cable application-type** [**bucket-no** *n*] **Example:** `Router# show cable application-buckets 5`	Displays rules for any or all buckets supporting SFAC on the Cisco CMTS. The configured rules for any given bucket are displayed in order of precedence in the Rule field. • **bucket-no***n* —You may specify a specific bucket number on the Cisco CMTS to display parameters for that bucket and no others. Valid range is 1 to 8, or all buckets if no specific bucket is designated.

The following example illustrates sample output of the **show cable application-type** command.

```
Router# show cable application-type
For bucket 1, Name PktCable
     Packetcable normal priority gates
     Packetcable high priority gates
For bucket 2, Name PCMM-Vid
     PCMM gate app-id = 30
For bucket 3, Name Gaming
     PCMM gate app-id = 40
For bucket 4, Name
For bucket 5, Name
For bucket 6, Name
For bucket 7, Name
For bucket 8, Name HSD
     Best-effort (CIR) flows
```

What to Do Next

The change made with this procedure is displayed with the **show application-buckets** command.

Displaying Service Flow Reservation Levels

Cisco IOS Release 12.3(21)BC introduces a new command to display service flows, application categorizations, and bandwidth consumption on the Cisco CMTS.

Before You Begin

This procedure presumes that SFAC is configured and operational on the Cisco CMTS.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router> enable`	• Enter your password if prompted.
Step 2	**show interface cable** { *slot* / *port* | *slot* / *subslot* / *port* } **admission-control reservation** { **downstream** | **upstream** *port-no* } **Example:** `Router# show interface cable 5/1/1 admission-control reservation downstream`	Displays service flows, categorizations, and bandwidth consumption on the Cisco CMTS, for the specified interface, and the specified service flow direction. • *slot* —Slot where the line card resides. ◦ Cisco uBR7225VXR router—The valid range is from 1 to 2. ◦ Cisco uBR7246VXR router—The valid range is from 3 to 6. • *port* —Downstream controller number on the line card. The valid *port* values are 0 or 1. • *slot* / *subslot* / *port* —Designates the cable interface on the Cisco uBR10012 router. ◦ *slot* —Slot where the line card resides. The permitted range is from 5 to 8. ◦ *subslot* —Subslot where the line card resides. The available slots are 0 or 1. ◦ *port* —The downstream controller number on the line card. The permitted *port* range is from 0 to 4. • **downstream**—Displays downstream service flow information for the designated cable interface. • **upstream** —Displays upstream service flow information for the designated cable interface. The port number may be specified here for more limited display. • *port-no*—*Port number to which this destination applies; applicable if the upstream ports are configured for SFAC.*

The following example illustrates sample output and status of the SFAC feature, and the **show interface cable admission-control reservation** { **downstream | upstream** } *port-no* command.

```
Router# show interface cable 5/1/1 admission-control reservation downstream
SfId   Mac Address       Bucket    Bucket Name          State    Current Reserv
4      0000.cad6.f052       8                          act       0
88     0000.cad6.f052       8                          act       2000
6      0000.cad6.eece       8                          act       0
21     0000.cad6.eece       8                          act       2000
8      0000.cad6.eebe       8                          act       0
24     0000.cad6.eebe       8                          act       2000
10     0000.cadb.30a6       8                          act       0
27     0000.cadb.30a6       8                          act       2000
```

Displaying SFAC Configuration and Status

Cisco IOS Release 12.3(21)BC supports an enhanced command to display service flows, application categorizations, and bandwidth consumption status on the Cisco CMTS. This command also displays DS threshold values, reservations per bucket on a modular cable or interface cable or DS channel bonding.

Before You Begin

This procedure presumes that SFAC is configured and operational on the Cisco CMTS.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show cable admission-control** [**global**] [**interface** *slot/port* | *slot/subslot/port*] [**all**] **Example:** `Router# show cable admission-control interface cable 5/1/1 upstream 0`	Displays the current SFAC configuration and status on the Cisco CMTS, or on a specified interface. • **global—**(Optional) Displays the following information: ◦ Parameters that have been configured for admission control ◦ Number of requests that have crossed minor, major, and critical levels for each resource • **interface** *slot/port* | *slot/subslot/port* Option allows you to display SFAC information for the specified interface or port. This includes the following: ◦ Values for US throughput resources ◦ Values for DS throughput resources ◦ *slot/port* **—**Designates the cable interface on the Cisco uBR7246VXR and Cisco uBR7225VXR routers. ◦ *slot/subslot/port* **—**Designates the cable interface on the Cisco uBR10012 router. • **all—**Displays information for all interfaces configured for SFAC on the Cisco CMTS.

The following example illustrates further information for the SFAC feature. This example displays threshold levels and current reservation per bucket, and the oversubscribed bandwidth per bucket. Cisco IOS indicates implicitly calculated threshold with asterisk.

```
Router# show cable admission-control interface cable 5/1/1 upstream 0
Interface  Cable5/1/1
Upstream Bit Rate (bits per second) = 4096000
```

```
Resource - Upstream Bandwidth
-----------------------------
Bucket Names  Minor # of  Major # of  Excls # of  Non-Ex Curr. Curr. Conf  # of
No            Level Times Level Times Level Times Level  Resv  Ovrsb Level Rejec
1             5     1312  7     1262  45    0     0      31    0     I    36
2             0     0     0     0     0     0     6*     0     0     I     0
3             0     0     0     0     0     0     6*     0     0     I     0
4             0     0     0     0     0     0     6*     0     0     I     0
5             0     0     0     0     0     0     6*     0     0     I     0
6             0     0     0     0     0     0     6*     0     0     I     0
7             0     0     0     0     0     0     6*     0     0     I     0
8             5     31    7     29    49    11    5      79    25    I     0
```

Debugging SFAC for Different Event Types

Cisco IOS Release 12.3(21)BC supports the debugging of service flow events for SFAC on the Cisco CMTS.

Before You Begin

Default or manual configuration of the following procedure is required for using this **debug** command, with additional SFAC settings presumed, according to your requirements.

Enabling SFAC for Event Types, on page 166

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**debug cable admission-control event** **Example:** `Router# debug cable admission-control event`	Enables event-oriented troubleshooting for SFAC. Use the **no** form of this command to disable this debugging.

The following example illustrates the enabling and display of the debug cable admission-control event command.

```
Router# debug cable admission-control event
*Sep 12 23:15:22.867: Entering admission control check on PRE and it's a cm-registration
*Sep 12 23:15:22.867: Admission control event check is TRUE
```

Debugging SFAC for CPU Resources

Cisco IOS Release 12.3(21)BC supports the debugging of CPU resources configured for SFAC on the Cisco CMTS.

Before You Begin

Default or manual configuration of the following procedure is required for using this **debug** command, with additional SFAC settings presumed, according to your requirements.

Configuring SFAC Based on CPU Utilization, on page 167

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**debug cable admission-control cpu** **Example:** `Router# debug cable admission-control cpu`	Enables CPU troubleshooting processes for SFAC. Use the **no** form of this command to disable this debugging.

The following example illustrates enabling and display of the **debug cable admission-control cpu** command.

```
Router# debug cable admission-control cpu
*Sep 12 23:08:53.255: CPU admission control check succeeded
*Sep 12 23:08:53.255: System admission control check succeeded
*Sep 12 23:08:53.255: CPU admission control check succeeded
*Sep 12 23:08:53.255: System admission control check succeeded
```

Debugging SFAC for Memory Resources

Cisco IOS Release 12.3(21)BC supports the debugging of memory resources configured for SFAC on the Cisco CMTS.

Before You Begin

Default or manual configuration of the following procedure is required for using this **debug** command, with additional SFAC settings presumed, according to your requirements.

Configuring SFAC Based on Memory Resources, on page 169

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**debug cable admission-control cpu** **Example:** `Router# debug cable admission-control memory`	Enables memory troubleshooting processes for SFAC. Use the **no** form of this command to disable this debugging.

The following example illustrates the enablement and displays of the **debug cable admission-control memory** command.

```
Router# debug cable admission-control memory
*Sep 12 23:08:53.255: CPU admission control check succeeded
*Sep 12 23:08:53.255: System admission control check succeeded
*Sep 12 23:08:53.255: CPU admission control check succeeded
*Sep 12 23:08:53.255: System admission control check succeeded
```

Debugging SFAC for Downstream Bandwidth

Cisco IOS Release 12.3(21)BC supports the debugging of downstream bandwidth resources configured for SFAC on the Cisco CMTS.

Before You Begin

Default or manual configuration of the following procedure is required for using this **debug** command, with additional SFAC settings presumed, according to your requirements.

Setting Downstream and Upstream Application Thresholds, on page 174

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**debug cable admission-control ds-bandwidth** **Example:** `Router# debug cable admission-control ds-bandwidth`	Enables downstream throughput troubleshooting processes for SFAC. Use the **no** form of this command to disable this debugging.

The following example illustrates the enablement and displays of the **debug cable admission-control ds-bandwidth** command.

```
Router# debug cable admission-control ds-bandwidth
```

```
Oct  8 23:29:11: Failed to allocate DS bandwidth for
CM 0007.0e01.1db5 in adding a new service entry
```

Debugging SFAC for Upstream Throughput

Cisco IOS Release 12.3(21)BC supports the debugging of upstream bandwidth resources configured for SFAC on the Cisco CMTS.

Before You Begin

Default or manual configuration of the following procedure is required for using this **debug** command, with additional SFAC settings presumed, according to your requirements.

Setting Downstream and Upstream Application Thresholds, on page 174

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**debug cable admission-control us-bandwidth** **Example:** `Router# debug cable admission-control us-bandwidth`	Enables enable upstream throughput troubleshooting processes for SFAC. Use the **no** form of this command to disable this debugging.

The following example illustrates the enablement and displays of the **debug cable admission-control us-bandwidth** command.

```
Router# debug cable admission-control us-bandwidth
Router#
Oct  8 23:29:11: Failed to allocate US bandwidth for
CM 0007.0e01.9b45 in adding a new service entry
```

Debugging Flow Categorization for SFAC

Cisco IOS Release 12.3(21)BC introduces a new **debug** command that accounts for the bucket-flow scheme of SFAC. This **debug** command displays service flow categorization results—when a service flow is classified, the **debug** command displays the application by which it was categorized, along with which rule is matched.

Before You Begin

Default or manual configuration of the following procedure is required for using this **debug** command, with additional SFAC settings presumed, according to your requirements.

Defining Rules for Service Flow Categorization, on page 170

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**debug cable admission-control flow-categorization** **Example:** `Router# debug cable admission-control flow-categorization`	Enables debugging of service flow categorization processes for SFAC. This command displays service flow categorizations currently enabled on the Cisco CMTS. Use the **no** form of this command to disable this debugging.

Below is a shortened example of the information displayed when the **debug cable admission-control flow-categorization** command is enabled on the Cisco CMTS. This command displays interface-level information.

```
Router# debug cable admission-control flow-categorization
int ca 5/1/1 sfid 55 identified as video pcmm priority 6 matched.
```

Debugging Wideband Interfaces for SFAC

Cisco IOS Release 12.2(33)SCC supports debugging of the wideband interface for SFAC on the Cisco CMTS using a new **debug** command.

Before You Begin

Default or manual configuration of the following procedure is required for using this **debug** command, with additional SFAC settings presumed, according to your requirements.

Defining Rules for Service Flow Categorization, on page 170

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**debug cable wbcmts admission-control** **Example:** `Router# debug cable wbcmts admission-control`	Enables debugging of the wideband interface admission control on the Cisco CMTS. Use the **no** form of this command to disable this debugging.

The following example shows a sample output of the **debug cable wbcmts admission-control** command.

```
Router> enable
Router# debug cable wbcmts admission-control
Oct  5 15:43:32.230: Wideband-Cable1/0/0:0    NB 6/1/0 app 1, nb cir = 0, total bkt cir =
0
Oct  5 15:43:32.230:  total_cfg_non_ex_pct: 0, prev_bkt_resv: 0
Oct  5 15:43:32.230: total_cfg_ex_pct: 100, total_cfg_non_ex_pct: 0, total_ex_cir_cfg_bps:
 72000000, total bkt resv 0
Oct  5 15:43:32.230: Wideband-Cable1/0/0:0    app 1, per_bucket_cfg_excl_bps: 0,
max_non_ex_bps: 0,
total_nonex_resvd_bps: 0, bkt type: 0
```

What to Do Next

Refer to additional non-default procedures in this document, or to the following procedures for monitoring or troubleshooting SFAC on the Cisco CMTS:

- Displaying Application Buckets for SFAC, on page 181
- Displaying Service Flow Reservation Levels, on page 182
- Debugging SFAC for Different Event Types, on page 185
- Debugging SFAC for CPU Resources, on page 185
- Debugging SFAC for Memory Resources, on page 186
- Debugging SFAC for Downstream Bandwidth, on page 187
- Debugging SFAC for Upstream Throughput, on page 188
- Debugging Flow Categorization for SFAC, on page 188

Troubleshooting Tips

SFAC supports **debug** and **show** commands for monitoring and troubleshooting functions on the Cisco CMTS. Refer to the following procedures:

If SFAC checks fail for memory resources, refer to the following sections for additional information about memory thresholds, events and configuration:

- **debug cable admission-control**
- **show cable admission-control**
- How to Configure, Monitor, and Troubleshoot Service Flow Admission Control, on page 165

Configuration Examples for SFAC

This section describes solutions-level examples of the SFAC feature on the Cisco CMTS. This section illustrates the functioning of SFAC in default or non-default but properly operational configurations. This section presumes the proper use of configuration and monitoring procedures and commands described elsewhere in this document.

This section contains the following examples to illustrate SFAC:

Example: SFAC Configuration Commands

In this section of configuration examples, the following SFAC parameters are set on the Cisco CMTS:

- All the packetcable flows are mapped into bucket 1.
- The BE service flows are mapped into bucket 8.

The following configuration commands enable these settings:

- To map the packetcable voice flows, these commands are used:

```
cable application-type 1 include packetcable normal
cable application-type 1 include packetcable priority
cable application-type 1 name PktCable
```

- To map the BE flows into bucket 8, these commands are used.

```
cable application-type 8 name HSD
cable application-type 8 include best-effort
```

- Given the above configurations, you may also control bandwidth allocation to a PCMM streaming video application. The streaming video application is identified by the PCMM application ID 35. The following commands implement this configuration:

```
cable application-type 2 name PCMM-Vid
cable application-type 2 include pcmm app-id 35
```

- These configurations may be verified on the Cisco CMTS using the following **show** commands:

```
Router# show cable application-type
For bucket 1, Name PktCable
     Packetcable normal priority gates
     Packetcable high priority gates
For bucket 2, Name PCMM-Vid
     PCMM gate app-id = 30
For bucket 3, Name Gaming
     PCMM gate app-id = 40
For bucket 4, Name
For bucket 5, Name
For bucket 6, Name
For bucket 7, Name
For bucket 8, Name HSD
     Best-effort (CIR) flows
```

These above configuration examples might be omitted or changed, but the remaining examples in this section presume the above configurations.

Example: SFAC for Downstream Traffic

This example presumes that you have configured the rules according to the commands illustrated at the start of this section. All the voice flows in bucket 1. All the CIR data flows are categorized in bucket 8.

This example illustrates a sample configuration for SFAC with downstream traffic. In this example, if voice traffic exceeds 30% bandwidth consumption, additional voice flows are denied.

- 30% downstream throughput is reserved exclusively for voice traffic.
- Minor and major alarms for voice traffic to be generated at 15% and 25% respectively.

The following Cisco IOS command implements this configuration:

```
Router(config)# cable admission-control ds-bandwidth bucket-no 1 minor 15 major 25 exclusive
 30
```

In this example, the voice flows are rejected when the bandwidth usage of the flows exceeds 30%.

In addition, you can allow for some flexibility by allowing flows to exceed their exclusive share, and to consume up to 50% of the total downstream throughput (30% + 20%). The following command accomplishes this:

```
Router(config)# cable admission control downstream bucket-no 1 minor 15 major 25 exclusive
 30 non-exclusive 20
```

With this previous command, the bucket 1 flows are rejected when the voice usage exceeds 50% (30% + 20%).

Similarly you can configure data thresholds as follows:

```
Router(config)# cable admission control bucket-no 8 minor 15 major 25 exclusive 50
non-exclusive 10
```

With the configuration commands as above, the following multi-stage scenario illustrates how the lending and borrowing of throughput is achieved in the presence of multiple traffic classes.

Stage I—Initial Throughput Allocations

Assume downstream throughput distribution is as follows:

- Downstream voice threshold is configured at 30%, with current consumption at 20%.
- Downstream data threshold is configured at 50%, with current consumption at 40%.

Table below summarizes this throughput distribution:

Table 31: Throughput Allocation and Consumption for Stage 1 of this Example

Throughput Type	Exclusive Threshold	Non-exclusive Threshold	% Consumed	% Available
Bucket-no 1 (Voice)	30%	20%	20%	30%
Bucket-no 8 (Data)	50%	10%	40%	20%
Uncategorized Traffic			0%	40% (100% -20% - 40%)

Stage 2—Voice Traffic Exceeds 30% Exclusive Throughput

Now assume conditions change as follows:

- Voice throughput increases to 40%. Voice obtains 10% from the non-exclusive share.
- Data (Best Effort CIR) throughput usage increases to 50%, consuming all exclusive data throughput.
- Bandwidth available for uncategorized traffic shrinks to 30%.

Table below summarizes this throughput distribution:

Table 32: Throughput Allocation and Consumption for Stage 1 of this Example

Throughput Type	Exclusive Threshold	Non-exclusive Threshold	% Consumed	% Available
Voice	30%	20%	40% (30% + 10%)	10%
Data	50%	10%	50%	10%
Uncategorized Traffic			0%	10% (100% - 40% - 50%)

Step 3—Bandwidth Consumption Increases by 10%

Now assume that data throughput usage increases by 10% for a new consumption total of 60%, and voice usage remains same. This consumes all remaining non-exclusive bandwidth from Best Effort.

Table below summarizes this throughput distribution:

Table 33: Throughput Allocation and Consumption for Stage 1 of this Example

Throughput Type	Exclusive Threshold	Non-exclusive Threshold	% Consumed	% Available
Voice	30%	20%	40% (30% + 10%)	0%
Data	50%	10%	60% (50% + 10%)	0%
Uncategorized Traffic				0% (100%-40%-60%)

Note For the first time in this multi-stage example, bandwidth consumption on the Cisco CMTS has reached 100%, and there is no bandwidth available for uncategorized flows after the events of Stage 3.

Example: SFAC for Bonding Groups

This example shows configuration of SFAC with the following line card configurations:

- Modular cable interface with 3 Gigabit Ethernet cards
- Wideband interface with 3 Gigabit Ethernet cards
- MC20x20 line card with 3Gigabit Ethernet cards

```
Router(config-if)#cable application-type 1 include scheduling-type ugs
Router(config-if)#cable application-type 1 include packetcable normal
Router(config-if)#cable application-type 1 include packetcable high-priority
Router(config-if)#cable application-type 1 include pcmm priority 2
Router(config-if)#cable application-type 2 include BE
Router(config-if)#cable application-type 3 include multicast 12
!
Router(config)#interface Wideband-Cable1/0/0:0
 cable bundle 2
 cable bonding-group-id 1
 cable rf-channel 1
 cable rf-channel 2
 cable rf-channel 3 bandwidth-percent 1
Router(config-if)#cable admission-control max-reserved-bandwidth 60302
Router(config-if)#cable admission-control ds-bandwidth 1 minor 10 major 20 exclusive 30
non-exclusive 40
Router(config-if)#cable admission-control ds-bandwidth 2 minor 5 major 10 exclusive 15
non-exclusive 25
```

Additional References

The following topics provide references related to SFAC for the Cisco CMTS.

Related Documents

Related Topic	Document Title
Cisco CMTS Cable Commands	Cisco CMTS Cable Command Reference
DOCSIS 1.1 for the Cisco CMTS Routers	*DOCSIS 1.1 for the Cisco CMTS* http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/cmts_docsis11.html
CISCO-CABLE-ADMISSION-CTRL-MIB for the Cisco Cable Modem Termination System	*Cisco CMTS Universal Broadband Series Router MIB Specifications Guide 12.2 SC* http://www.cisco.com/en/US/docs/cable/cmts/mib/12_2sc/reference/guide/ubrmibv5.html

Standards

Standard	Title
CableLabs™ DOCSIS 1.1 specifications	http://www.cablelabs.com/cablemodem/
CableLabs™ PacketCable specifications	http://www.cablelabs.com/packetcable/
CableLabs™ PacketCable MultiMedia specifications	http://www.cablelabs.com/packetcable/specifications/multimedia.html

MIBs

MIB	MIBs Link
MIBs for the Cisco Cable Modem Termination System	*Cisco CMTS Universal Broadband Series Router MIB Specifications Guide 12.2 SC* http://www.cisco.com/en/US/docs/cable/cmts/mib/12_2sc/reference/guide/ubrmibv5.html
MIBs Supporting Cisco IOS	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

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for SFAC for the Cisco Cable Modem Termination System

Table below lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

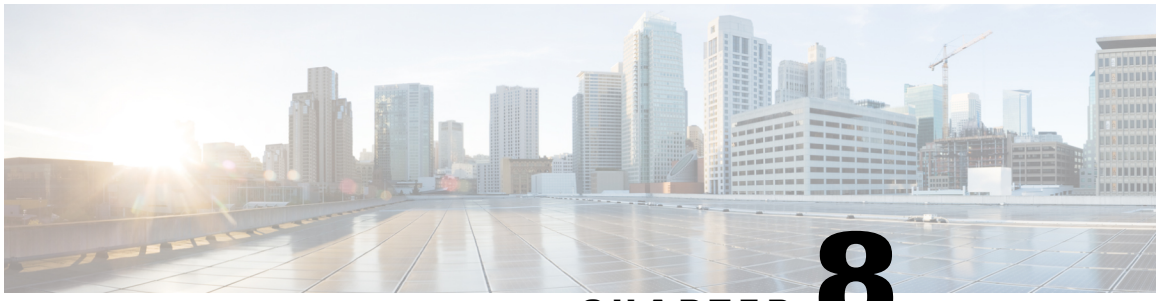
Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on Cisco.com is not required.

Note Table 34: Feature Information for Admission Control , on page 196 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 34: Feature Information for Admission Control

Feature Name	Releases	Feature Information
Admission Control for the Cisco CMTS Routers	12.3(13a)BC	The Service Flow Admission Control feature was introduced on the Cisco uBR10012 and Cisco uBR7246VXR universal broadband routers.
Service Flow Admission Control for the Cisco CMTS Routers	12.3(21)BC	This feature was introduced on the Cisco uBR10012 and the Cisco uBR7246VXR universal broadband routers. It supersedes the previous form of admission control supported on these CMTSs.
Service Flow Admission Control for the Cisco CMTS Routers	12.2(33)SCA	This feature was integrated into Cisco IOS Release 12.2(33)SCA. Support for the Cisco uBR7225VXR Universal Broadband Router was added.
Service Flow Admission Control for Bonding Groups.	12.2(33)SCC	The Service Flow Admission Control feature has been updated to extend the functionality to US and DS bonding groups to Cisco uBR10012 routers.

Feature Name	Releases	Feature Information
Service Flow Admission Control for Bonding Groups.	12.2(33)SCD	The Service Flow Admission Control feature has been updated to extend the functionality to US and DS bonding groups for Cisco uBR7200 series routers.



CHAPTER 8

Subscriber Traffic Management for the Cisco CMTS Routers

First Published: February 14, 2008

Last Updated: November 29, 2010

Note Cisco IOS Release 12.2(33)SCA integrates support for this feature on the Cisco CMTS routers. This document contains information that references many legacy documents from Cisco IOS Release 12.3BC. In general, references to Cisco IOS Release 12.3BC also apply to Cisco IOS Release 12.2SC. The updates to this feature in Cisco IOS Release 12.3(23)BC2 are supported from Cisco IOS Release 12.2(33)SCB and later.

This document describes the Subscriber Traffic Management (STM) feature Version 1.3. STM feature supports all DOCSIS-compliant cable modems.

The STM feature allows a service provider to configure a maximum bandwidth threshold over a fixed period for a specific service class (or quality of service [QoS] profile)). The subscribers who exceed this configured threshold can then be identified and allocated reduced QoS. STM works as a low-CPU alternative to Network-Based Application Recognition (NBAR) and access control lists (ACLs). However, using STM does not mean that NBAR and ACLs have to be turned off; STM can be applied along with NBAR and ACLs. STM also works in conjunction with the Cisco Broadband Troubleshooter to support additional network management and troubleshooting functions in the Cisco CMTS.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see 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 document.

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

Contents

Prerequisites for Subscriber Traffic Management on the Cisco CMTS Routers

The Subscriber Traffic Management feature is supported on the Cisco CMTS routers in Cisco IOS Release 12.3BC and 12.2SC. Table below shows the hardware compatibility prerequisites for this feature.

Note The hardware components introduced in a given Cisco IOS Release are supported in all subsequent releases unless otherwise specified.

Table 35: Cable Hardware Compatibility Matrix for the Subscriber Traffic Management feature

CMTS Platform	Processor Engine	Cable Interface Line Cards
Cisco uBR10012 Universal Broadband Router	**Cisco IOS Release 12.2(33)SCB and later releases** • PRE2 • PRE4 **Cisco IOS Release 12.2(33)SCH and later releases** • PRE5	**Cisco IOS Release 12.2(33)SCB and later releases** • Cisco uBR10-MC5X20U/H **Cisco IOS Release 12.2(33)SCC and later releases** • Cisco UBR-MC20X20V **Cisco IOS Release 12.2(33)SCE and later releases** • Cisco uBR-MC3GX60V [20]
Cisco uBR7246VXR Universal Broadband Routers	**Cisco IOS Release 12.3(21)BC and later** • NPE-G1 **Cisco IOS Release 12.2(33)SCD and later** • NPE-G2)	**Cisco IOS Release 12.3(21)BC and later** • Cisco uBR-MC28U/X **Cisco IOS Release 12.2(33)SCD and later** • Cisco uBR-MC88V [21]

CMTS Platform	Processor Engine	Cable Interface Line Cards
Cisco uBR7225VXR Universal Broadband Router	**Cisco IOS Release 12.2(33)SCA and later** • NPE-G1 **Cisco IOS Release 12.2(33)SCD and later** • NPE-G2	**Cisco IOS Release 12.2(33)SCD and later** • Cisco uBR-MC28U/X • Cisco uBR-MC88V

[20] The Cisco uBR-3GX60V cable interface line card is not compatible with PRE2.

[21] The Cisco uBR-MC88V cable interface line card is compatible only with NPE-G2.

Restrictions for Subscriber Traffic Management on the Cisco CMTS Routers

Note In this document, the phrase QoS profile is synonymously used to indicate a service class for a DOCSIS 1.1 cable modem. However, QoS profile applies only to DOCSIS 1.0 operations. In instances where QoS profile is mentioned to indicate DOCSIS 1.1 operations, the QoS profile should be treated as a service class.

The STM feature has the following restrictions and limitations:

- Cisco IOS Release 12.2(15)BC1 supports monitoring and controlling only cable modems that have registered for DOCSIS 1.0 operations (using the quality of service [QoS] profile or service ID [SID] model).
- Cisco IOS Release 12.3(9a)BC supports monitoring and controlling cable modems that have registered for DOCSIS1.0 or DOCSIS 1.1 operations (using the QoS profile ID or service ID [SID] model).
- In STM version 1.1, the sampling rate range (duration) is calculated using the monitoring duration rather than the constant range (10 to 30 minutes) used in STM 1.0.
  - If the monitoring duration is more than a day (1440 minutes), the duration sample rate is calculated as (duration / 100).
  - If the monitoring duration is less than a day, the sample rate range is from 10 to 30 minutes.
  - If you are using STM 1.0 with a duration of two days and a sample rate of 20 minutes, and you try to restore that configuration in STM 1.1, the command fails because now the valid range is from 28 to 86 minutes.
- For DOCSIS1.0, the registered QoS profile specified by an enforce-rule must match exactly a QoS profile that exists on the Cisco CMTS. To manage a cable modem that is using a modem-created QoS profile, you must first create that same exact QoS profile on the Cisco CMTS. All parameters in the QoS profile must match before the cable modem can be managed by the enforce-rule.

- The Cisco CMTS routers support a certain maximum number of enforce-rules depending on your Cisco IOS software release. If you have created the maximum number of enforce-rules and want to create another rule, you must first delete one of the existing rules.
  - Cisco IOS Release 12.2(15)BC1 and later—Supports a maximum of 20 enforce-rules.
  - Beginning in Cisco IOS Release 12.3(23)BC2—Supports a maximum of 40 enforce-rules.
- Changing the configuration of an enforce-rule automatically resets all byte counters for the subscribers who are mapped to that enforce-rule.
- When specifying a QoS profile to be enforced when users violate their registered QoS profiles, both the originally provisioned QoS profile and the enforced QoS profile must be created on the Cisco CMTS.
- The Subscriber Traffic Management feature calculates duration based on the time set on the router, not uptime. Therefore, if you use the **clock set** command to change the time on the router, you might affect the STM monitoring behavior.
- The maximum cycle for subscriber traffic management is 31 days. If you choose a cycle of 31 days, the minimum sample rate that you can set is (31 days/100) minutes.

Information About Subscriber Traffic Management on the Cisco CMTS Routers

This section contains the following:

Feature Overview

The STM feature allows service providers to configure a maximum bandwidth threshold over a fixed period, for a specific service class (or QoS profile). The subscribers who exceed this configured threshold can then be identified and allocated a reduced QoS. This feature supplements current techniques such as NBAR and ACLs, to ensure that a minority of users do not consume a majority of a cable network's bandwidth.

Current subscriber controls, such as NBAR and ACLs, examine all packets coming into the CMTS. These techniques can curb a large volume of problem traffic, but they are not as effective in dealing with the latest generation of peer-to-peer file-sharing applications that can place heavy demands on a network's available bandwidth.

The STM feature allows service providers to focus on a minority of potential problem users without impacting network performance or other users who are abiding by their service agreements.

The STM feature supports two types of monitoring:

- Legacy Monitoring—Legacy monitoring allows you to set up a single monitoring duration without the ability to choose the time of day when that monitoring is performed. The configured monitoring parameters remain constant throughout the day.
- Peak-Offpeak Monitoring—Peak-Offpeak monitoring allows you to specify up to two high-traffic periods in a day for monitoring, in addition to the ability to continue monitoring during the remaining (or off-peak) periods. By combining the peak time option with weekend monitoring, you can identify and limit the bandwidth usage of certain subscribers for up to two peak network usage periods during weekdays, and during a different set of peak usage periods on weekends.

When a cable modem goes offline and remains offline for 24 hours, the Cisco CMTS router deletes its service flow IDs from its internal databases, and also deletes the modem's traffic counters. This can allow some users to exceed their bandwidth limits, go offline, and come back online with new counters. The Subscriber Traffic Management feature helps to thwart these types of theft-of-service attacks by implementing a penalty period for cable modems that violate their service level agreements (SLAs). Even if a cable modem goes offline, its counters are still reset, and the CMTS continues to enforce the penalty period.

Feature List

The Subscriber Traffic Management feature has the following operational features:

- Subscriber Traffic Management 1.1 (STM 1.1) supports cable modems that have registered for DOCSIS 1.1 operations (using the service class/service flow ID [SFID] model).
- Up to 20 enforce-rules can be created on each CMTS in Cisco IOS software releases prior to Cisco IOS Release 12.3(23)BC2. Beginning in Cisco IOS Release 12.3(23)BC2, you can create up to 40 enforce-rules.
- Separate enforce-rules can be used for downstream traffic and for upstream traffic. However, the limit on the total number of enforce-rules that can be configured includes the upstream and downstream rules combined.
- Each enforce-rule uses a subscriber's registered QoS profile to identify which users should be monitored for excessive traffic. The registered QoS profile must exist on the Cisco CMTS. If you want to manage cable modems that are using QoS profiles that were created by the cable modem, you must first manually create a QoS profile with the exact same QoS parameters on the Cisco CMTS, and then allow the cable modem to come online using the manually created profile.
- Each enforce-rule specifies the maximum number of kilobytes a user can transmit during a specified window.
- Subscribers who exceed the maximum bandwidth that is specified by their enforce-rule can be automatically switched to a separate enforced QoS profile that limits their network use for a customizable penalty period. The enforced QoS profile can change the guaranteed bandwidth, priority, or any other aspect of the traffic that the service provider considers an acceptable response to subscribers who violate their service agreements.
- Subscribers are automatically switched back to their registered QoS profile at the end of their penalty period. A technician at the service provider's network operations center (NOC) can also switch them back before the penalty period expires.

Note To manually switch back, delete the cable modem and allow it to register again.

- This feature also supports a **no-persistence** option, so that the enforced QoS profile does not remain in effect when a cable modem reboots. This option is particularly useful when the feature is initially implemented, so that the service providers can identify problem subscribers and applications, without creating a major impact on the entire user base. When repeat offenders are found, they can then be switched to an enforce-rule that does keep the enforced QoS profile in effect even when the cable modem reboots.
- Service providers can display a list of all subscribers' current usage statistics. Service providers can also display a list of just those subscribers who are overconsuming bandwidth.

- The penalty period persists across reboots of the cable modem, so subscribers cannot avoid the enforced QoS profile by resetting their modems and reregistering on the cable network. This allows service providers to set an appropriate penalty for those users that consistently exceed the maximum bandwidth they have been allocated. Service providers also can specify a time of day when CMs that are identified for penalty can be released from the penalty period.
- If a user that is using excessive bandwidth decides to upgrade to a higher level of service, the service provider can reconfigure the provisioning system to assign a new QoS profile to the cable modem. The user can then reboot the cable modem and come online using the new level of service.
- Service providers can change subscriber service classes for a particular modem using the **cable modem service-class-name** command.
- Different subscriber monitoring parameters can be configured for weekends, including peak and offpeak monitoring windows. You can also establish the same monitoring windows for every day of the week, or turn off monitoring altogether on the weekends as desired.

Sliding Window for Monitoring Service Flows

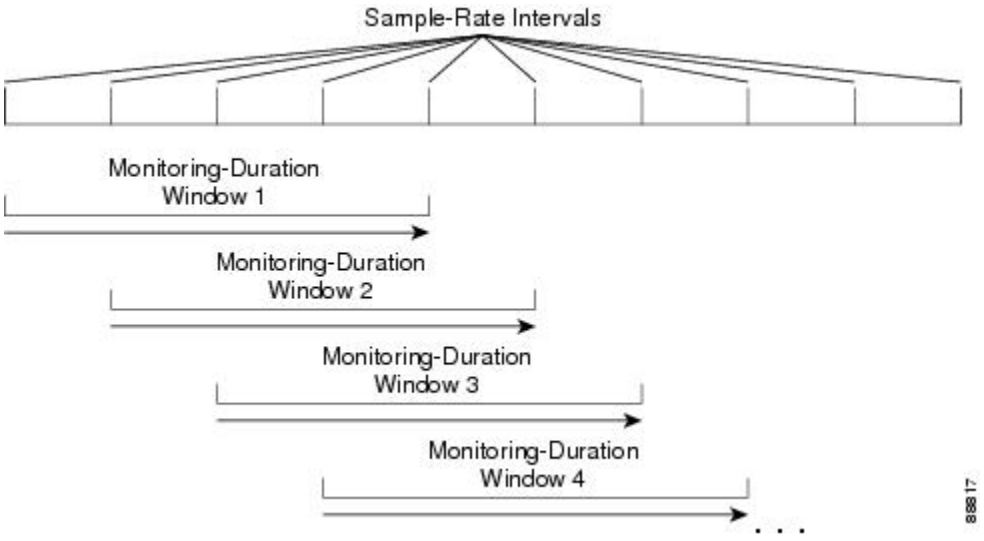
When an enforce-rule is activated, the CMTS periodically checks the bandwidth being used by subscribers to determine whether any subscribers are consuming more bandwidth than that specified by their registered QoS profiles. The CMTS keeps track of the subscribers using a sliding window that begins at each sample-rate interval and continues for the monitoring-duration period.

Each sample-rate interval begins a new sliding window period for which the CMTS keeps track of the total bytes transmitted. At the end of each sliding window period, the CMTS examines the byte counters to determine if any subscriber is currently overconsuming bandwidth on the network.

For example, with the default sample-rate interval of 15 minutes and the default monitoring-duration window of 360 minutes (6 hours), the CMTS samples the bandwidth usage every 15 minutes and determines the total bytes transmitted at the end of each 360-minute window. Therefore, every 15 minutes, the CMTS determines each subscriber's usage statistics for the preceding 6-hour period.

Figure below illustrates how this process works, with a new sliding window beginning at the beginning of each sample-rate interval period.

Figure 2: Monitoring-Duration Windows



Weekend Monitoring

With standard legacy and peak-offpeak monitoring configuration, monitoring continues to occur on the weekends, but in releases prior to Cisco IOS Release 12.3(23)BC2, there was not an ability to establish different monitoring criteria during the weekend days.

Beginning in Cisco IOS Release 12.3(23)BC2 for STM version 1.2, support for configuration of different monitoring conditions on weekends is introduced. Weekend monitoring options support the same parameters that are available in the existing monitoring options, but use a separate set of commands to configure alternate monitoring on weekend days. This includes configuration of peak and offpeak weekend monitoring windows.

In addition, the CLI supports the ability to turn off any monitoring on the weekend, or to use the same monitoring conditions for every day of the week.

SNMP Trap Notifications

Cisco IOS Release 12.2(15)BC1 (for the Cisco uBR10012 router) and Cisco IOS Release 12.3(9a)BC (for the Cisco uBR7246VXR router and the Cisco uBR7100 series routers) support a Simple Network Management Protocol (SNMP) trap notification that can be sent whenever a subscriber violates the enforce-rule. This trap is defined in the CISCO-CABLE-QOS-MONITOR-MIB and is enabled using the **snmp-server enable traps cable** command.

Each SNMP trap notification contains the following information:

- MAC address of the subscriber's cable modem
- Name of the enforce-rule being applied to this subscriber
- Total bytes sent by the subscriber during the monitoring-duration window

- Time at which the subscriber's penalty period expires

The CISCO-CABLE-QOS-MONITOR-MIB also contains the following tables that provide information about the Subscriber Traffic Management configuration and about subscribers who violate their enforce-rules:

- ccqmCmtsEnforceRuleTable—Contains the attributes of the enforce-rules that are currently configured on the Cisco CMTS.
- ccqmEnfRuleViolateTable—Provides a snapshot list of the subscribers who violated their enforce-rules over the sliding monitoring-duration window.

Beginning in Cisco IOS Release 12.3(23)BC2, the following new objects are introduced to support feature enhancements in STM Version 1.2:

- ccqmCmtsEnfRulePenaltyEndTime
- ccqmCmtsEnfRuleWkndOff
- ccqmCmtsEnfRuleWkndMonDuration
- ccqmCmtsEnfRuleWkndAvgRate
- ccqmCmtsEnfRuleWkndSampleRate
- ccqmCmtsEnfRuleWkndFirstPeakTime
- ccqmCmtsEnfRuleWkndFirstDuration
- ccqmCmtsEnfRuleWkndFirstAvgRate
- ccqmCmtsEnfRuleWkndSecondPeakTime
- ccqmCmtsEnfRuleWkndSecondDuration
- ccqmCmtsEnfRuleWkndSecondAvgRate
- ccqmCmtsEnfRuleWkndOffPeakDuration
- ccqmCmtsEnfRuleWkndOffPeakAvgRate
- ccqmCmtsEnfRuleWkndAutoEnforce

Beginning in Cisco IOS Release 12.3(33)SCD2, the following new objects are introduced to support feature enhancements in STM Version 1.3:

- ccqmCmtsEnfRuleFirstPeakTimeMin
- ccqmCmtsEnfRuleSecondPeakTimeMin
- ccqmCmtsEnfRuleWkndFirstPeakTimeMin
- ccqmCmtsEnfRuleWkndSecondPeakTimeMin
- ccqmCmtsEnfRulePenaltyEndTimeMin
- ccqmCmtsEnfRuleWkPenaltyPeriod
- ccqmCmtsEnfRuleWkndPenaltyPeriod
- ccqmCmtsEnfRuleRelTimeMonitorOn

Restrictions for SNMP Trap Notifications

In Cisco IOS Release 12.3(23)BC2, the MIB objects for weekend monitoring support only the SNMP GET and GETMANY operations.

Cable Modem Interaction with the Subscriber Traffic Management Feature

The Subscriber Traffic Management feature ensures that users cannot bypass the QoS restrictions by rebooting their cable modems or performing other configuration changes. The service provider, however, continues to be able to change the modems' profiles and other configuration parameters as desired.

When the Subscriber Traffic Management feature is enabled, the following behavior is in effect:

- The primary service flow counters for downstream and upstream traffic are preserved when the cable modem reboots. The service provider, however, can reset the counters by changing the QoS profile for the cable modem using the **cable modem qos profile** command and resetting the cable modem.
- Secondary service flow counters are reset whenever the cable modem reboots. This happens regardless of the enforce-rule configuration.
- The cable modem retains its current primary downstream and upstream service flows when it reboots. If the cable modem is in an enforced QoS profile penalty period when it reboots, it continues using the enforced QoS profile after the reboot. Service providers can manually change the profile by assigning a new QoS profile using the **cable modem qos profile** command.

Note Changing the QoS profile for a cable modem using the **cable modem qos profile** command, also changes the enforce-rule for the cable modem when it reboots. When the cable modem comes back online, it begins operating under the enforce-rule whose registered QoS profile (see the **qos-profile registered** command) matches the new QoS profile the modem is using.

- Service providers can also change the enforce-rule configuration. The following happens when the provider changes the enforce-rule configuration:
  - If the enforce-rule is disabled (using the **no enabled** command), all cable modems using that rule's registered QoS profile are no longer managed by the Subscriber Traffic Management feature. Configuring no enabled, deactivates the enforce-rule and moves all the modems in penalty to its registered QoS.
  - If the registered QoS profile for the rule is changed (using the **qos-profile registered** command), the cable modems that are using the previous registered QoS profile are no longer managed by the Subscriber Traffic Management feature. Instead, any cable modems that use the new registered QoS profile begin being managed by this rule.
  - If the enforced QoS profile for the rule is changed (using the **qos-profile enforced** command), any cable modems using this rule that are currently in the penalty period continue using the previously configured enforced QoS profile. Any cable modems that enter the penalty period after this configuration change, however, use the new enforced QoS profile.
- Service providers also have the option of making an enforce-rule nonpersistent, so that the enforced QoS profile does not remain in force when a cable modem reboots. Instead, when the cable modem

reboots and reregisters with the Cisco CMTS, the CMTS assigns it the QoS profile that is specified in its DOCSIS configuration file.

How to Configure the Subscriber Traffic Management Feature on the Cisco CMTS Routers

This section contains the following:

Creating and Configuring an Enforce-Rule

Every service class name that needs to be monitored will be linked with an enforce-rule. An enforce-rule defines the monitoring duration, the sample rate, the penalty period, and the registered service class name that the enforce-rule is linked to and the enforced service class name.

Use the procedure given below to create and configure an enforce-rule. An enforce-rule does not become active until the **enabled** command is given.

Before You Begin

- The registered and enforced service (QoS) profiles must be created on the CMTS before creating an enforce-rule that uses those profiles. If you want to manage a cable modem that currently uses a modem-created QoS profile, you must first manually create a new QoS profile on the CMTS with the same QoS parameters as the modem-created profile. Then allow the modem to come online using the manually created profile before beginning this procedure.
  - To display quality of service (QoS) profiles for a Cisco CMTS, use the show cable qos profile command in privileged EXEC mode.
  - To configure a QoS profile, use the cable qos profile command in global configuration mode. To set a particular value to its default, or to delete the profile when no specific parameters have been set, use the no form of this command.
- For monitoring of DOCSIS 1.1 cable modems:
  - Only DOCSIS 1.1 modems that register with a service class name are monitored.
  - To ensure that the DOCSIS 1.1 service flow counters remain across a reboot of the CM, configure the **cable primary-sflow-qos11 keep all** global configuration command.
- Only primary upstream and downstream service flows are supported.

Restriction

- When configuring peak-offpeak monitoring, you can define a maximum of two peak durations within a day, and also monitoring of the remaining hours, if you configure the offpeak duration. The monitoring duration and threshold for first peak, second peak, and offpeak, can be different. However, the monitoring duration for any peak or offpeak configuration cannot be more than a day.
- The parameters defined by the named service class should always be a compatible subset of the registered set of parameters for the CM. Only certain options can be changed using a CMTS router service class, such as the **max-rate**, **priority**, or **tos-overwrite** options. The **max-burst** option in both the enforced and registered CMTS router service classes must strictly match the value for **max-burst** in the registered DOCSIS configuration file. If the service class value does not match, either the cable modem registration will fail with a reject-c state, or the enforced class will fail.

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 the global configuration mode.
Step 3	**cable qos enforce-rule** *name* **Example:** `Router(config)# cable qos enforce-rule test`	Creates an enforce-rule with the specified *name* and enters the enforce-rule configuration mode. The *name* parameter can be any arbitrary and unique string that is from 1 to 15 characters in length. **Note** Each enforce-rule can be created by giving it a name.
Step 4	**monitoring-basics** {**legacy** | **peak-offpeak**} {**docsis10** | **docsis11**} **Example:** `Router(enforce-rule)# monitoring-basics peak-offpeak docsis11`	Defines the kind of monitoring desired and the type of modems to be monitored. • **legacy—**Provides only one threshold and one monitoring duration. • **peak-offpeak—**Allows the selection of two peak durations within a day. • **docsis10—**Specifies application of the enforce-rule to DOCSIS 1.0 cable modems. • **docsis11—**Specifies application of the enforce-rule to DOCSIS 1.1 cable modems. The default is legacy and DOCSIS 1.0.

	Command or Action	Purpose
Step 5	**qos-profile registered** *profile-id* **Example:** `Router(enforce-rule)# qos-profile registered 1`	Specifies the registered quality of service (QoS) profile that should be used for this enforce-rule. *profile-id* is a number from 0 to 16383. **Note** If you want to manage a cable modem that currently uses a modem-created QoS profile, you must first manually create a new QoS profile on the CMTS with the same QoS parameters as the modem-created profile. Then allow the modem to come online using the manually created profile before using this command.
Step 6	**qos-profile enforced** *profile-id* [**no-persistence**] **Example:** `Router(enforce-rule)# qos-profile enforced 4`	Specifies the quality of service (QoS) profile that should be enforced when users violate their registered QoS profiles. • *profile-id* Number from 0 to 16383. • **no-persistence—**(Optional) Configures the rule so that the enforced QoS profile does not remain in effect when a cable modem reboots.
Step 7	**service-class** {**enforced** | **registered**} *name* **Example:** `Router(enforce-rule)# service-class enforced test`	Identifies a particular service class with the specified *name* for cable modem monitoring in an enforce-rule. • **enforced—**Specifies an enforced service class. • **registered—**Specifies the service class using which the cable modem registered. **Note** This command is applicable only for DOCSIS 1.1 (or later) cable modems.
Step 8	**duration** *minutes* **avg-rate** *rate* **sample-interval** *minutes*[**penalty** *minutes*] {**downstream** | **upstream**} [**enforce**] **Example:** `Router(enforce-rule)# duration 10 avg-rate 500 sample-interval 10 penalty 120 downstream enforce`	Specifies the time period and sample rate used for monitoring subscribers when legacy monitoring is configured (Step 4, on page 209). • *minutes***—**Specifies the size of the sliding window (in minutes) during which subscriber usage is monitored. The valid range is 10 to 44640, with a default of 360 (6 hours). • **avg-rate** *rate***—**Specifies the average sampling rate in kilobits per second for the specified duration. The valid range is 1 to 400000 with no default. • **sample-interval** *minutes***—**Specifies how often (in minutes) the CMTS router should sample a service flow to get an estimate o f subscriber usage. The valid range is 1 to 30 minutes, with a default value of 15 minutes. • **penalty—**(Optional) Specifies the period (in minutes) during which a cable modem can be under penalty. This weekday penalty duration, if configured, takes precedence over the duration specified using the penalty-period command. The valid range is 1 to 10080. • **downstream—**Specifies monitoring of traffic in the downstream direction. • **upstream—**Specifies monitoring of traffic in the upstream direction. • **enforce—**(Optional) Specifies that the enforce-rule QoS profile should be applied automatically if a user violates their registered QoS profile.

	Command or Action	Purpose

Step 9	**peak-time1** {*hour* | *hour:minutes*} **duration** *minutes* **avg-rate** *rate* [**peak-time2** {*hour* | *hour:minutes*} **duration** *minutes* **avg-rate** *rate*][**duration** *offpeak-minutes* **avg-rate** *offpeak-rate*] **sample-interval** *minutes*[**penalty** *minutes*] {**downstream** | **upstream**}[**enforce**]
	
	Example:
	
	`Router(enforce-rule)# peak-time1 6 duration 180 avg-rate 2 peak-time2 18 duration 180 avg-rate 2 duration 120 avg-rate 3 sample-interval 10 upstream enforce`
	`Router(enforce-rule)# peak-time1 6:30 duration 180 avg-rate 2 peak-time2 18:40 duration 180 avg-rate 2 duration 120 avg-rate 3 sample-interval 10 penalty 120 upstream enforce`
		Specifies peak monitoring periods when peak-offpeak monitoring is configured (Step 4, on page 209).
		
		• **peak-time1** {*hour* | *hour:minutes*}—Specifies the time of day during which monitoring occurs for the first peak time. This value can be specified in hour (hh) or hour:minutes (hh:mm) format. The valid range for hour is 0 to 23 using a 24-hour clock. The valid range for minutes is 0 to 59.
		
		• **duration** *minutes*—Specifies the size of the sliding window during which the subscriber usage is monitored for the first peak time, and optionally for a second peak time when used with the **peak-time2** keyword. Valid range is 60 to 1440 minutes.
		
		• **avg-rate** *rate*—Specifies the average sampling rate in kilobytes per second for the specified duration. The valid range is 1 to 400000 with no default.
		
		• **peak-time2** {*hour* | *hour:minutes*}—(Optional) Specifies the time of day during which monitoring occurs for a second peak time. This value can be specified in hour (hh) or hour:minutes (hh:mm) format. The valid range for hours is 0 to 23 using a 24-hour clock. The valid range for minutes is 0 to 59.
		
		• **duration** *offpeak-minutes*—(Optional) Specifies the size of the sliding window during which the subscriber usage is monitored for the remaining offpeak time (time not specified for peak monitoring). The valid range is 60 to 1440 minutes.
		
		• **avg-rate** *offpeak-rate*—(Optional) Specifies the average sampling rate in kilobytes per second for the specified offpeak duration. The valid range is 1 to 400000 with no default.
		
		• **sample-interval** *minutes*—Specifies how often (in minutes) the CMTS router should sample a service flow to get an estimate of subscriber usage. The valid range is 1 to 30 minutes, with a default value of 15 minutes.
		
		• **penalty**—(Optional) Specifies the period (in minutes) during which a CM can be under penalty. This weekday penalty duration, if configured, takes precedence over the duration specified using the penalty-period command. The valid range is 1 to 10080.

Step 10		• **downstream**—Specifies monitoring of traffic in the downstream direction. • **upstream**—Specifies monitoring of traffic in the upstream direction. • **enforce**—(Optional) Specifies that the enforce-rule QoS profile should be applied automatically if a user violates the registered QoS profile.
Step 11	**penalty-period** *minutes* [**time-of-day** {*hour*|*hour:minutes*}] [**monitoring-on**]	(Optional) Specifies the period for which an enforced QoS profile should be in effect for subscribers who violate their registered QoS profiles.

	Command or Action	Purpose
	Example: `Router(enforce-rule)# penalty-period 10`	• *minutes*—Number from 1 to 10080 minutes, with a default value of 10080 minutes (7 days). • **time-of-day** {*hour* |*hour*:*minutes*}—(Optional) Specifies the time of day when a penalized cable modem can be released from its enforced profile. The time can be specified in the hh (hours) or hh:mm (hours:minutes) format. The valid range for hours is 0 to 23 using a 24-hour clock. The valid range for minutes is 0 to 59. • monitoring-on—(Optional) Specifies that the monitoring should be turned on after the cable modem is released from the penalty, that is, after time-of-day. If this keyword is not specified, by default, monitoring is turned off after the release time.
Step 12	**enabled** **Example:** `Router(enforce-rule)# enabled`	(Optional) Activates the enforce-rule and begins subscriber traffic management.
Step 13	**end** **Example:** `Router(enforce-rule)# end`	Exits enforce-rule configuration mode and returns to privileged EXEC mode.

Examples

This section provides command-line interface (CLI) examples, including the help feature for some of the enforce-rule commands.

Example: Legacy Monitoring Configuration

The following example shows a sample configuration of an enforce-rule for legacy monitoring:

```
Router(config)# cable qos enforce-rule test
Router(enforce-rule)# monitoring-basics ?
  legacy        Enable legacy (same average rate for all day)  monitoring
  peak-offpeak  Enable peak-offpeak monitoring
Router(enforce-rule)# monitoring-basics legacy ?
  docsis10  Enforce-rule will map to docsis 1.0 modems
  docsis11  Enforce-rule will map to docsis 1.1 modems
Router(enforce-rule)# monitoring-basics legacy docsis11
Router(enforce-rule)# service-class ?
  enforced    Enforced service class
  registered  Registered service class
Router(enforce-rule)# service-class registered ?
  WORD  Registered service class name
Router(enforce-rule)# service-class registered BEUS
Router(enforce-rule)# service-class enforced test
Router(enforce-rule)# duration ?
  <10-10080>  Duration in minutes
```

```
Router(enforce-rule)# duration 10 ?
  avg-rate  Average rate for the duration in kbits/sec
Router(enforce-rule)# duration 10 avg-rate ?
  <1-4294967>  average rate in kbits/sec
Router(enforce-rule)# duration 10 avg-rate 2 ?
  sample-interval  Rate of sampling in Minutes
Router(enforce-rule)# duration 10 avg-rate 2 sample-interval ?
  <1-30>  Sampling rate in Minutes
Router(enforce-rule)# duration 10 avg-rate 2 sample-interval 10 ?
  downstream  downstream
  upstream    upstream
Router(enforce-rule)# duration 10 avg-rate 2 sample-interval 10 upstream ?
  enforce  enforce the qos-profile automatically
  <cr>
Router(enforce-rule)# duration 10 avg-rate 2 sample-interval 10 upstream enf
Router(enforce-rule)# $ avg-rate 2 sample-interval 10 upstream enforce
Router(enforce-rule)# enabled
Router(enforce-rule)# end
```

Example: Peak-offpeak Monitoring Configuration

The following example shows a sample configuration of an enforce-rule for peak-offpeak monitoring:

```
Router(config)# cable qos enforce-rule test
Router(enforce-rule)# monitoring-basics peak-offpeak
Router(enforce-rule)# monitoring-basics peak-offpeak docsis10
Router(enforce-rule)# qos-profile ?
  enforced    Enforced qos profile
  registered  QoS profile index
Router(enforce-rule)# qos-profile registered ?
  <1-255>  Registered QoS profile index
Router(enforce-rule)# qos-profile registered 5
Router(enforce-rule)# qos-profile enforced 4
Router(enforce-rule)# peak-time1 6 ?
  duration  First peak duration
Router(enforce-rule)# peak-time1 6 duration ?
  <60-1440>  Duration in minutes
Router(enforce-rule)# peak-time1 6 duration 180 ?
  avg-rate  First peak average rate in kbits/sec
Router(enforce-rule)# peak-time1 6 duration 180 avg-rate ?
  <1-4294967>  Average rate in kbits/sec
Router(enforce-rule)# peak-time1 6 duration 180 avg-rate 2 ?
  duration         Off-peak duration
  peak-time2       Second peak time
  sample-interval  Rate of sampling in minutes

Router(enforce-rule)# peak-time1 6 duration 180 avg-rate 2 peak-time2 ?
  <10-1440>  Start of second peak time
Router(enforce-rule)# peak-time1 6 duration 180 avg-rate 2 peak-time2 18 ?
  duration  Second peak duration
Router(enforce-rule)# $6 duration 180 avg-rate 2 peak-time2 18 duration ?
  <10-1440>  Duration in minutes
Router(enforce-rule)# $6 duration 180 avg-rate 2 peak-time2 18 duration 240 ?
  avg-rate  Second peak average rate in kbits/sec
Router(enforce-rule)# $ 180 avg-rate 2 peak-time2 18 duration 240 avg-rate ?
  <1-4294967>  Average rate in kbits/sec
Router(enforce-rule)# $ 180 avg-rate 2 peak-time2 18 duration 240 avg-rate 3 ?
  duration         Off-peak duration
  sample-interval  Rate of sampling in minutes
Router(enforce-rule)# $ 180 avg-rate 2 peak-time2 18 duration 240 avg-rate 3 d
Router(enforce-rule)# $-time2 18 duration 240 avg-rate 3 duration 120 ?
  avg-rate  Off-peak average rate in kbits/sec
Router(enforce-rule)# $duration 240 avg-rate 3 duration 120 avg-rate 1 ?

  sample-interval  Rate of sampling in minutes
Router(enforce-rule)# $40 avg-rate 3 duration 120 avg-rate 1 sample-interval ?
  <1-30>  Sampling rate in Minutes
Router(enforce-rule)# $e 3 duration 120 avg-rate 1 sample-interval 10 ?
```

```
  downstream  downstream
  upstream    upstream
Router(enforce-rule)# $e 3 duration 120 avg-rate 1 sample-interval 10 upstream ?
  enforce  enforce the qos-profile automatically
  <cr>
Router(enforce-rule)# $on 120 avg-rate 1 sample-interval 10 upstream enforce
Router(enforce-rule)# enabled
Router(enforce-rule)# end
```

Example: CLI Help for peak-time Command

The following example shows output from the CLI help for the **peak-time** command:

```
Router(enforce-rule)# peak-time ?

<0-23> Start of first peak time, use 24 hour clock

Router(enforce-rule)# peak-time 1 ?

duration First peak duration

Router(enforce-rule)# peak-time 1 d ?

<60-1440> Duration in minutes

Router(enforce-rule)# peak-time 1 d 65 ?

First peak average rate in kbits/sec

Router(enforce-rule)# peak-time 1 d 65 a ?

<1-400000> Average rate in kbits/sec

Router(enforce-rule)# peak-time 1 d 65 a 1000 ?

duration Off-peak duration

peak-time2 Second peak time

sample-interval Rate of sampling in minutes

Router(enforce-rule)# peak-time 1 d 65 a 1000 d ?

<60-1440> Duration in minutes

Router(enforce-rule)# peak-time 1 d 65 a 1000 d 65 ?

avg-rate Off-peak average rate in kbits/sec

Router(enforce-rule)# peak-time 1 d 65 a 1000 d 65 a ?

<1-400000> Average rate in kbits/sec

Router(enforce-rule)# peak-time 1 d 65 a 1000 d 65 a 1000 ?

sample-interval Rate of sampling in minutes

Router(enforce-rule)# peak-time 1 d 65 a 1000 d 65 a 1000 s ?

<1-30> Sampling rate in Minutes

Router(enforce-rule)# peak-time 1 d 65 a 1000 d 65 a 1000 s 5 ?

downstream downstream

upstream upstream

Router(enforce-rule)# peak-time 1 d 65 a 1000 d 65 a 1000 s 5 d ?

enforce enforce the qos-profile automatically
```

```
<cr>

Router(enforce-rule)# peak-time 1 d 65 a 1000 d 65 a 1000 s 5 d
```

Configuring Weekend Monitoring

This section describes the tasks required to configure weekend monitoring for STM on a Cisco CMTS router.

Prerequisites

You must first configure the weekday monitoring parameters for an enforce-rule before configuring weekend monitoring. See the Creating and Configuring an Enforce-Rule, on page 208.

Restrictions

- Up to 40 total enforce-rules across both upstream and downstream configurations are supported.
- When using SNMP for weekend monitoring, only SNMP GET and GETMANY operations are supported.

Configuring Different Legacy Monitoring Conditions for Weekends

Use the following procedure if you want to establish different legacy monitoring conditions for subscribers for either upstream or downstream traffic on weekend days.

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	**cable qos enforce-rule** *name* **Example:** `Router(config)# cable qos enforce-rule test`	Accesses the enforce-rule with the specified *name* and enters enforce-rule configuration mode.
Step 4	**weekend duration** *minutes* **avg-rate** *rate* **sample-interval** *minutes* {**downstream** | **upstream**} [**penalty** *minutes*] [**enforce**]	Specifies the time period and sample rate used for monitoring subscribers on weekends.

	Command or Action	Purpose
	Example: `Router(enforce-rule)# weekend duration 15 avg-rate 500 sample-interval 10 penalty 120 downstream enforce`	• *minutes*—Specifies the size of the sliding window during which subscriber usage is monitored. The valid range is 10 to 44640, with a default of 360 minutes. • **avg-rate** *rate*—Specifies the average sampling rate in kilobits per second for the specified duration. The valid range is 1 to 400000 with no default. • **sample-interval** *minutes*—Specifies how often (in minutes) the CMTS router should sample a service flow to get an estimate of subscriber usage. The valid range is 1 to 30, with a default value of 15. • **penalty—**(Optional) Specifies the period (in minutes) during which a CM can be under penalty. This weekend penalty duration, if configured, takes precedence over the duration specified using the penalty-period command. The valid range is 1 to 10080. • **downstream—**Specifies monitoring of traffic in the downstream direction. • **upstream—**Specifies monitoring of traffic in the upstream direction. • **enforce—**(Optional) Specifies that the enforce-rule QoS profile should be applied automatically if a user violates their registered QoS profile.
Step 5	**end** **Example:** `Router(enforce-rule)# end`	Exits enforce-rule configuration mode and returns to privileged EXEC mode.

Configuring Different Peak-Offpeak Monitoring Conditions for Weekends

Use the following procedure if you want to establish different peak and offpeak monitoring conditions for subscribers for either upstream or downstream traffic on weekend days.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable qos enforce-rule** *name* **Example:** `Router(config)# cable qos enforce-rule test`	Accesses the enforce-rule with the specified *name* and enters enforce-rule configuration mode.

Step 4	**weekend peak-time1** {*hour* | *hour*:*minutes*} **duration** *minutes* **avg-rate** *rate* [**peak-time2** *hour* **duration** *minutes* **avg-rate** *rate*] [**duration** *offpeak-minutes* **avg-rate** *offpeak-rate*] **sample-interval** *minutes*[**penalty** *minutes*] {**downstream**| **upstream**}[**enforce**]
	
	Example:
	
	`Router(enforce-rule)# weekend peak-time1 9 duration 180 avg-rate 2 peak-time2 16 duration 180 avg-rate 2 duration 120 avg-rate 3 sample-interval 10 upstream enforce`
	
	Example:
	
	`Router(enforce-rule)# weekend peak-time1 9:30 duration 180 avg-rate 2 peak-time2 16:58 duration 180 avg-rate 2 duration 120 avg-rate 3 sample-interval 10 penalty 120 upstream enforce`
		Specifies peak and offpeak monitoring times on weekends.
		• **peak-time1** {*hour* | *hour:minutes}*—Specifies the first peak time, in hour (hh) or hour:minutes (hh:mm) format. The valid range for hours is 0 to 23 and for minutes is 0 to 59.
		• **duration** *minutes*—Specifies the size of the sliding window during which subscriber usage is monitored for the first peak time, and optionally for a second peak time when used with the **peak-time2** keyword. The valid range is 60 to 1440 minutes.
		• **avg-rate** *rate*—Specifies the average sampling rate in kilobytes per second for the specified duration. The valid range is 1 to 400000 with no default.
		• **peak-time2** {*hour* | *hour:minutes}*—(Optional) Specifies the second peak time, in hour (hh) or hour:minutes (hh:mm) format. The valid range for hour is 0 to 23 and for minutes is 0 to 59.
		• **duration** *offpeak-minutes*—(Optional) Specifies the size of the sliding window during which the subscriber usage is monitored for the remaining offpeak time (time not specified for peak monitoring). The valid range is 60 to 1440 minutes.
		• **avg-rate** *offpeak-rate*—(Optional) Specifies the average sampling rate in kbps for the specified offpeak duration. The valid range is 1 to 400000.
		• **sample-interval** *minutes*—Specifies how often (in minutes) the CMTS router should sample a service flow to get an estimate of subscriber usage. The valid range is 1 to 30 minutes, with a default value of 15 minutes.
		• **penalty**—(Optional) Specifies the period (in minutes) during which a CM can be under penalty. This weekend penalty duration, if configured, takes precedence over the duration specified using the penalty-period command. The valid range is 1 to 10080.
		• **downstream**—Specifies monitoring of traffic in the downstream direction.

	Command or Action	Purpose
		• **upstream—**Specifies monitoring of traffic in the upstream direction. • **enforce—**(Optional) Specifies that the enforce-rule QoS profile should be applied automatically if a users violate their registered QoS profile.
Step 5	**end** **Example:** `Router(enforce-rule)# end`	Exits enforce-rule configuration mode and returns to privileged EXEC mode.

Disabling Weekend Monitoring

Use the following procedure to turn off the weekend monitoring configuration and monitor on weekdays only.

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	**cable qos enforce-rule** *name* **Example:** `Router(config)# cable qos enforce-rule test`	Accesses the enforce-rule with the specified *name* and enters enforce-rule configuration mode.
Step 4	**weekend off** **Example:** `Router(enforce-rule)#  weekend off`	Disables monitoring on weekends.
Step 5	**end** **Example:** `Router(enforce-rule)# end`	Exits enforce-rule configuration mode and returns to privileged EXEC mode.

Removing Weekend Monitoring Conditions and Use the Same Monitoring Criteria Every Day

Use the following procedure to remove the specified weekend monitoring conditions and use the same monitoring criteria all week (including weekends).

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	**cable qos enforce-rule** *name* **Example:** `Router(config)# cable qos enforce-rule test`	Accesses the enforce-rule with the specified *name* and enters enforce-rule configuration mode.
Step 4	**no weekend** **Example:** `Router(enforce-rule)# no weekend`	Performs monitoring on the weekends using the same parameters for weekdays and weekends.
Step 5	**end** **Example:** `Router(enforce-rule)# end`	Exits enforce-rule configuration mode and returns to privileged EXEC mode.

Disabling an Enforce-Rule

Use the following procedure to disable an enforce-rule. The enforce-rule remains in the CMTS configuration file, but any subscriber traffic management that uses this enforce-rule ends.

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	**cable qos enforce-rule***name* **Example:** `Router(config)# cable qos enforce-rule test`	Creates an enforce-rule with the specified *name* and enters enforce-rule configuration mode.
Step 4	**no enabled** **Example:** `Router(enforce-rule)# no enabled`	Disables the enforce-rule and ends subscriber traffic management for users with the rule's registered QoS profile. It moves all modems in penalty to its registered QoS.
Step 5	**end** **Example:** `Router(enforce-rule)# end`	Exits enforce-rule configuration mode and returns to privileged EXEC mode.

Removing an Enforce-Rule

Use the following procedure to delete an enforce-rule and remove it from the CMTS configuration file. Any subscriber traffic management that uses this rule also ends.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**no cable qos enforce-rule***name* **Example:** `Router(config)# no cable qos enforce-rule ef-rule`	Deletes the enforce-rule with the specified *name* . This enforce-rule and its configuration are removed from the CMTS configuration, and any subscriber traffic management that uses this rule ends.
Step 4	**end** **Example:** `Router(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Changing a Cable Modem Service Class

Use the following procedure to change a QoS service class for a particular DOCSIS 1.1 cable modem.

Restriction

- The command is supported only on DOCSIS 1.1 CM primary service flows.
- You can specify the **cable modem service-class-name** command only after the CM has been online for at least 200 seconds.
- The parameters defined by the named service class should always be a compatible subset of the registered set of parameters for the CM. Only certain options can be changed using a CMTS router service class, such as the **max-rate**, **priority**, or **tos-overwrite** options. The **max-burst** option in both the enforced and registered CMTS router service classes must strictly match the value for **max-burst** in the registered DOCSIS configuration file. If the service class value does not match, then CM registration will fail with a reject-c state, or the enforced class will fail.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.

	Command or Action	Purpose
Step 2	**cable modem** {*ip-address* | *mac-address*} **service-class-name** *name* **Example:** `Router# cable modem aaaa.bbbb.cccc service-class-name test`	Changes a QoS service class for a particular cable modem. • *ip-address*—Specifies the IP address of the CM to be assigned the named service class. • *mac-address*—Specifies the MAC address of the CM to be assigned the named service class. • *name*—Specifies the name of the QoS service class.
Step 3	**end** **Example:** `Router# end`	Exits privileged EXEC mode.

Monitoring the Subscriber Traffic Management Feature on the Cisco CMTS Routers

This section describes the following tasks that can be used to monitor the Subscriber Traffic Management feature:

Displaying the Currently Defined Enforce-Rules

To display all enforce-rules that are currently defined on the Cisco CMTS router, or the definitions for a particular enforce-rule, use the **show cable qos enforce-rule** command in privileged EXEC mode.

For offpeak monitoring, use the **show cable qos enforce-rule** command to display the monitoring duration and average-rate values applicable for that time of day. If no monitoring is taking place, 0 is displayed.

The following example shows sample output from the **show cable qos enforce-rule** command for all configured enforce-rules:

```
Router# show cable qos enforce-rule
            Name              Dur  Dir byte-cnt Auto rate  penalty Reg Enf Ena Persist
                             (min)     (kbytes) enf  (min) (min)   QoS QoS
 residential                  10   us  5        act  1     10080   5   10  Yes Yes
 ef-q11d                      30   ds  150      act  1     20      11  99  Yes Yes
 ef-q11u                      30   us  60       act  1     20      11  99  Yes Yes
 ef-q21                       720  us  60       act  1     10      21  81  Yes Yes
 ef-q21d                      300  ds  150      act  1     10      21  81  Yes Yes
 ef-q22                       720  us  60       act  1     10      22  82  Yes Yes
 ef-q22d                      300  ds  150      act  1     10      22  82  Yes No
 ef-q23                       720  us  60       act  1     10      23  83  Yes Yes
 ef-q23d                      300  ds  150      act  1     10      23  83  Yes Yes
 ef-q24                       720  us  60       act  1     10      24  84  Yes Yes
 ef-q24d                      300  ds  150      act  1     10      24  84  Yes Yes
 ef-q25                       720  us  60       act  1     10      25  85  Yes Yes
 ef-q25d                      300  ds  150      act  1     10      25  85  Yes Yes
 ef-q26                       720  us  60       act  1     10      26  86  Yes Yes
```

```
 ef-q26d                      300  ds  150      act  1     10      26  86  Yes Yes
 ef-q27                       720  us  60       act  1     10      27  87  Yes Yes
 ef-q27d                      300  ds  150      act  1     10      27  87  Yes Yes
 ef-q28                       720  us  60       act  1     10      28  88  Yes Yes
 ef-q28d                      300  ds  150      act  1     10      28  88  Yes No
 ef-q5d                       300  ds  150      act  1     10      5   99  Yes Yes
 ef-q5u                       720  us  600      act  1     10      5   99  Yes Yes
```

The following example shows sample output from the **show cable qos enforce-rule** command for a particular enforce-rule named “test”:

```
Router# show cable qos enforce-rule test
     Name        Type Dur  Dir Avg-rate Auto rate     Reg        Enf      En Per
                      (min)    kbits/s  enf  (min)
test           p-off 120   us 1        act  10     255        4        Y  Y
```

The following example shows the sample output from the **show cable qos enforce-rule verbose** command for an enforce-rule named “test”:

```
Router# show cable qos enforce-rule test verbose
Name                          : test
Version                       : docsis11
Monitoring Type               : peak-offpeak
Registered                    : REG-DS
Enforced                      : ENF-DS
Monitoring Duration           : 70 (in minutes)
Sample-rate                   : 10 (in minutes)
Average-rate                  : 3 kbits/sec
Direction                     : downstream
Auto Enforce                  : Yes
Current Penalty Duration      : 10 (in minutes)
Default Penalty Duration      : 10 (in minutes)
Penalty End-time              : 23:0 (time of day)
Rule Enabled                  : Yes
Persistence                   : Yes
Weekend                       : No
Penalty Off                   : No
Monitor Weekend               : Yes
Monitoring after RelTime      : Off
First Peak Time               : 10:0
Duration                      : 60 (in minutes)
First Average-rate            : 1 kbits/sec
Second Peak Time              : 19:0
Duration                      : 65 (in minutes)
Second Average-rate           : 2 kbits/sec
Offpeak Duration              : 70 (in minutes)
Offpeak Average-rate          : 3 kbits/sec
Auto Enforce                  : Yes
Sample Rate                   : 10
Penalty-Period for week-days  : 0
Weekend First Peak Time       : 11:0
Weekend Duration              : 75 (in minutes)
Weekend First Average-rate    : 4 kbits/sec
Weekend Second Peak Time      : 20:0
Weekend Duration              : 80 (in minutes)
Weekend Second Average-rate   : 5 kbits/sec
Weekend Offpeak Duration      : 85 (in minutes)
Weekend Offpeak Average-rate  : 6 kbits/sec
Weekend Auto Enforce          : Yes
Weekend Sample Rate           : 12
Penalty-Period for week-ends  : 0
router#sh clock
*17:30:50.259 UTC Mon Apr 19 2010
```

The following example shows sample output from the **show cable qos enforce-rule verbose** command for a particular enforce-rule named “test” that has specified peak-offpeak weekend monitoring options:

```
Router# show cable qos enforce-rule test verbose
Name : test
Version : docsis10
Monitoring Type : peak-offpeak
```

```
Registered : 255
Enforced : 4
Monitoring Duration : 120 (in minutes)
Sample-rate : 10 (in minutes)
Average-rate : 1 kbits/sec
Direction : upstream
Penalty Time : 10080 (in minutes)
Penalty End-time : 23 (time of day in hrs)
Rule Enabled : Yes
Persistence : Yes
Week-end : Yes
First Peak Time : 6
Duration : 180 (in minutes)
First Average-rate : 2 kbits/sec
Second Peak Time : 18
Duration : 240 (in minutes)
Second Averate-rate : 3 kbits/sec
Offpeak Duration : 120 (in minutes)
Offpeak Average-rate : 1 kbits/sec
Auto-enforce : active
Weekend First Peak Time : 8
Weekend First Duration : 120 (in minutes)
Weekend First Average-rate : 2 kbits/sec
Weekend Second Peak Time : 18
Weekend Second Duration : 180 (in minutes)
Weekend Second Average-rate : 5 kbits/sec
Weekend Offpeak Duration : 240 (in minutes)
Weekend Offpeak Average-rate : 4 kbits/sec
Weekend Auto-enforce : active
```

Displaying the Current Subscriber Usage

To display the usage for all subscribers on a cable interface, use the show cable subscriber-usage command in privileged EXEC mode without any options.

To display the usage for just those subscribers who are violating their registered quality of service (QoS) profiles, use the show cable subscriber-usage over-consume form of the command.

The following example shows sample output from the **show cable subscriber-usage** command for all users on the specified cable interface:

```
Router# show cable subscriber-usage cable 6/0/1
Sfid Mac Address   Enforce-rule Total-Kbyte    Last-detect    Last-penalty   Pen
                       Name        Count         time           time        Flag
3    0007.0e03.110d efrule-q5   121944817  Jan1  03:44:08  Jan1  03:54:08  Act
4    0007.0e03.110d efrule-q5d  1879076068 Jan1  03:35:05  Jan1  03:45:06  Act
5    0007.0e03.1431 efrule-q5   120052387  Jan1  03:44:18  Jan1  03:54:18  Act
6    0007.0e03.1431 efrule-q5d  1838493626 Jan1  03:34:55  Jan1  03:44:55  Act
7    0007.0e03.1445 efrule-q5   120919427  Jan1  03:44:08  Jan1  03:54:08  Act
8    0007.0e03.1445 efrule-q5d  1865955172 Jan1  03:35:06  Jan1  03:45:06  Act
9    0007.0e03.1225 efrule-q5   120200155  Jan1  03:44:18  Jan1  03:54:18  Act
10   0007.0e03.1225 efrule-q5d  1839681070 Jan1  03:34:55  Jan1  03:44:55   -
11   0007.0e03.0cb1 efrule-q5   122941643  Jan1  03:43:58  Jan1  03:53:58  Act
12   0007.0e03.0cb1 efrule-q5d  1889107176 Jan1  03:35:06  Jan1  03:45:06  Act
13   0007.0e03.1435 efrule-q5   119504795  Jan1  03:44:18  Jan1  03:54:18  Act
14   0007.0e03.1435 efrule-q5d  1835164034 Jan1  03:34:55  Jan1  03:44:55   -
```

By default, the display is sorted by the service flow ID (SFID). To sort the display by the subscriber byte count, with the largest byte counts listed first, use the **sort-byte-count** option. The following example shows sample output for **show cable subscriber-usage sort-byte-count** form of the command:

Note The **sort-byte-count** option was replaced by the **sort-avg-rate** option.

```
Router# show cable subscriber-usage
```

```
 sort-byte-count

Sfid Mac Address   Enforce-rule Total-Kbyte  Last-detect    Last-penalty   Pen
                      Name        Count       time            time        Flag
7    0007.0e03.2cad test1       65157114   Feb24 11:36:34  Mar3  11:36:34  Act
9    0007.0e03.2c45 test1       16381014                                   -
5    0007.0e03.2c25 test1       13440960                                   -
```

Configuration Examples for Subscriber Traffic Management on the Cisco CMTS Routers

This section lists sample configurations for the Subscriber Traffic Management feature on a CMTS router:

Example: DOCSIS Configuration File and STM Service Classes

The following example shows a sample DOCSIS configuration file along with sample registered and enforced QoS service classes that you could define on a Cisco CMTS router to perform subscriber traffic management.

DOCSIS Configuration File Options

This is an example of a very basic set of options that you can configure for a cable modem in your DOCSIS configuration file that supports a successful configuration of new QoS service class options on the Cisco CMTS router.

Note There are certain QoS parameters that cannot be changed from the registered QoS parameter set and a new service class. For example, the **max-burst** value must match the originally registered in the DOCSIS configuration file, and the registered and enforced QoS service classes on the Cisco CMTS router. If the **max-burst** value differs from the registered CMTS service class and the DOCSIS configuration file, the CM might go into reject-c state, or the enforced class could fail.

The following example shows the configuration of two service classes named “BE-STM-US-1” and “BE-STM-DS-1” in a DOCSIS configuration file to define a basic set of upstream and downstream parameters:

```
03 (Net Access Control) = Yes
17 (Baseline Privacy Block)
S01 (Authorize Wait Timeout) = 10
18 (Maximum Number of CPE) = 10
24 (Upstream Service Flow Block)
S01 (Flow Reference) = 1
S04 (Service Class Name) = BE-STM-US-1
S06 (QoS Parameter Set Type) = 7
25 (Downstream Service Flow Block)
S01 (Flow Reference) = 2
S04 (Service Class Name) = BE-STM-DS-1
S06 (QoS Parameter Set Type) = 7
29 (Privacy Enable) = Yes
```

The following example shows sample **cable service class** commands on the Cisco CMTS router for configuration of subscriber traffic management that correspond to the service class names in the DOCSIS configuration file of “BE-STM-US-1” and “BE-STM-DS-1.” These service classes correspond to the registered service classes configured by the **service-class registered** command for the QoS enforce-rules shown later in this example:

```
cable service class 2 name BE-STM-US-1
cable service class 2 upstream
cable service class 2 max-rate 2000000
cable service class 2 max-burst 3044
```

```
cable service class 2 max-concat-burst 8000
cable service class 3 name BE-STM-DS-1
cable service class 3 downstream
cable service class 3 max-rate 30000000
cable service class 3 max-concat-burst 8000
```

For the cable modem to achieve maximum US thoroughput, provide a large value to the max-concat-burst keyword in the cable service class command.

The following example shows sample **cable service class** commands on the Cisco CMTS router that configure new QoS parameters for identified subscribers to limit bandwidth using the **max-rate** parameter. These service classes correspond to the enforced service classes configured by the **service-class enforced** command for the QoS enforce rules shown later in this example:

```
cable service class 102 name BEUS-1
cable service class 102 upstream
cable service class 102 max-rate 48888
cable service class 102 max-burst 3044
cable service class 102 max-concat-burst 8000
cable service class 103 name BEDS-1
cable service class 103 downstream
cable service class 103 max-rate 988888
cable service class 103 max-concat-burst 8000
```

The following example shows configuration of the corresponding enforce-rules for upstream and downstream monitoring, which identifies the registered and enforced service classes:

```
cable qos enforce-rule US-1
  monitoring-basics legacy docsis11
  penalty-period 10
  service-class registered BE-STM-US-1
  service-class enforced BEUS-1
  duration 10 avg-rate 1 sample-interval 10 up enf
  enabled
!
cable qos enforce-rule DS-1
  monitoring-basics legacy docsis11
  penalty-period 10
  service-class registered BE-STM-DS-1
  service-class enforced BEDS-1
  duration 10 avg-rate 1 sample-interval 10 do enf
  enabled
```

Example: Downstream Configuration

The following example shows a typical enforce-rule configuration for traffic in the downstream direction:

```
!
cable qos enforce-rule downstream-rule
  monitoring-basics legacy docsis11
  penalty-period 10
  service-class registered class5
  service-class enforced class99
  duration 30 avg-rate 1 sample-interval 10 downstream enforce
  enabled
```

Example: Upstream Configuration

The following example shows a typical enforce-rule configuration for traffic in the upstream direction:

```
!
cable qos enforce-rule upstream-rule
  monitoring-basics legacy docsis11
```

```
  penalty-period 10
  service-class registered class5
  service-class enforced class99
  duration 30 avg-rate 1 sample-interval 10 upstream enforce
  enabled
```

Example: Downstream and Upstream Configuration

The following example shows a typical enforce-rule configuration for traffic in both the downstream and upstream directions. Two separate rules are created, using the identical configuration, except for the keywords **upstream** and **downstream** in the **duration** command.

Note The enforce rules for the upstream and downstream directions can use either an identical configuration, or they can use their own individual configurations.

```
!
cable qos enforce-rule upstream-rule
  monitoring-basics legacy docsis11
  penalty-period 10
  service-class registered class5
  service-class enforced class99
  duration 30 avg-rate 5 sample-interval 10 upstream enforce
  enabled
cable qos enforce-rule downstream-rule
  monitoring-basics legacy docsis11
  penalty-period 10
  service-class registered class5
  service-class enforced class99
  duration 30 avg-rate 5 sample-interval 10 downstream enforce
  enabled
```

The following example shows an enforce-rule configuration for traffic in upstream direction. A unique penalty duration is configured for upstream, with monitoring turned on after the penalty release time.

Note For upstream direction, a unique penalty duration (120 minutes) is configured, which takes precedence over the duration configured using the penalty-period command (60 minutes). A fresh monitoring starts after the penalty release time (23:00), when all the traffic counters are reset to 0.

```
!
cable qos enforce-rule upstream_rule
  monitoring-basics peak-offpeak docsis10
  penalty-period 60 time-of-day 23:00 monitoring-on
  qos-profile registered 6
  qos-profile enforced 100
  peak-time1 10:30 duration 120 avg-rate 10 peak-time2 22:10 duration 60 avg-rate 10
sample-interval 10 penalty 120 upstream enforce
enabled
```

Example: Weekend Monitoring Configuration

The following example shows a sample configuration of peak-offpeak weekend monitoring for DOCSIS 1.0 cable modems:

```
cable qos enforce-rule monitoring
    monitoring-basics peak-offpeak docsis10
```

```
    penalty-period 60
    qos-profile registered 6
    qos-profile enforced 100
    peak-time1 10 duration 120 avg-rate 10 peak-time2 23 duration 60 avg-rate 10
sample-interval 10 upstream enforce
    weekend peak-time1 8 duration 60 avg-rate 100 peak-time2 20 duration 60 avg-rate 10000
 duration 90 avg-rate 20000 sample-interval 20 downstream enforce
    enabled
```

Additional References

For additional information related to the Subscriber Traffic Management feature, refer to the following references:

Related Documents

Related Topic	Document Title
Cable commands	Cisco IOS CMTS Cable Command Reference

Standards

Standards[22]	Title
SP-RFIv1.1-I09-020830	*Data-over-Cable Service Interface Specifications Radio Frequency Interface Specification, version 1.1* (http://www.cablemodem.com)
draft-ietf-ipcdn-docs-rfmibv2-06	*Radio Frequency (RF) Interface Management Information Base for DOCSIS 2.0 Compliant RF Interfaces*

22 Not all supported standards are listed.

MIBs

MIBs[23]	MIBs Link
• CISCO-CABLE-QOS-MONITOR-MIB • DOSCIS-QOS-MIB	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

23 Not all supported MIBs are listed.

RFCs

RFCs[24]	Title
RFC 2233	DOCSIS OSSI Objects Support
RFC 2665	DOCSIS Ethernet MIB Objects Support
RFC 2669	Cable Device MIB

24 Not all supported RFCs are listed.

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Subscriber Traffic Management for the Cisco CMTS Routers

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note The table below 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.

Table 36: Feature Information for Subscriber Traffic Management for the Cisco CMTS Routers

Feature Name	Releases	Feature Information
Subscriber Traffic Monitoring 1.0	12.2(15)BC1	This feature was introduced on the Cisco uBR7100 series routers, Cisco uBR7200 series routers, and Cisco uBR10012 router.
Subscriber Traffic Management Version 1.1	12.3(9a)BC	This feature was modified on the Cisco uBR7200 series routers and the Cisco uBR10012 router to extend the earlier STM functions and monitor a subscriber's traffic on the DOCSIS 1.1 primary service flows, and support these additional features: • Cisco STM Version 1.1 supports Cisco Broadband Troubleshooter 3.2. • Cisco STM Version 1.1 supports DOCSIS 1.1 cable modems. • Cisco STM Version 1.1 monitors and applies traffic management policies on a service-flow basis. • Cisco STM Version 1.1 increases the available monitoring window from 7 to 30 days.
Subscriber Traffic Management Version 1.1	12.2(33)SCA	This feature was integrated into Cisco IOS Release 12.2(33)SCA to support the Cisco uBR7246VXR router, Cisco uBR7225VXR router, and Cisco uBR10012 router.

Feature Name	Releases	Feature Information
Subscriber Traffic Management Version 1.2	12.3(23)BC2	

Feature Name	Releases	Feature Information
		This feature was enhanced with the following support on the Cisco uBR7246VXR and Cisco uBR10012 routers: • Support was added for the Cisco Wideband SPA (Cisco uBR10012 router only). • Support for suspension of the cable modem (CM) penalty period at a certain time of day. • Support for weekday and weekend traffic monitoring. • Support of up to 40 enforce-rules. • Support for service providers to change subscriber service classes for a particular modem using the cable modem service-class-name command. • Addition of the following SNMP objects to the CISCO-CABLE-QOS-MONITOR-MIB: ◦ ccqmCmtsEnfRulePenaltyEndTime ◦ ccqmCmtsEnfRuleWkndOff ◦ ccqmCmtsEnfRuleWkndMonDuration ◦ ccqmCmtsEnfRuleWkndAvgRate ◦ ccqmCmtsEnfRuleWkndSampleRate ◦ ccqmCmtsEnfRuleWkndFirstPeakTime ◦ ccqmCmtsEnfRuleWkndFirstDuration ◦ ccqmCmtsEnfRuleWkndFirstAvgRate ◦ ccqmCmtsEnfRuleWkndSecondPeakTime ◦ ccqmCmtsEnfRuleWkndSecondDuration ◦ ccqmCmtsEnfRuleWkndSecondAvgRate ◦ ccqmCmtsEnfRuleWkndOffPeakDuration ◦ ccqmCmtsEnfRuleWkndOffPeakAvgRate ◦ ccqmCmtsEnfRuleWkndAutoEnforce • The following commands are new or modified: ◦ **cable modem service-class-name** ◦ **penalty-period** ◦ **show cable qos enforce-rule verbose**

Feature Name	Releases	Feature Information
		◦ **weekend duration** ◦ **weekend off** ◦ **weekend peak-time1**
Subscriber Traffic Management Version 1.2	12.2(33)SCB	This feature enhancement was integrated into Cisco IOS Release 12.2(33)SCB to bring feature parity with Cisco IOS Release 12.3(23)BC2.

Feature Name	Releases	Feature Information
Subscriber Traffic Management Version 1.3	12.2(33)SCD2	This feature was enhanced with the following support on the Cisco uBR7246VXR, Cisco uBR7225VXR, and Cisco uBR10012 routers: • Support for configuring minute-level peak time—Peak time can now be configured in the hh:mm format, which enables a user to pinpoint the exact time at which monitoring should start. • Support for configuring minute-level penalty end time—Penalty end time can now be configured in the hh:mm format, which enables a user to pinpoint the exact time at which monitoring should stop. • Ability to configure a unique penalty duration for weekdays and weekends. • Ability to specify whether monitoring should be turned on after the CM is released from penalty. • Addition of the following SNMP objects to the CISCO-CABLE-QOS-MONITOR-MIB: ◦ ccqmCmtsEnfRuleFirstPeakTimeMin ◦ ccqmCmtsEnfRuleSecondPeakTimeMin ◦ ccqmCmtsEnfRuleWkndFirstPeakTimeMin ◦ ccqmCmtsEnfRuleWkndSecondPeakTimeMin ◦ ccqmCmtsEnfRulePenaltyEndTimeMin ◦ ccqmCmtsEnfRuleWkPenaltyPeriod ◦ ccqmCmtsEnfRuleWkndPenaltyPeriod ◦ ccqmCmtsEnfRuleRelTimeMonitorOn • The following commands are modified: **duration**, **peak-time1, penalty-period, show cable qos enforce-rule verbose, weekend duration, weekend peak-time1**