Cisco cBR Series Converged Broadband Routers Quality of Services Configuration Guide for Cisco IOS XE Fuji 16.8.x

First Published: 2018-03-07

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

© 2018 Cisco Systems, Inc. All rights reserved.

CONTENTS

CHAPTER 1 **Dynamic Bandwidth Sharing** 1

Hardware Compatibility Matrix for the Cisco cBR Series Routers 1

Information About Dynamic Bandwidth Sharing 2

How to Configure Dynamic Bandwidth Sharing 3

Configuring DBS for a Wideband Cable Interface 3

Configuring DBS for an Integrated Cable Interface 3

Verifying the Dynamic Bandwidth Sharing Configuration 4

Additional References 7

Feature Information for Dynamic Bandwidth Sharing 8

CHAPTER 2 **Modular Quality of Service Command-Line Interface QoS** 9

Finding Feature Information 9

Hardware Compatibility Matrix for the Cisco cBR Series Routers 9

Restrictions for Applying QoS Features Using the MQC 10

About 11

The MQC Structure 11

Elements of a Traffic Class 11

Elements of a Traffic Policy 13

Nested Traffic Classes 14

match-all and match-any Keywords of the class-map Command 15

input and output Keywords of the service-policy Command 15

Benefits of Applying QoS Features Using the MQC 16

How to Apply QoS Features Using the MQC 16

Creating a Traffic Class 16

Creating a Traffic Policy 17

Attaching a Traffic Policy to an Interface Using the MQC 18

Verifying the Traffic Class and Traffic Policy Information 19
Configuration Examples for Applying QoS Features Using the MQC 20
Creating a Traffic Class 20
Creating a Policy Map 20
Example: Attaching a Traffic Policy to an Interface 21
Using the match not Command 21
Configuring a Default Traffic Class 21
How Commands "class-map match-any" and "class-map match-all" Differ 22
Establishing Traffic Class as a Match Criterion (Nested Traffic Classes) 22
Example: Nested Traffic Class for Maintenance 23
Example: Nested Traffic Class to Combine match-any and match-all Characteristics in One Traffic Class 23
Example: Traffic Policy as a QoS Policy (Hierarchical Traffic Policies) 24
How to Configure Input MQC on the Port-Channel Interfaces 24
Creating a Traffic Class 24
Creating a Policy Map 25
Defining QoS Actions in a Policy Map 25
Set Actions 25
Configuring Aggregate Port-Channel Interface 25
Attaching a Traffic Policy to an Interface 26
Example: Configuring Input MQC on the Port-Channel Interfaces 26
Additional References 26
Feature Information for Modular Quality of Service Command-Line Interface QoS 27

CHAPTER 3 **DOCSIS 1.1 for the Cisco CMTS Routers 29**
Hardware Compatibility Matrix for the Cisco cBR Series Routers 29
Prerequisites for DOCSIS 1.1 Operations 30
Restrictions for DOCSIS 1.1 Operations 31
Information about DOCSIS 1.1 33
Baseline Privacy Interface Plus 33
Concatenation 34
Dynamic MAC Messages 34
Enhanced Quality of Service 34
Fragmentation 35

Interoperability 35
Payload Header Suppression 35
Downstream ToS Overwrite 35
DOCSIS 1.1 Quality of Service 36
Service Flow 36
Service Class 37
Packet Classifiers 38
Packet Header Suppression Rules 39
Quality of Service Comparison 39
Enhanced Rate Bandwidth Allocation (ERBA) Support for DOCSIS 1.0 Cable Modems 41
DOCSIS 3.0 Downstream Peak Traffic Rate TLV Support for ERBA 42
Suppressing Upstream and Downstream Peak Rate TLVs for pre DOCSIS 3.0 Cable Modems 43
Downstream Classification Enhancement with MAC Addresses 44
Benefits 44
How to Configure the Cisco CMTS for DOCSIS 1.1 Operations 46
Configuring Baseline Privacy Interface 46
Downloading the DOCSIS Root Certificate to the CMTS 49
Adding a Manufacturer's Certificate as a Trusted Certificate 51
Adding a Certificate as a Trusted Certificate Using SNMP Commands 51
Adding a Manufacturer's or CM Certificate to the Hotlist 53
Adding a Certificate to the Hotlist Using SNMP Commands 53
Enabling Concatenation 54
Enabling DOCSIS Fragmentation 55
Enabling DOCSIS 1.1 Downstream Maximum Transmit Burst on the Cisco cBR-8 Router 57
Monitoring DOCSIS Operations 58
Monitoring the DOCSIS Network 58
Displaying the Status of Cable Modems 58
Displaying a Summary Report for the Cable Modems 60
Displaying the Capabilities of the Cable Modems 61
Displaying Detailed Information About a Particular Cable Modem 61
Monitoring the RF Network and Cable Interfaces 61
Displaying Information About Cloned Cable Modems 61
Denying RF Access For Cable Modems 61
Displaying Information About the Mac Scheduler 61

Displaying Information About QoS Parameter Sets 62
Displaying Information About Service Flows 62
Displaying Information About Service IDs 62
Monitoring BPI+ Operations 62
Displaying the Current BPI+ State of Cable Modems 62
Displaying the BPI+ Timer Values on the CMTS 63
Displaying the Certificate List on the CMTS 63
Configuration Examples for DOCSIS 1.1 Operations 64
Example: DOCSIS 1.1 Configuration for Cisco cBR-8 Router (with BPI+) 64
Additional References 67
Feature Information for DOCSIS 1.1 for Cisco CMTS Routers 68

CHAPTER 4 **Default DOCSIS 1.0 ToS Overwrite 69**
Hardware Compatibility Matrix for the Cisco cBR Series Routers 69
Restrictions for Default DOCSIS 1.0 ToS Overwrite 70
Information About Default DOCSIS 1.0 ToS Overwrite 70
Default DOCSIS 1.0 ToS Overwrite Overview 71
DOCSIS 71
Type-of-Service (ToS) 71
How to Configure Default DOCSIS 1.0 ToS Overwrite 71
Enabling Default DOCSIS 1.0 ToS Overwrite 71
Editing QoS Profiles 73
Additional References 73
Feature Information for Default DOCSIS 1.0 ToS Overwrite 74

CHAPTER 5 **DOCSIS WFQ Scheduler on the Cisco CMTS Routers 75**
Hardware Compatibility Matrix for the Cisco cBR Series Routers 75
Prerequisites for DOCSIS WFQ Scheduler 76
Restrictions for DOCSIS WFQ Scheduler 76
Information About DOCSIS WFQ Scheduler 76
Queue Types 77
Priority Queues 78
CIR Queues 78
Best Effort Queues 78

DOCSIS QoS Support 78
Traffic Priority 79
Maximum Sustained Traffic Rate 80
Minimum Reserved Traffic Rate 80
High Priority Traffic 80
Enhanced Rate Bandwidth Allocation 80
Peak Traffic Rate 81
DOCSIS 3.0 Downstream Bonding Support with Bonding Group Dynamic Bandwidth Sharing 82
How to Configure DOCSIS WFQ Scheduler 82
Mapping DOCSIS Priority to Excess Ratio 82
Verifying the Downstream Queues Information 83
Additional References 83
Feature Information for DOCSIS WFQ Scheduler 84

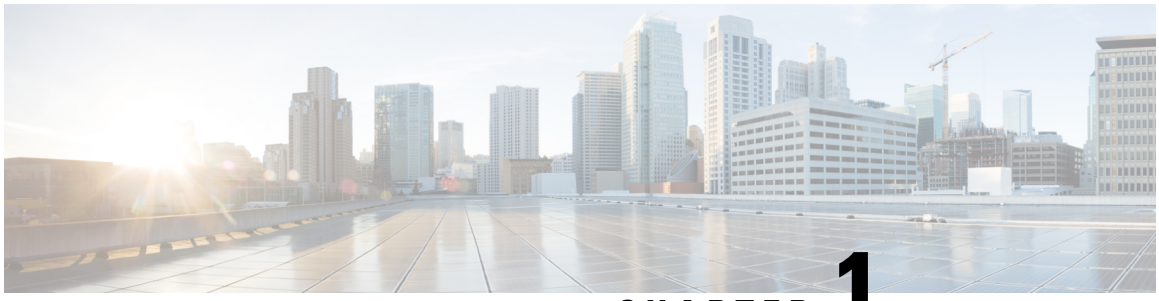
CHAPTER 6 **Fairness Across DOCSIS Interfaces** 85
Hardware Compatibility Matrix for the Cisco cBR Series Routers 85
Prerequisites for Fairness Across DOCSIS Interfaces 86
Restrictions for Fairness Across DOCSIS Interfaces 86
Information About Fairness Across DOCSIS Interfaces 87
On-demand CIR Acquisition 87
Fairness Across Bonding Groups 87
OFDM Channels 88
Interface Bandwidth 88
How to Configure Fairness Across DOCSIS Interfaces 88
Configuring Fairness Across DOCSIS Interfaces 88
Configuring Maximum Excess Information Rate Ratio 89
Configuring Constant Excess Information Rate Demand 90
Configuring Maximum Bonus Bandwidth 91
Verifying the Fairness Across DOCSIS Interfaces 92
Verifying Reservable Bandwidth 92
Verifying Global Fairness Across DOCSIS Interfaces Status and Statistics 93
Verifying Per-Controller Fairness Across DOCSIS Interfaces Status and Statistics 93
Verifying Per-Interface Fairness Across DOCSIS Interfaces Status and Statistics 94
Configuration Examples for Fairness Across DOCSIS Interfaces 94

Example: Fairness Across DOCSIS Interfaces 95
Example: Maximum EIR Demand Ratio 95
Example: Constant EIR Demand 96
Example: Maximum Bonus Bandwidth 96
Additional References 97
Feature Information for Fairness Across DOCSIS Interfaces 97

CHAPTER 7 **Service Group Admission Control** 99
Finding Feature Information 99
Hardware Compatibility Matrix for the Cisco cBR Series Routers 99
Restrictions for Service Group Admission Control 100
Information About Service Group Admission Control 100
Overview 100
SGAC and Downstream Bandwidth Utilization 101
Categorization of Service Flows 101
Thresholds for Downstream Bandwidth 102
Overview of Bonding Group Admission Control 102
How to Configure, Monitor, and Troubleshoot Service Group Admission Control 102
Defining Rules for Service Flow Categorization 102
Naming Application Buckets 105
Preempting High-Priority Emergency 911 Calls 105
Calculating Bandwidth Utilization 106
Enabling SGAC Check 107
Configuration Examples for SGAC 108
Example: SGAC Configuration Commands 108
Example: SGAC for Downstream Traffic 110
Additional References 110
Feature Information for Service Group Admission Control 111

CHAPTER 8 **Subscriber Traffic Management** 113
Hardware Compatibility Matrix for the Cisco cBR Series Routers 114
Restrictions for Subscriber Traffic Management on the Cisco CMTS Routers 114
Information About Subscriber Traffic Management on the Cisco CMTS Routers 115
Feature Overview 115

Feature List 116
Sliding Window for Monitoring Service Flows 117
Weekend Monitoring 118
SNMP Trap Notifications 118
Cable Modem Interaction with the Subscriber Traffic Management Feature 119
How to Configure the Subscriber Traffic Management Feature on the Cisco CMTS Routers 120
Creating and Configuring an Enforce-Rule 120
Examples 123
Configuring Weekend Monitoring 125
Prerequisites 125
Restrictions 125
Configuring Different Legacy Monitoring Conditions for Weekends 125
Configuring Different Peak-Offpeak Monitoring Conditions for Weekends 126
Disabling Weekend Monitoring 127
Removing Weekend Monitoring Conditions and Use the Same Monitoring Criteria Every Day 128
Disabling an Enforce-Rule 129
Removing an Enforce-Rule 129
Changing a Cable Modem Service Class 130
Monitoring the Subscriber Traffic Management Feature on the Cisco CMTS Routers 131
Displaying the Currently Defined Enforce-Rules 131
Displaying the Current Subscriber Usage 133
Configuration Examples for Subscriber Traffic Management on the Cisco CMTS Routers 134
Example: DOCSIS Configuration File and STM Service Classes 134
Example: Downstream Configuration 136
Example: Upstream Configuration 136
Example: Downstream and Upstream Configuration 136
Example: Weekend Monitoring Configuration 137
Additional References 137
Feature Information for Subscriber Traffic Management 139



CHAPTER 1

Dynamic Bandwidth Sharing

The Cisco cBR series router enables dynamic bandwidth sharing (DBS) on integrated cable (IC) and wideband (WB) cable interfaces.

Finding Feature Information

Your software release may not support all the features that are documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. The Feature Information Table at the end of this document provides information about the documented features and lists the releases in which each feature is supported.

Contents

- Hardware Compatibility Matrix for the Cisco cBR Series Routers, on page 1
- Information About Dynamic Bandwidth Sharing, on page 2
- How to Configure Dynamic Bandwidth Sharing, on page 3
- Verifying the Dynamic Bandwidth Sharing Configuration, on page 4
- Additional References, on page 7
- Feature Information for Dynamic Bandwidth Sharing, on page 8

Hardware Compatibility Matrix for the Cisco cBR Series Routers

Note The hardware components that are introduced in a given Cisco IOS-XE Release are supported in all subsequent releases unless otherwise specified.

Table 1: Hardware Compatibility Matrix for the Cisco cBR Series Routers

Cisco CMTS Platform	Processor Engine	Interface Cards
Cisco cBR-8 Converged Broadband Router	**Cisco IOS-XE Release 16.5.1 and Later Releases** Cisco cBR-8 Supervisor: • PID—CBR-SUP-250G • PID—CBR-CCAP-SUP-160G • PID—CBR-CCAP-SUP-60G • PID—CBR-SUP-8X10G-PIC	**Cisco IOS-XE Release 16.5.1 and Later Releases** Cisco cBR-8 CCAP Line Cards: • PID—CBR-LC-8D30-16U30 • PID—CBR-LC-8D31-16U30 • PID—CBR-RF-PIC • PID—CBR-RF-PROT-PIC • PID—CBR-CCAP-LC-40G • PID—CBR-CCAP-LC-40G-R Cisco cBR-8 Downstream PHY Modules: • PID—CBR-D30-DS-MOD • PID—CBR-D31-DS-MOD Cisco cBR-8 Upstream PHY Modules: • PID—CBR-D30-US-MOD • PID—CBR-D31-US-MOD

Information About Dynamic Bandwidth Sharing

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

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 Supervisor switchovers with no loss of functionality.

How to Configure Dynamic Bandwidth Sharing

Dynamic bandwidth sharing is enabled by default on the integrated and wideband cable interfaces on the Cisco cBR router. You can configure the bandwidth allocation for the WB and IC interfaces.

Important Dynamic bandwidth sharing cannot be disabled on the Cisco cBR router.

This section contains the following procedures:

Configuring DBS for a Wideband Cable Interface

Perform the following to configure the bandwidth allocation for a wideband cable interface.

Procedure

	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 wideband-cable** *slot/subslot/portwideband-channel* **Example:** `Router(config)# interface wideband-cable 1/0/0:0`	Configures a wideband cable interface.
Step 4	**cable rf-channel channel-list** *grouplist* [**bandwidth-percent** *bw-percent*] **Example:** `Router(config-if)# cable rf-channel channel-list 10 bandwidth-percent 50`	Configures the bandwidth allocation for the wideband channel interface.

Configuring DBS for an Integrated Cable Interface

Perform this procedure to configure the bandwidth allocation for an integrated cable interface.

Procedure

	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/subslot/portrf-channel* **Example:** `Router(config)# interface integrated-cable 1/0/0:0`	Enters the cable interface mode.
Step 4	**cable rf-bandwidth-percent** *bw-percent* **Example:** `Router(config-if)# cable rf-bandwidth-percent 50`	Configures the bandwidth allocation for the integrated cable interface.

Verifying the Dynamic Bandwidth Sharing Configuration

Use the following commands to verify the dynamic bandwidth sharing information:

- **show controllers Integrated-Cable** *slot/subslot/port* **bandwidth rf-channel**—Displays the bandwidth information for RF channels.

  Following is a sample output of the command:

```
Router# show controllers integrated-Cable 2/0/0 bandwidth rf-channel

Ctrlr    RF       IF          CIR(Kbps)    Guar(Kbps)
2/0/0    0        In2/0/0:0   7500         13750
                  Wi2/0/0:0   7500         13750
                  Wi2/0/0:1   3750         10000
2/0/0    1        In2/0/0:1   7500         13750
                  Wi2/0/0:0   7500         13750
                  Wi2/0/0:1   3750         10000
2/0/0    2        In2/0/0:2   7500         12500
                  Wi2/0/0:0   7500         12500
                  Wi2/0/0:1   7500         12500
2/0/0    3        In2/0/0:3   7500         12500
                  Wi2/0/0:0   7500         12500
                  Wi2/0/0:1   7500         12500
2/0/0    4        In2/0/0:4   7500         12500
                  Wi2/0/0:0   7500         12500
                  Wi2/0/0:1   7500         12500
2/0/0    5        In2/0/0:5   7500         12500
```

```
                 Wi2/0/0:0    7500         12500
                 Wi2/0/0:1    7500         12500
2/0/0    6       In2/0/0:6    7500         12500
                 Wi2/0/0:0    7500         12500
                 Wi2/0/0:1    7500         12500
2/0/0    7       In2/0/0:7    7500         12500
                 Wi2/0/0:0    7500         12500
                 Wi2/0/0:1    7500         12500
2/0/0    8       In2/0/0:8    7500         18750
                 Wi2/0/0:1    7500         18750
                 Wi2/0/0:2    7500         0
2/0/0    9       In2/0/0:9    7500         18750
                 Wi2/0/0:1    7500         18750
                 Wi2/0/0:2    7500         0
2/0/0    10      In2/0/0:10   7500         18750
                 Wi2/0/0:1    7500         18750
                 Wi2/0/0:2    7500         0
2/0/0    11      In2/0/0:11   7500         18750
                 Wi2/0/0:1    7500         18750
                 Wi2/0/0:2    7500         0
2/0/0    12      In2/0/0:12   7500         37500
                 Wi2/0/0:2    7500         0
                 Wi2/0/0:3    7500         0
2/0/0    13      In2/0/0:13   7500         37500
                 Wi2/0/0:2    7500         0
                 Wi2/0/0:3    7500         0
```

- **show controllers Integrated-Cable** *slot/subslot/port* **bandwidth wb-channel**—Displays the bandwidth information for wideband channels.

  Following is a sample output of the command:

```
Router# show controllers Integrated-Cable 2/0/0 bandwidth wb-channel

Ctrlr    WB      RF         CIR(Kbps)    Guar(Kbps)
2/0/0    0                  60000        102500
                 2/0/0:0    7500         13750
                 2/0/0:1    7500         13750
                 2/0/0:2    7500         12500
                 2/0/0:3    7500         12500
                 2/0/0:4    7500         12500
                 2/0/0:5    7500         12500
                 2/0/0:6    7500         12500
                 2/0/0:7    7500         12500
2/0/0    1                  82500        170000
                 2/0/0:0    3750         10000
                 2/0/0:1    3750         10000
                 2/0/0:2    7500         12500
                 2/0/0:3    7500         12500
                 2/0/0:4    7500         12500
                 2/0/0:5    7500         12500
                 2/0/0:6    7500         12500
                 2/0/0:7    7500         12500
                 2/0/0:8    7500         18750
                 2/0/0:9    7500         18750
                 2/0/0:10   7500         18750
                 2/0/0:11   7500         18750
                 2/0/0:32   0            0
                 2/0/0:33   0            0
                 2/0/0:34   0            0
                 2/0/0:35   0            0
2/0/0    2                  60000        0
                 2/0/0:8    7500         0
                 2/0/0:9    7500         0
```

```
2/0/0:10   7500         0
2/0/0:11   7500         0
2/0/0:12   7500         0
2/0/0:13   7500         0
2/0/0:14   7500         0
2/0/0:15   7500         0
2/0/0:64   0            0
2/0/0:65   0            0
2/0/0:66   0            0
2/0/0:67   0            0
```

- **show controllers Integrated-Cable** *slot/subslot/port* **mapping rf-channel**—Displays the mapping for RF channels.

  Following is a sample output of the command:

```
Router# show controllers integrated-Cable 2/0/0 mapping rf-channel

Ctrlr    RF       IC %       IC Rem     WB         WB %      WB Rem
2/0/0    0        20         1          2/0/0:0    20        1
                                       2/0/0:1    10        1
2/0/0    1        20         1          2/0/0:0    20        1
                                       2/0/0:1    10        1
2/0/0    2        20         1          2/0/0:0    20        1
                                       2/0/0:1    20        1
2/0/0    3        20         1          2/0/0:0    20        1
                                       2/0/0:1    20        1
2/0/0    4        20         1          2/0/0:0    20        1
                                       2/0/0:1    20        1
2/0/0    5        20         1          2/0/0:0    20        1
                                       2/0/0:1    20        1
2/0/0    6        20         1          2/0/0:0    20        1
                                       2/0/0:1    20        1
2/0/0    7        20         1          2/0/0:0    20        1
                                       2/0/0:1    20        1
2/0/0    8        20         1          2/0/0:1    20        1
                                       2/0/0:2    20        1
2/0/0    9        20         1          2/0/0:1    20        1
                                       2/0/0:2    20        1
2/0/0    10       20         1          2/0/0:1    20        1
                                       2/0/0:2    20        1
```

- **show controllers Integrated-Cable** *slot/port/interface-number* **mapping wb-channel**—Displays the mapping for wideband channels.

  Following is a sample output of the command:

```
Router# show controllers integrated-Cable 2/0/0 mapping wb-channel

Ctrlr    WB       RF         WB %   WB Rem
2/0/0    0        2/0/0:0    20     1
                  2/0/0:1    20     1
                  2/0/0:2    20     1
                  2/0/0:3    20     1
                  2/0/0:4    20     1
                  2/0/0:5    20     1
                  2/0/0:6    20     1
                  2/0/0:7    20     1
2/0/0    1        2/0/0:0    10     1
                  2/0/0:1    10     1
                  2/0/0:2    20     1
                  2/0/0:3    20     1
                  2/0/0:4    20     1
                  2/0/0:5    20     1
```

```
                    2/0/0:6     20      1
                    2/0/0:7     20      1
                    2/0/0:8     20      1
                    2/0/0:9     20      1
                    2/0/0:10    20      1
                    2/0/0:11    20      1
                    2/0/0:32    20      1
                    2/0/0:33    20      1
                    2/0/0:34    20      1
                    2/0/0:35    20      1
2/0/0     2         2/0/0:8     20      1
                    2/0/0:9     20      1
                    2/0/0:10    20      1
                    2/0/0:11    20      1
                    2/0/0:12    20      1
                    2/0/0:13    20      1
                    2/0/0:14    20      1
                    2/0/0:15    20      1
                    2/0/0:64    20      1
                    2/0/0:65    20      1
                    2/0/0:66    20      1
                    2/0/0:67    20      1
2/0/0     3         2/0/0:12    20      1
                    2/0/0:13    20      1
                    2/0/0:14    20      1
                    2/0/0:15    20      1
                    2/0/0:16    20      1
                    2/0/0:17    20      1
```

Additional References

Related Documents

Related Topic	Document Title
Cisco CMTS cable commands	*Cisco CMTS Cable Command Reference*

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

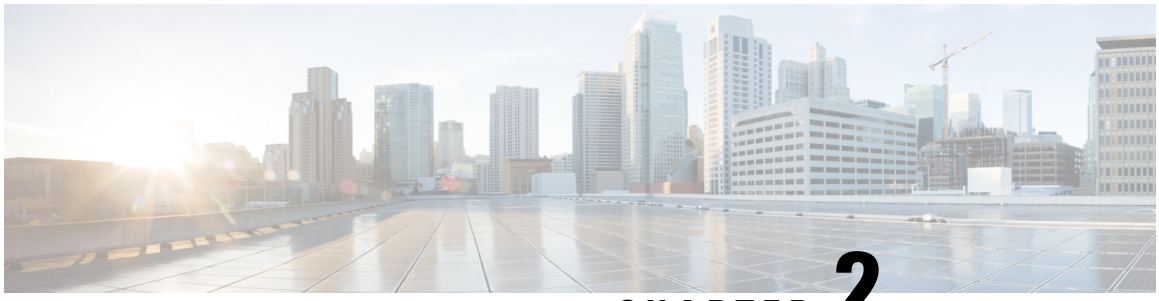
Feature Information for Dynamic Bandwidth Sharing

Use Cisco Feature Navigator to find information about the 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 the www.cisco.com/go/cfn link. An account on the Cisco.com page is not required.

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

Table 2: Feature Information for Dynamic Bandwidth Sharing

Feature Name	Releases	Feature Information
Dynamic bandwidth sharing	Cisco IOS XE Everest 16.6.1	This feature was integrated into Cisco IOS XE Everest 16.6.1 on the Cisco cBR Series Converged Broadband Routers.



CHAPTER 2

Modular Quality of Service Command-Line Interface QoS

This module contains the concepts about applying QoS features using the Modular Quality of Service (QoS) Command-Line Interface (CLI) (MQC) and the tasks for configuring the MQC. The MQC allows you to define a traffic class, create a traffic policy (policy map), and attach the traffic policy to an interface. The traffic policy contains the QoS feature that will be applied to the traffic class.

- Finding Feature Information, on page 9
- Hardware Compatibility Matrix for the Cisco cBR Series Routers, on page 9
- Restrictions for Applying QoS Features Using the MQC, on page 10
- About, on page 11
- How to Apply QoS Features Using the MQC, on page 16
- Configuration Examples for Applying QoS Features Using the MQC, on page 20
- How to Configure Input MQC on the Port-Channel Interfaces, on page 24
- Example: Configuring Input MQC on the Port-Channel Interfaces, on page 26
- Additional References, on page 26
- Feature Information for Modular Quality of Service Command-Line Interface QoS, on page 27

Finding Feature Information

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

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

Hardware Compatibility Matrix for the Cisco cBR Series Routers

Note The hardware components that are introduced in a given Cisco IOS-XE Release are supported in all subsequent releases unless otherwise specified.

Table 3: Hardware Compatibility Matrix for the Cisco cBR Series Routers

Cisco CMTS Platform	Processor Engine	Interface Cards
Cisco cBR-8 Converged Broadband Router	**Cisco IOS-XE Release 16.5.1 and Later Releases** Cisco cBR-8 Supervisor: • PID—CBR-SUP-250G • PID—CBR-CCAP-SUP-160G • PID—CBR-CCAP-SUP-60G • PID—CBR-SUP-8X10G-PIC	**Cisco IOS-XE Release 16.5.1 and Later Releases** Cisco cBR-8 CCAP Line Cards: • PID—CBR-LC-8D30-16U30 • PID—CBR-LC-8D31-16U30 • PID—CBR-RF-PIC • PID—CBR-RF-PROT-PIC • PID—CBR-CCAP-LC-40G • PID—CBR-CCAP-LC-40G-R Cisco cBR-8 Downstream PHY Modules: • PID—CBR-D30-DS-MOD • PID—CBR-D31-DS-MOD Cisco cBR-8 Upstream PHY Modules: • PID—CBR-D30-US-MOD • PID—CBR-D31-US-MOD

Restrictions for Applying QoS Features Using the MQC

The MQC-based QoS does not support classification of legacy Layer 2 protocol packets such as Internetwork Packet Exchange (IPX), DECnet, or AppleTalk. When these types of packets are being forwarded through a generic Layer 2 tunneling mechanism, the packets can be handled by MQC but without protocol classification. As a result, legacy protocol traffic in a Layer 2 tunnel is matched only by a "match any" class or class-default.

The number of QoS policy maps and class maps supported varies by platform and release.

Note The policy map limitations do not refer to the number of applied policy map instances, only to the definition of the policy maps.

About

The MQC Structure

The MQC (Modular Quality of Service (QoS) Command-Line Interface (CLI)) enables you to set packet classification and marking based on a QoS group value. MQC CLI allows you to create traffic classes and policies, enable a QoS feature (such as packet classification), and attach these policies to interfaces.

The MQC structure necessitates developing the following entities: traffic class, policy map, and service policy.

Elements of a Traffic Class

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

The **match** commands are used for classifying packets. Packets are checked to determine whether they meet the criteria specified in the **match**commands; if a packet meets the specified criteria, that packet is considered a member of the class. Packets that fail to meet the matching criteria are classified as members of the default traffic class.

Available match Commands

The table below lists *some* of the available **match** commands that can be used with the MQC. The available **match** commands vary by Cisco IOS XE release. For more information about the commands and command syntax, see the *Cisco IOS Quality of Service Solutions* Command Reference.

Table 4: match Commands That Can Be Used with the MQC

Command	Purpose
match access-group	Configures the match criteria for a class map on the basis of the specified access control list (ACL).
match any	Configures the match criteria for a class map to be successful match criteria for all packets.
match cos	Matches a packet based on a Layer 2 class of service (CoS) marking.
match destination-address mac	Uses the destination MAC address as a match criterion.
match discard-class	Matches packets of a certain discard class.
match [**ip**] **dscp**	Identifies a specific IP differentiated service code point (DSCP) value as a match criterion. Up to eight DSCP values can be included in one match statement.
match input-interface	Configures a class map to use the specified input interface as a match criterion.
match ip rtp	Configures a class map to use the Real-Time Transport Protocol (RTP) port as the match criterion.

Command	Purpose
match mpls experimental	Configures a class map to use the specified value of the Multiprotocol Label Switching (MPLS) experimental (EXP) field as a match criterion.
match mpls experimental topmost	Matches the MPLS EXP value in the topmost label.
match not	Specifies the single match criterion value to use as an unsuccessful match criterion. **Note** The **match not** command, rather than identifying the specific match parameter to use as a match criterion, is used to specify a match criterion that prevents a packet from being classified as a member of the class. For instance, if the **match not qos-group 6** command is issued while you configure the traffic class, QoS group 6 becomes the only QoS group value that is not considered a successful match criterion. All other QoS group values would be successful match criteria.
match packet length	Specifies the Layer 3 packet length in the IP header as a match criterion in a class map.
match port-type	Matches traffic on the basis of the port type for a class map.
match [**ip**] **precedence**	Identifies IP precedence values as match criteria.
match protocol	Configures the match criteria for a class map on the basis of the specified protocol. **Note** A separate **match protocol** (NBAR) command is used to configure network-based application recognition (NBAR) to match traffic by a protocol type known to NBAR.
match protocol fasttrack	Configures NBAR to match FastTrack peer-to-peer traffic.
match protocol gnutella	Configures NBAR to match Gnutella peer-to-peer traffic.
match protocol http	Configures NBAR to match Hypertext Transfer Protocol (HTTP) traffic by URL, host, Multipurpose Internet Mail Extension (MIME) type, or fields in HTTP packet headers.
match protocol rtp	Configures NBAR to match RTP traffic.
match qos-group	Identifies a specific QoS group value as a match criterion.
match source-address mac	Uses the source MAC address as a match criterion.

Multiple match Commands in One Traffic Class

If the traffic class contains more than one **match** command, you need to specify how to evaluate the **match** commands. You specify this by using either the **match-any** or **match-all** keyword of the **class-map** command. Note the following points about the **match-any** and **match-all** keywords:

- If you specify the **match-any** keyword, the traffic being evaluated by the traffic class must match *one* of the specified criteria.
- If you specify the **match-all** keyword, the traffic being evaluated by the traffic class must match *all* of the specified criteria.
- If you do not specify either keyword, the traffic being evaluated by the traffic class must match *all* of the specified criteria (that is, the behavior of the **match-all** keyword is used).

Elements of a Traffic Policy

A traffic policy contains three elements: a traffic policy name, a traffic class (specified with the **class** command), and the command used to enable the QoS feature.

The traffic policy (policy map) applies the enabled QoS feature to the traffic class once you attach the policy map to the interface (by using the **service-policy** command).

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.

Commands Used to Enable QoS Features

The commands used to enable QoS features vary by Cisco IOS XE release. The table below lists *some* of the available commands and the QoS features that they enable. For complete command syntax, see the *Cisco IOS QoS Command Reference*.

For more information about a specific QoS feature that you want to enable, see the appropriate module of the Cisco IOS XE Quality of Service Solutions Configuration Guide.

Table 5: Commands Used to Enable QoS Features

Command	Purpose
bandwidth	Configures a minimum bandwidth guarantee for a class.
bandwidth remaining	Configures an excess weight for a class.
fair-queue	Enables the flow-based queueing feature within a traffic class.
fair-queue pre-classify	Configures and checks whether the **qos pre-classify** command can be used for fair queue. When the **qos pre-classify** command is enabled on the tunnel inteface, and then the **fair-queue pre-classify** command is enabled for the policy-map, the policy-map is attached to either the tunnel interface or the physical interface. The inner IP header of the tunnel will be used for the hash algorithm of the fair queue.
drop	Discards the packets in the specified traffic class.
police	Configures traffic policing.

Command	Purpose
police (percent)	Configures traffic policing on the basis of a percentage of bandwidth available on an interface.
police (two rates)	Configures traffic policing using two rates, the committed information rate (CIR) and the peak information rate (PIR).
priority	Gives priority to a class of traffic belonging to a policy map.
queue-limit	Specifies or modifies the maximum number of packets the queue can hold for a class configured in a policy map.
random-detect	Enables Weighted Random Early Detection (WRED).
random-detect discard-class	Configures the WRED parameters for a discard-class value for a class in a policy map.
random-detect discard-class-based	Configures WRED on the basis of the discard class value of a packet.
random-detect exponential-weighting-constant	Configures the exponential weight factor for the average queue size calculation for the queue reserved for a class.
random-detect precedence	Configure the WRED parameters for a particular IP Precedence for a class policy in a policy map.
service-policy	Specifies the name of a traffic policy used as a matching criterion (for nesting traffic policies [hierarchical traffic policies] within one another).
set atm-clp	Sets the cell loss priority (CLP) bit when a policy map is configured.
set cos	Sets the Layer 2 class of service (CoS) value of an outgoing packet.
set discard-class	Marks a packet with a discard-class value.
set [**ip**] **dscp**	Marks a packet by setting the differentiated services code point (DSCP) value in the type of service (ToS) byte.
set fr-de	Changes the discard eligible (DE) bit setting in the address field of a Frame Relay frame to 1 for all traffic leaving an interface.
set mpls experimental	Designates the value to which the MPLS bits are set if the packets match the specified policy map.
set precedence	Sets the precedence value in the packet header.
set qos-group	Sets a QoS group identifier (ID) that can be used later to classify packets.
shape	Shapes traffic to the indicated bit rate according to the algorithm specified.

Nested Traffic Classes

The MQC does not necessarily require that you associate only one traffic class to one traffic policy.

In a scenario where packets satisfy more than one match criterion, the MQC enables you to associate multiple traffic classes with a single traffic policy (also termed nested traffic classes) using the **match class-map** command. (We term these *nested class maps* or *MQC Hierarchical class maps*.) This command provides the only method of combining match-any and match-all characteristics within a single traffic class. By doing so, you can create a traffic class using one match criterion evaluation instruction (either match-any or match-all) and then use that traffic class as a match criterion in a traffic class that uses a different match criterion type. For example, a traffic class created with the match-any instruction must use a class configured with the match-all instruction as a match criterion, or vice versa.

Consider this likely scenario: Suppose A, B, C, and D were all separate match criterion, and you wanted traffic matching A, B, or C and D (i.e., A or B or [C and D]) to be classified as belonging to a traffic class. Without the nested traffic class, traffic would either have to match all four of the match criterion (A and B and C and D) or match any of the match criterion (A or B or C or D) to be considered part of the traffic class. You would not be able to combine "and" (match-all) and "or" (match-any) statements within the traffic class; you would be unable to configure the desired configuration.

The solution: Create one traffic class using match-all for C and D (which we will call criterion E), and then create a new match-any traffic class using A, B, and E. The new traffic class would have the correct evaluation sequence (A or B or E, which is equivalent to A or B or [C and D]).

match-all and match-any Keywords of the class-map Command

One of the commands used when you create a traffic class is the **class-map** command. The command syntax for the **class-map** command includes two keywords: **match-all** and **match-any** . The **match-all** and **match-any** keywords need to be specified only if more than one match criterion is configured in the traffic class. Note the following points about these keywords:

- The **match-all** keyword is used when *all* of the match criteria in the traffic class must be met in order for a packet to be placed in the specified traffic class.
- The **match-any** keyword is used when only *one* of the match criterion in the traffic class must be met in order for a packet to be placed in the specified traffic class.
- If neither the **match-all** keyword nor **match-any** keyword is specified, the traffic class will behave in a manner consistent with the **match-all** keyword.

input and output Keywords of the service-policy Command

As a general rule, the QoS features configured in the traffic policy can be applied to packets entering the interface or to packets leaving the interface. Therefore, when you use the **service-policy** command, you need to specify the direction of the traffic policy by using the **input** or **output** keyword.

For instance, the **service-policy output policy-map1** command would apply the QoS features in the traffic policy to the interface in the output direction. All packets leaving the interface (output) are evaluated according to the criteria specified in the traffic policy named policy-map1.

Note For Cisco releases, queueing mechanisms are not supported in the input direction. Nonqueueing mechanisms (such as traffic policing and traffic marking) are supported in the input direction. Also, classifying traffic on the basis of the source MAC address (using the **match source-address mac** command) is supported in the input direction only.

Benefits of Applying QoS Features Using the MQC

The MQC structure allows you to create the traffic policy (policy map) once and then apply it to as many traffic classes as needed. You can also attach the traffic policies to as many interfaces as needed.

How to Apply QoS Features Using the MQC

Creating a Traffic Class

To create a traffic class, use the **class-map** command to specify the traffic class name. Then use one or more **match** commands to specify the appropriate match criteria. Packets matching the criteria that you specify are placed in the traffic class. For more information about the **match-all** and **match-any** keywords of the class-map comand, see the "match-all and match-any Keywords of the class-map Command" section.

Note The **match cos** command is shown in Step 4. The **match cos** command is simply an example of one of the **match** commands that you can use. For information about the other available **match** commands, see the "match-all and match-any Keywords of the class-map Command" section.

Procedure

	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-map-name* **Example:** `Router(config)# class-map match-any 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. • Enter the class name. **Note** The **match-all** keyword specifies that all match criteria must be met. The **match-any** keyword specifies that one of the match criterion must be met. Use these keywords only if you will be specifying more than one **match** command.

	Command or Action	Purpose
Step 4	**match cos** *cos-number* **Example:** `Router(config-cmap)# match cos 2`	Matches a packet on the basis of a Layer 2 class of service (CoS) number. • Enter the CoS number. **Note** The **match cos** command is an example of the **match** commands you can use. For information about the other **match** commands that are available, see the "match-all and match-any Keywords of the class-map Command" section.
Step 5	Enter additional match commands, if applicable; otherwise, continue with step 6.	--
Step 6	**end** **Example:** `Router(config-cmap)# end`	(Optional) Exits QoS class-map configuration mode and returns to privileged EXEC mode.

Creating a Traffic Policy

Note The **bandwidth** command is shown in Step 5. The **bandwidth** command is an example of the commands that you can use in a policy map to enable a QoS feature (in this case, Class-based Weighted Fair Queuing (CBWFQ). For information about other available commands, see the "Elements of a Traffic Policy" section.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**policy-map** *policy-map-name* **Example:** `Router(config)# policy-map policy1`	Creates or specifies the name of the traffic policy and enters QoS policy-map configuration mode. • Enter the policy map name.

	Command or Action	Purpose
Step 4	**class** { *class-name* | **class-default** } **Example:** `Router(config-pmap)# class class1`	Specifies the name of a traffic class and enters QoS policy-map class configuration mode. **Note** This step associates the traffic class with the traffic policy.
Step 5	**bandwidth** {*bandwidth-kbps* | **percent** *percent* } **Example:** `Router(config-pmap-c)# bandwidth 3000`	(Optional) Specifies a minimum bandwidth guarantee to a traffic class in periods of congestion. • A minimum bandwidth guarantee can be specified in kb/s or by a percentage of the overall available bandwidth. **Note** The **bandwidth** command enables CBWFQ. The **bandwidth** command is an example of the commands that you can use in a policy map to enable a QoS feature. For information about the other commands available, see the "Elements of a Traffic Policy" section.
Step 6	Enter the commands for any additional QoS feature that you want to enable, if applicable; otherwise, continue with Step 7.	--
Step 7	**end** **Example:** `Router(config-pmap-c)# end`	(Optional) Exits QoS policy-map class configuration mode and returns to privileged EXEC mode.

Attaching a Traffic Policy to an Interface Using the MQC

Procedure

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

	Command or Action	Purpose
Step 3	**interface** *type number* **Example:** `Router(config)# interface TenGigabitEthernet 4/1/0`	Configures an interface type and enters interface configuration mode. • Enter the interface type and interface number.
Step 4	**service-policy** {**input** | **output**} *policy-map-name* **Example:** `Router(config-if)# service-policy input policy1`	Attaches a policy map to an interface. • Enter either the **input** or **output** keyword and the policy map name.
Step 5	**end** **Example:** `Router(config-if)# end`	(Optional) Exits interface configuration mode and returns to privileged EXEC mode.

Verifying the Traffic Class and Traffic Policy Information

The show commands described in this section are optional and can be entered in any order.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show class-map** **Example:** `Router# show class-map`	(Optional) Displays all class maps and their matching criteria.
Step 3	**show policy-map** *policy-map-name* **class** *class-name* **Example:** `Router# show policy-map policy1 class class1`	(Optional) Displays the configuration for the specified class of the specified policy map. • Enter the policy map name and the class name.
Step 4	**show policy-map** **Example:** `Router# show policy-map`	(Optional) Displays the configuration of all classes for all existing policy maps.

	Command or Action	Purpose
Step 5	**show policy-map interface** *type number* **Example:** `Router# show policy-map interface TengigabitEthernet 4/1/0`	(Optional) Displays the statistics and the configurations of the input and output policies that are attached to an interface. • Enter the interface type and number.
Step 6	**exit** **Example:** `Router# exit`	(Optional) Exits privileged EXEC mode.

Configuration Examples for Applying QoS Features Using the MQC

Creating a Traffic Class

In the following example, we create traffic classes and define their match criteria. For the first traffic class (class1), we use access control list (ACL) 101 as match criteria; for the second traffic class (class2), ACL 102. We check the packets against the contents of these ACLs to determine if they belong to the class.

```
class-map class1
  match access-group 101
  exit
class-map class2
  match access-group 102
  end
```

Creating a Policy Map

In the following example, we define a traffic policy (policy1) containing the QoS features that we will apply to two classes: class1 and class2. The match criteria for these classes were previously defined in Creating a Traffic Class, on page 20).

For class1, the policy includes a bandwidth allocation request and a maximum packet count limit for the queue reserved for that class. For class2, the policy specifies only a bandwidth allocation request.

```
policy-map policy1
  class class1
    bandwidth 3000
    queue-limit 30
    exit
  class class2
    bandwidth 2000
    end
```

Example: Attaching a Traffic Policy to an Interface

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 in the input direction and only one traffic policy attached in the output direction.

```
Router(config)# interface TengigabitEthernet 4/1/0
Router(config-if)# service-policy output policy1
Router(config-if)# exit
Router(config)# interface TengigabitEthernet 4/1/0
Router(config-if)# service-policy output policy1
Router(config-if)# end
```

Using the match not Command

Use the **match not** command to specify a QoS policy value that is not used as a match criterion. All other values of that QoS policy become successful match criteria. For instance, if you issue the **match not qos-group 4** command in QoS class-map configuration mode, the specified class will accept all QoS group values except 4 as successful match criteria.

In the following traffic class, all protocols except IP are considered successful match criteria:

```
class-map noip
  match not protocol ip
  end
```

Configuring a Default Traffic Class

Traffic that does not meet the match criteria specified in the traffic classes (that is, *unclassified traffic*) is treated as belonging to the default traffic class.

If you do not configure a default class, packets are still treated as members of that class. The default class has no QoS features enabled so packets belonging to this class have no QoS functionality. Such packets are placed into a first-in, first-out (FIFO) queue managed by tail drop, which is a means of avoiding congestion that treats all traffic equally and does not differentiate between classes of service. Queues fill during periods of congestion. When the output queue is full and tail drop is active, packets are dropped until the congestion is eliminated and the queue is no longer full.

The following example configures a policy map (policy1) for the default class (always called class-default) with these characteristics: 10 queues for traffic that does not meet the match criteria of other classes whose policy is defined by class policy1, and a maximum of 20 packets per queue before tail drop is enacted to handle additional queued packets.

In the following example, we configure a policy map (policy1) for the default class (always termed class-default) with these characteristics: 10 queues for traffic that does not meet the match criterion of other classes whose policy is defined by the traffic policy policy1.

```
policy-map policy1
  class class-default
    shape average 100m
```

How Commands "class-map match-any" and "class-map match-all" Differ

This example shows how packets are evaluated when multiple match criteria exist. It illustrates the difference between the **class-map match-any** and **class-map match-all** commands. Packets must meet either all of the match criteria (**match-all**) or one of the match criteria (**match-any**) to be considered a member of the traffic class.

The following examples show a traffic class configured with the **class-map match-all** command:

```
class-map match-all cisco1
  match qos-group 4
  match access-group 101
```

If a packet arrives on a router with traffic class cisco1 configured on the interface, we assess whether it matches the IP protocol, QoS group 4, and access group 101. If all of these match criteria are met, the packet is classified as a member of the traffic class cisco1 (a logical AND operator; Protocol IP AND QoS group 4 AND access group 101).

```
class-map match-all vlan
  match vlan 1
  match vlan inner 1
```

The following example illustrates use of the **class-map match-any** command. Only one match criterion must be met for us to classify the packet as a member of the traffic class (i.e., a logical OR operator; protocol IP OR QoS group 4 OR access group 101):

```
class-map match-any cisco2
  match protocol ip
  match qos-group 4
  match access-group 101
```

In the traffic class cisco2, the match criterion are evaluated consecutively until a successful match is located. The packet is first evaluated to determine whether the IP protocol can be used as a match criterion. If so, the packet is matched to traffic class cisco2. If not, then QoS group 4 is evaluated as a match criterion and so on. If the packet matches none of the specified criteria, the packet is classified as a member of the default traffic class (*class default-class*).

Establishing Traffic Class as a Match Criterion (Nested Traffic Classes)

There are two reasons to use the **match class-map** command. One reason is maintenance; if a large traffic class currently exists, using the traffic class match criterion is easier than retyping the same traffic class configuration. The second and more common reason is to mix match-all and match-any characteristics in one traffic policy. This enables you to create a traffic class using one match criterion evaluation instruction (either match-any or match-all) and then use that traffic class as a match criterion in a traffic class that uses a different match criterion type.

Consider this likely scenario: Suppose A, B, C, and D were all separate match criterion, and you wanted traffic matching A, B, or C and D (i.e., A or B or [C and D]) to be classified as belonging to a traffic class. Without the nested traffic class, traffic would either have to match all four of the match criterion (A and B and C and D) or match any of the match criterion (A or B or C or D) to be considered part of the traffic class. You would not be able to combine “and” (match-all) and “or” (match-any) statements within the traffic class; you would be unable to configure the desired configuration.

The solution: Create one traffic class using match-all for C and D (which we will call criterion E), and then create a new match-any traffic class using A, B, and E. The new traffic class would have the correct evaluation sequence (A or B or E, which is equivalent to A or B or [C and D]).

Example: Nested Traffic Class for Maintenance

In the following example, the traffic class called class1 has the same characteristics as the traffic class called class2, with the exception that traffic class class1 has added a destination address as a match criterion. Rather than configuring traffic class class1 line by line, you can enter the **match class-map class2** command. This command allows all of the characteristics in the traffic class called class2 to be included in the traffic class called class1, and you can add the new destination address match criterion without reconfiguring the entire traffic class.

```
Router(config)# class-map match-any class2
Router(config-cmap)# match protocol ip
Router(config-cmap)# match qos-group 3
Router(config-cmap)# match access-group 2
Router(config-cmap)# exit
Router(config)# class-map match-all class1
Router(config-cmap)# match class-map class2
Router(config-cmap)# match destination-address mac 0000.0000.0000
Router(config-cmap)# exit
```

Example: Nested Traffic Class to Combine match-any and match-all Characteristics in One Traffic Class

The only method of including both match-any and match-all characteristics in a single traffic class is to use the **match class-map** command. To combine match-any and match-all characteristics into a single class, use the match-any instruction to create a traffic class that uses a class configured with the match-all instruction as a match criterion (through the **match class-map** command).

The following example shows how to combine the characteristics of two traffic classes, one with match-any and one with match-all characteristics, into one traffic class with the **match class-map** command. The result requires a packet to match one of the following three match criteria to be considered a member of traffic class class4: IP protocol *and* QoS group 4, destination MAC address 00.00.00.00.00.00, or access group 2.

In this example, only the traffic class called class4 is used with the traffic policy called policy1.

```
Router(config)# class-map match-all class3
Router(config-cmap)# match protocol ip
Router(config-cmap)# match qos-group 4
Router(config-cmap)# exit
Router(config)# class-map match-any class4
Router(config-cmap)# match class-map class3
Router(config-cmap)# match destination-address mac 00.00.00.00.00.00
Router(config-cmap)# match access-group 2
Router(config-cmap)# exit
Router(config)# policy-map policy1
Router(config-pmap)# class class4
Router(config-pmap-c)# police 8100 1500 2504 conform-action transmit exceed-action
set-qos-transmit 4
Router(config-pmap-c)# end
```

Example: Traffic Policy as a QoS Policy (Hierarchical Traffic Policies)

A traffic policy can be included in a QoS policy when the **service-policy** command is used in QoS policy-map class configuration mode. A traffic policy that contains a traffic policy is called a hierarchical traffic policy.

A hierarchical traffic policy contains a child policy and a parent policy. The child policy is the previously defined traffic policy that is being associated with the new traffic policy through the use of the **service-policy** command. The new traffic policy using the preexisting traffic policy is the parent policy. In the example in this section, the traffic policy called child is the child policy and traffic policy called parent is the parent policy.

Hierarchical traffic policies can be attached to subinterfaces. When hierarchical traffic policies are used, a single traffic policy (with a child and parent policy) can be used to shape and priority traffic on subinterfaces.

```
Router(config)# policy-map child
Router(config-pmap)# class voice
Router(config-pmap-c)# priority 50
Router(config)# policy-map parent
Router(config-pmap)# class class-default
Router(config-pmap-c)# shape average 10000000
Router(config-pmap-c)# service-policy child
```

The value used with the **shape** command is provisioned from the committed information rate (CIR) value from the service provider.

How to Configure Input MQC on the Port-Channel Interfaces

To configure input MQC on a port-channel interface to differentiate traffic flow 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.

Creating a Traffic Class

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.

To create traffic classes and define their match criteria, complete the following procedure:

```
configure terminal
class-map class
match type
```

Creating a Policy Map

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.

To define a traffic policy, complete the following procedure:

```
configure terminal
policy-map policy
class class
```

Defining QoS Actions in a Policy Map

Action commands can be added from within class mode on a policy map.

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.

To define a set action, complete the following procedure:

```
configure terminal
policy-map policy
class class
set option
```

Configuring Aggregate Port-Channel Interface

To configure port-channel interface, complete the following procedure:

```
configure terminal
platform qos port-channel-aggregate port_channel_number
interface port-channel port_channel_number
ip address ip musk
interface name
channel-group number
```

Attaching a 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 in the input direction and only one traffic policy attached in the output direction.

To attach a traffic policy to an interface, complete the following procedure:

```
configure terminal
interface port-channel port_channel_number
service-policy input policy
```

Example: Configuring Input MQC on the Port-Channel Interfaces

The following example shows how to configure input MQC on the port-channel interfaces.

```
Router# configure terminal
Router(config)# class-map class1
Router(config-cmap)# match any
Router(config-cmap)# exit
Router(config)# policy-map policy1
Router(config-pmap)# class class1
Router(config-pmap-c)# set dscp af11
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# platform qos port-channel-aggregate 2 Router(config)# interface port-channel
 2
Router(config-if)# ip address 192.168.0.1 255.255.255.0
Router(config-if)# no shut
Router(config-if)# interface tenGigabitEthernet 4/1/1
Router(config-if)# no ip address
Router(config-if)# no shut
Router(config-if)# channel-group 2
Router(config-if)# interface port-channel 2
Router(config-if)# service-policy input policy1
Device(config-if)# end
```

Additional References

Related Documents

Related Topic	Document Title
QoS commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	*Cisco IOS Quality of Service Solutions Command Reference*
Packet classification	“Classifying Network Traffic” module
Frame Relay Fragmentation (FRF) PVCs	“FRF .20 Support” module
Selective Packet Discard	“IPv6 Selective Packet Discard” module

Related Topic	Document Title
Scaling and performance information	"Broadband Scalability and Performance" module of the Cisco ASR 1000 Series Aggregation Services Routers Software Configuration Guide .

Technical Assistance

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

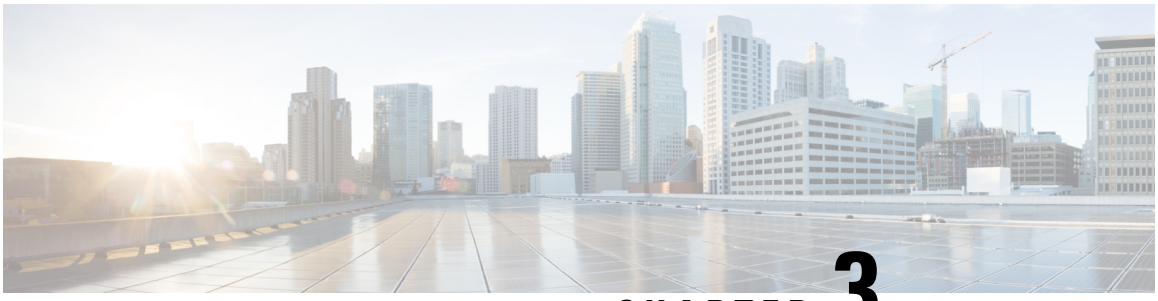
Feature Information for Modular Quality of Service Command-Line Interface QoS

Use Cisco Feature Navigator to find information about the 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 the www.cisco.com/go/cfn link. An account on the Cisco.com page is not required.

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

Table 6: Feature Information for Modular Quality of Service Command-Line Interface QoS

Feature Name	Releases	Feature Information
Modular Quality of Service Command-Line Interface QoS	Cisco IOS XE Everest 16.6.1	This feature was integrated into Cisco IOS XE Everest 16.6.1 on Cisco cBR Series Converged Broadband Routers.
Service Policy on Port-Channel Interfaces	Cisco IOS XE Everest 16.6.1	This feature was integrated into Cisco IOS XE Everest 16.6.1 on Cisco cBR Series Converged Broadband Routers.



CHAPTER 3

DOCSIS 1.1 for the Cisco CMTS Routers

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 that are documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. The Feature Information Table at the end of this document provides information about the documented features and lists the releases in which each feature is supported.

Contents

- Hardware Compatibility Matrix for the Cisco cBR Series Routers, on page 29
- Prerequisites for DOCSIS 1.1 Operations, on page 30
- Restrictions for DOCSIS 1.1 Operations, on page 31
- Information about DOCSIS 1.1, on page 33
- How to Configure the Cisco CMTS for DOCSIS 1.1 Operations, on page 46
- Monitoring DOCSIS Operations, on page 58
- Configuration Examples for DOCSIS 1.1 Operations, on page 64
- Additional References, on page 67
- Feature Information for DOCSIS 1.1 for Cisco CMTS Routers, on page 68

Hardware Compatibility Matrix for the Cisco cBR Series Routers

Note The hardware components that are introduced in a given Cisco IOS-XE Release are supported in all subsequent releases unless otherwise specified.

Table 7: Hardware Compatibility Matrix for the Cisco cBR Series Routers

Cisco CMTS Platform	Processor Engine	Interface Cards
Cisco cBR-8 Converged Broadband Router	**Cisco IOS-XE Release 16.5.1 and Later Releases** Cisco cBR-8 Supervisor: • PID—CBR-SUP-250G • PID—CBR-CCAP-SUP-160G • PID—CBR-CCAP-SUP-60G • PID—CBR-SUP-8X10G-PIC	**Cisco IOS-XE Release 16.5.1 and Later Releases** Cisco cBR-8 CCAP Line Cards: • PID—CBR-LC-8D30-16U30 • PID—CBR-LC-8D31-16U30 • PID—CBR-RF-PIC • PID—CBR-RF-PROT-PIC • PID—CBR-CCAP-LC-40G • PID—CBR-CCAP-LC-40G-R Cisco cBR-8 Downstream PHY Modules: • PID—CBR-D30-DS-MOD • PID—CBR-D31-DS-MOD Cisco cBR-8 Upstream PHY Modules: • PID—CBR-D30-US-MOD • PID—CBR-D31-US-MOD

Prerequisites for DOCSIS 1.1 Operations

To support DOCSIS 1.1 operations, 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 cBR-8 Router

The current Cisco IOS-XE releases do not support using BPI+ encrypted multicast on bundled cable subinterfaces on the Cisco cBR-8 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 cBR-8 router.

BPI+ Not Supported with High Availability Configurations

The current Cisco IOS-XE 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.

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

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.

To display the ToS value, use the **show cable modem qos verbose** command as shown in the following example:

```
Router# show cable modem 30.140.0.41 qos verbose
Load for five secs: 5%/0%; one minute: 4%; five minutes: 4%
Time source is NTP, 15:22:46.911 CST Wed Apr 25 2018

Sfid: 29
Current State: Active
```

```
Sid: 8
Service Class Name:
Traffic Priority: 0
Maximum Sustained rate: 0 bits/sec
Maximum Burst: 3044 bytes
Minimum Reserved rate: 0 bits/sec
Minimum Packet Size: 0 bytes
Admitted QoS Timeout: 200 seconds
Active QoS Timeout: 0 seconds
Maximum Concatenated Burst: 1522 bytes
Scheduling Type: Best Effort
Request/Transmission policy: 0x0
IP ToS Overwrite[AND-mask, OR-mask]: 0xFF, 0x0
Peak Rate: 0 bits/sec
Current Throughput: 545 bits/sec, 0 packets/sec

Sfid: 30
Current State: Active
Sid: N/A
Low Latency App: No
Service Class Name:
Traffic Priority: 0
Maximum Sustained rate: 0 bits/sec
Maximum Burst: 3044 bytes
Minimum Reserved rate: 0 bits/sec
Minimum Packet Size: 0 bytes
Admitted QoS Timeout: 200 seconds
Active QoS Timeout: 0 seconds
Maximum Latency: 0 usecs
IP ToS Overwrite[AND-mask, OR-mask]: 0xFF, 0x0
Peak Rate: 0 bits/sec
Current Throughput: 446 bits/sec, 0 packets/sec
```

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

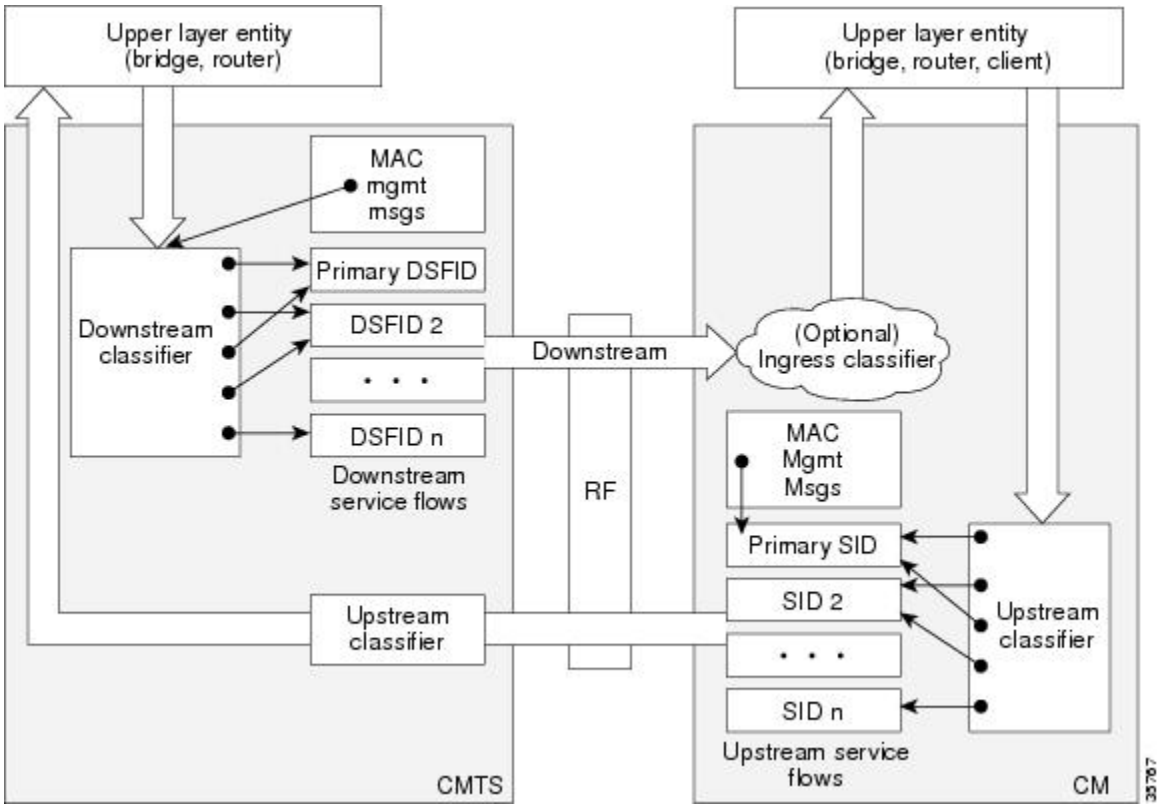
In DOCSIS 1.0 networks, a cable modem used only one set of QoS parameters for all of its traffic, so the CMTS simply had to route packets to and from the appropriate cable modems. In DOCSIS 1.1 networks, however, cable modems can be using multiple service flows, and each service flow can be given a different 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 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, 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 and CMTS 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 8: 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.
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

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 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.
- 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 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 cBR-8 Converged Broadband Router, the **cable ds-max-burst** command is used to control this behavior explicitly.

The *peak-rate* keyword is introduced to specify the peak rate an ERBA-enabled service flow can use. The peak rate value is applied to a specific service flow 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.

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*.

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 43.

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 cBR-8 router.

Table 9: Enhanced Rate Bandwidth Allocation Support for the Cisco cBR-8 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 cBR-8 routers, the dual token bucket-based shaper is used to support ERBA on the Cisco cBR-8 CCAP line card (the ERBA feature is always enabled on the Cisco cBR-8 CCAP 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 cBR-8 routers.

Table 10: 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

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.

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. 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. The downstream classifier combinations that are supported on the router are listed below:

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 67.

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 %CBR-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.

Procedure

	Command or Action	Purpose

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

	Command or Action	Purpose

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

Step 3	**interface cable***slot /subslot /port*
	Example:
	`Router(config)# interface cable 6/0/0`
	`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 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 6	**cable privacy authorize-multicast** **Example:** `Router(config-if)# cable privacy`	(Optional) Enables BPI+ encryption on the cable interface and uses AAA protocols to authorize all multicast stream (IGMP) join requests.

	Command or Action	Purpose
	`authorize-multicast` `Router(config-if)#`	**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 7	**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 8	**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.

Step 9	**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 10	**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 11	**exit**
	Example:
	`Router(config-if)# exit`
	`Router(config)#`
		Exits interface configuration mode.
		Note Repeat steps Step 3, on page 47 through Step 11, on page 48 for each cable interface.

Step 12	**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 11: 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.
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 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.

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:

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
cbrsup-universalk9.2015-03-18_03.30_johuynh.SSA.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 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
cbrsup-universalk9.2015-03-18_03.30_johuynh.SSA.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

The 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 SNMP commands, as described in the following section:

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.

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 51, 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:

Procedure

	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.

	Command or Action	Purpose

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:

Procedure

	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:**	Enters interface configuration mode for the cable interface line card at this particular slot.

	Command or Action	Purpose
	`Router(config)# interface cable 6/0` `Router(config-if)#`	

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 unfrag-slot-jitter limit 2000 cac-enforce`
	`Router(config-if)#`
		(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.
		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.

Example

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 cBR-8 Router

Perform the following steps to configure ERBA on the Cisco cBR-8 router. This procedure and the associated commands are subject to the guidelines and restrictions cited in this document.

Procedure

	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* **Example:** `Router(config)# cable ds-max-burst burst-threshold 2048`	Enables the support for DOCSIS 1.1 downstream max burst. To remove this configuration, use the **no** form of this command.

	Command or Action	Purpose
Step 4	**cable service class** *class-index* **peak-rate** *peak-rate* **Example:** `Router(config)# cable service class 1 peak-rate 1000`	Set the peak-rate value of a specific service class.

Step 5	**Ctrl^Z**
	Example:
	`Router(config)# Ctrl^Z`
	`Router#`
		Returns to privileged EXEC mode.

Example

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.

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.

Displaying the Status of Cable Modems

To display a list of known cable modems and their current status, use the **show cable modem** command.

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.

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

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

Table 12: 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).
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.

MAC State Value	Description
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. It can 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.
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.

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

Displaying the Capabilities of the Cable Modems

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

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

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.

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

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.

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.

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.

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.

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.

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

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.

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.

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

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

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

Table 13: 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+.

State	Description
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: `%CBR-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.

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 cBR-8 Router (with BPI+)

```
version 12.2
service timestamps log datetime msec localtime
service password-encryption
!
hostname cBR-8
!
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:

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

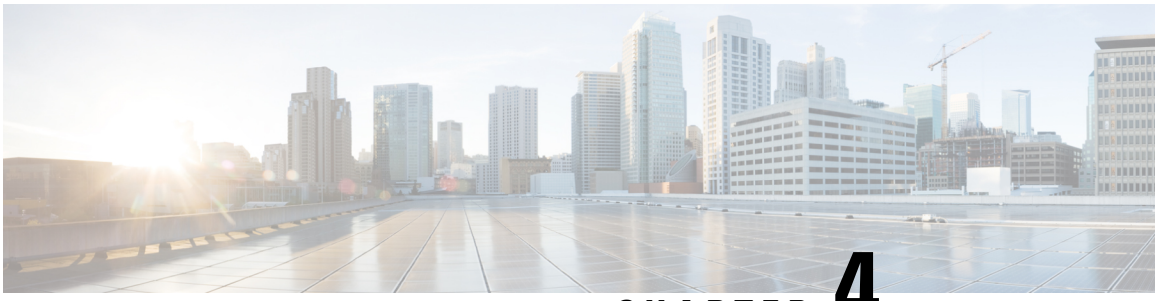
Feature Information for DOCSIS 1.1 for Cisco CMTS Routers

Use Cisco Feature Navigator to find information about the 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 the www.cisco.com/go/cfn link. An account on the Cisco.com page is not required.

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

Table 14: Feature Information for DOCSIS 1.1 for the Cisco CMTS Routers

Feature Name	Releases	Feature Information
DOCSIS 1.1 for the Cisco CMTS Routers	Cisco IOS XE Everest 16.6.1	This feature was integrated into Cisco IOS XE Everest 16.6.1 on Cisco cBR Series Converged Broadband Routers.



CHAPTER 4

Default DOCSIS 1.0 ToS Overwrite

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 that are documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. The Feature Information Table at the end of this document provides information about the documented features and lists the releases in which each feature is supported.

Contents

- Hardware Compatibility Matrix for the Cisco cBR Series Routers, on page 69
- Restrictions for Default DOCSIS 1.0 ToS Overwrite, on page 70
- Information About Default DOCSIS 1.0 ToS Overwrite, on page 70
- How to Configure Default DOCSIS 1.0 ToS Overwrite, on page 71
- Additional References, on page 73
- Feature Information for Default DOCSIS 1.0 ToS Overwrite, on page 74

Hardware Compatibility Matrix for the Cisco cBR Series Routers

Note The hardware components that are introduced in a given Cisco IOS-XE Release are supported in all subsequent releases unless otherwise specified.

Table 15: Hardware Compatibility Matrix for the Cisco cBR Series Routers

Cisco CMTS Platform	Processor Engine	Interface Cards
Cisco cBR-8 Converged Broadband Router	**Cisco IOS-XE Release 16.5.1 and Later Releases** Cisco cBR-8 Supervisor: • PID—CBR-SUP-250G • PID—CBR-CCAP-SUP-160G • PID—CBR-CCAP-SUP-60G • PID—CBR-SUP-8X10G-PIC	**Cisco IOS-XE Release 16.5.1 and Later Releases** Cisco cBR-8 CCAP Line Cards: • PID—CBR-LC-8D30-16U30 • PID—CBR-LC-8D31-16U30 • PID—CBR-RF-PIC • PID—CBR-RF-PROT-PIC • PID—CBR-CCAP-LC-40G • PID—CBR-CCAP-LC-40G-R Cisco cBR-8 Downstream PHY Modules: • PID—CBR-D30-DS-MOD • PID—CBR-D31-DS-MOD Cisco cBR-8 Upstream PHY Modules: • PID—CBR-D30-US-MOD • PID—CBR-D31-US-MOD

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 then 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.

Procedure

	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 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.

Procedure

	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 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.

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

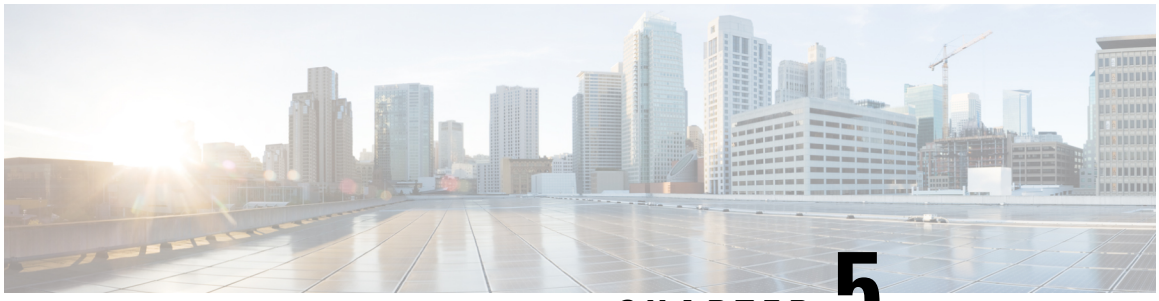
Feature Information for Default DOCSIS 1.0 ToS Overwrite

Use Cisco Feature Navigator to find information about the 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 the www.cisco.com/go/cfn link. An account on the Cisco.com page is not required.

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

Table 16: Feature Information for Default DOCSIS 1.0 ToS Overwrite

Feature Name	Releases	Feature Information
Default DOCSIS 1.0 ToS overwrite	Cisco IOS XE Everest 16.6.1	This feature was integrated into Cisco IOS XE Everest 16.6.1 on the Cisco cBR Series Converged Broadband Routers.



CHAPTER 5

DOCSIS WFQ Scheduler on the Cisco CMTS Routers

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 that are documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. The Feature Information Table at the end of this document provides information about the documented features and lists the releases in which each feature is supported.

Contents

- Hardware Compatibility Matrix for the Cisco cBR Series Routers, on page 75
- Prerequisites for DOCSIS WFQ Scheduler, on page 76
- Restrictions for DOCSIS WFQ Scheduler, on page 76
- Information About DOCSIS WFQ Scheduler, on page 76
- How to Configure DOCSIS WFQ Scheduler , on page 82
- Additional References, on page 83
- Feature Information for DOCSIS WFQ Scheduler, on page 84

Hardware Compatibility Matrix for the Cisco cBR Series Routers

Note The hardware components that are introduced in a given Cisco IOS-XE Release are supported in all subsequent releases unless otherwise specified.

Table 17: Hardware Compatibility Matrix for the Cisco cBR Series Routers

Cisco CMTS Platform	Processor Engine	Interface Cards
Cisco cBR-8 Converged Broadband Router	**Cisco IOS-XE Release 16.5.1 and Later Releases** Cisco cBR-8 Supervisor: • PID—CBR-SUP-250G • PID—CBR-CCAP-SUP-160G • PID—CBR-CCAP-SUP-60G • PID—CBR-SUP-8X10G-PIC	**Cisco IOS-XE Release 16.5.1 and Later Releases** Cisco cBR-8 CCAP Line Cards: • PID—CBR-LC-8D30-16U30 • PID—CBR-LC-8D31-16U30 • PID—CBR-RF-PIC • PID—CBR-RF-PROT-PIC • PID—CBR-CCAP-LC-40G • PID—CBR-CCAP-LC-40G-R Cisco cBR-8 Downstream PHY Modules: • PID—CBR-D30-DS-MOD • PID—CBR-D31-DS-MOD Cisco cBR-8 Upstream PHY Modules: • PID—CBR-D30-US-MOD • PID—CBR-D31-US-MOD

Prerequisites for DOCSIS WFQ Scheduler

No specialequipment or softwareis needed to use the DOCSIS WFQ Scheduler feature.

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 cBR-8 converged broadband router.

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).

The default queue size for the DOCSIS service flows (with bandwidth greater than 150 Mbps) is 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, buffer size in service class or downstream buffer control TLVs.

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 18: 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
12	450	767	63	741	1111	1482	7411
14	525	895	63	864	1296	1729	8646
16	600	1023	63	988	1482	1976	9881

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

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.
- All low latency flows on a DOCSIS downstream are aggregated to the single priority queue.

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.

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 excess ratio.

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 19: DOCSIS Priority to Excess Ratio Mapping

DOCSIS Traffic Priority	Excess Ratio
0	4
1	8
2	12
3	16
4	20
5	24
6	28
7	32

Custom DOCSIS Priority to Excess Ratio Mappings

This option is introduced 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.

The cable downstream qos wfq weights command is used to configure the mappings.

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.

Note The Cisco cBR Cisco Packet Processor (CPP) forwarding processor supports a maximum ratio of 1,000:1 between the highest MaxSusRate or MinRsvRate and the lowest MaxSusRate or MinRsvRate. The scheduler is impacted when the ratio exceeds the value. This limitation is per downstream forwarding interface (Wideband-Cable, Integrated-Cable, and Downstream-Cable).

However, flows implemented by Low Latency Queuing (LLQ) are not be affected by this limitation.

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. 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 cBR-8 Converged Broadband Router, the **cable ds-max-burst** command is used to control this behavior explicitly.

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 cBR-8 router.

Table 20: Enhanced Rate Bandwidth Allocation Support for the Cisco cBR-8 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

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

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.

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.

DBS is the dynamic allocation of bandwidth for wideband (WB) and integrated cable (IC) 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 or IC.

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

In the DBS mode, the bandwidth of the shared RF channels is dynamically allocated among the WB and IC 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 or IC interface level. By default, bandwidth for a WB or IC channel is statically allocated (non-DBS).

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. 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.

Procedure

	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** *slot*/*subslot*/*port* :*wideband-channel* or **interface integrated-cable** *slot*/*subslot*/*port* :*rf-channel* **Example:** `Router(config)# interface wideband-cable 2/0/0:0` or `Router(config)# interface integrated-cable 1/0/0:0`	Enters interface configuration mode for the indicated cable downstream 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: **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 Downstream Queues Information

To verify the downstream queue information for a modem, use the **show cable modem** [*mac-address* |*ip-address*]**service-flow** command.

To check queue stats of all queues on an Integrated-Cable or Wideband-Cable interface, use the **show cable dp queue** *interface* command.

Additional References

The following sections provide references related to the DOCSIS WFQ Scheduler 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

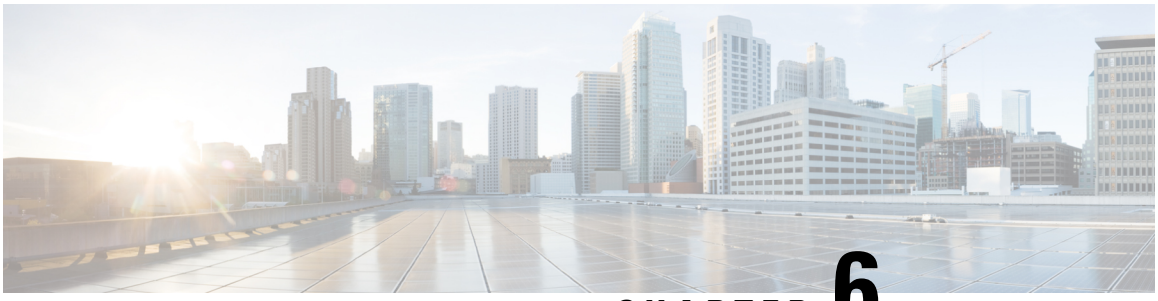
Feature Information for DOCSIS WFQ Scheduler

Use Cisco Feature Navigator to find information about the 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 the www.cisco.com/go/cfn link. An account on the Cisco.com page is not required.

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

Table 21: Feature Information for DOCSIS WFQ Scheduler

Feature Name	Releases	Feature Information
DOCSIS WFQ scheduler	Cisco IOS XE Everest 16.6.1	This feature was integrated into Cisco IOS XE Everest 16.6.1 on the Cisco cBR Series Converged Broadband Routers.



CHAPTER 6

Fairness Across DOCSIS Interfaces

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 that are documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. The Feature Information Table at the end of this document provides information about the documented features and lists the releases in which each feature is supported.

Contents

- Hardware Compatibility Matrix for the Cisco cBR Series Routers, on page 85
- Prerequisites for Fairness Across DOCSIS Interfaces , on page 86
- Restrictions for Fairness Across DOCSIS Interfaces, on page 86
- Information About Fairness Across DOCSIS Interfaces, on page 87
- How to Configure Fairness Across DOCSIS Interfaces, on page 88
- Verifying the Fairness Across DOCSIS Interfaces, on page 92
- Configuration Examples for Fairness Across DOCSIS Interfaces, on page 94
- Additional References, on page 97
- Feature Information for Fairness Across DOCSIS Interfaces, on page 97

Hardware Compatibility Matrix for the Cisco cBR Series Routers

Note The hardware components that are introduced in a given Cisco IOS-XE Release are supported in all subsequent releases unless otherwise specified.

Table 22: Hardware Compatibility Matrix for the Cisco cBR Series Routers

Cisco CMTS Platform	Processor Engine	Interface Cards
Cisco cBR-8 Converged Broadband Router	**Cisco IOS-XE Release 16.5.1 and Later Releases** Cisco cBR-8 Supervisor: • PID—CBR-SUP-250G • PID—CBR-CCAP-SUP-160G • PID—CBR-CCAP-SUP-60G • PID—CBR-SUP-8X10G-PIC	**Cisco IOS-XE Release 16.5.1 and Later Releases** Cisco cBR-8 CCAP Line Cards: • PID—CBR-LC-8D30-16U30 • PID—CBR-LC-8D31-16U30 • PID—CBR-RF-PIC • PID—CBR-RF-PROT-PIC • PID—CBR-CCAP-LC-40G • PID—CBR-CCAP-LC-40G-R Cisco cBR-8 Downstream PHY Modules: • PID—CBR-D30-DS-MOD • PID—CBR-D31-DS-MOD Cisco cBR-8 Upstream PHY Modules: • PID—CBR-D30-US-MOD • PID—CBR-D31-US-MOD

Prerequisites for Fairness Across DOCSIS Interfaces

Note The term ‘Bonding Group (BG)’ is used in this document to refer to all the integrated-cable (IC) and wideband-cable (WC) interfaces in the context of Fairness Across DOCSIS Interfaces feature context. The IC 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[1] of the RF bandwidth that is not statically reserved by the “bandwidth-percent”, in addition to the legacy CIR bandwidth.

[1] 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.

- 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 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. The weights (DOCSIS traffic priority (traffic priority + 1)) of all the BGs are equal for downstream BE service flows. The bandwidth, available for BE traffic, can be used to admit additional CIR flows.

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

On-demand CIR Acquisition

When multiple bonding groups sharing the RF-channel bandwidth and the current bonding group's guaranteed bandwidth is insufficient, this feature can "borrow" neighbor bonding group's non-reserved guaranteed bandwidth for current bonding group's CIR.

This feature is only used by multicast service flow.

Fairness Across Bonding Groups

Fairness Across DOCSIS Interfaces feature use the weight value of the aggregated active flow count, that is EIR demand, to periodically re-balance the reservable bandwidth. So that the service flows with the same weight in different bonding groups will have roughly the same throughput.

OFDM Channels

OFDM Channel

DOCSIS 3.1 introduces modes for higher throughput and higher spectral efficiency while still allowing backward compatibility to DOCSIS 3.0. OFDM Channel support includes 1 OFDM channel per port with channel bandwidth from 24 MHz to 192 MHz wide. In Cisco IOS-XE 16.5.1, a bonding group can consist of SC-QAMs and OFDM channels. An OFDM channel can have multiple profiles configured, and each profile may have different rate. The OFDM Channel rate can vary constantly depending on the profiles being used. For more information on OFDM channels, see *OFDM Channel Configuration Guide*.

OFDM Channel Rate

An OFDM channel can have multiple profiles configured, and each profile can have different rates. For example, with a 96MHz OFDM channel that is configured with profile A (Control Profile) with modulation 1024-QAM, profile B with modulation 2048-QAM, and profile C with modulation 4096-QAM, the profile rates of profile A, B, and C are 616Mbps, 680Mbps, and 736Mbps respectively.

In Cisco IOS-XE 16.5.1, if an OFDM channel has both Control Profile (profile A) and Data Profiles (profile B, C, and so on) configured, the lowest Data Profile rate is used for Fairness Across DOCSIS Interface calculation. Otherwise, the Control Profile rate is used.

Interface Bandwidth

A Wideband-Cable (WB) interface can consist of both SC-QAMs and OFDM channels. If it contains OFDM channels, the highest profile rates are used to calculate the interface bandwidth.

For example, with a 96MHz OFDM channel that is configured with profile A having modulation 1024-QAM, profile B with modulation 2048-QAM, and profile C with modulation 4096-QAM, the profile rates of profile A, B, and C are 616Mbps, 680Mbps, and 736Mbps respectively. Here, 736Mbps is used to calculate the interface bandwidth.

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 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.

Procedure

	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.

Procedure

	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 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.

Procedure

	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 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.

Procedure

	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** {**wideband-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.

	Command or Action	Purpose
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 1875 Kbps
Total downstream reserved/reservable bandwidth 20000/1500 Kbps
Total downstream guaranteed/non-guaranteed bonus bandwidth 20760/9741 Kbps
Router#
```

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” is 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.

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 1/0/0:0

Interface Wi1/0/0:0
BGID: 28673

Resource - Downstream Bandwidth
------------------------------
App-type    Name       Reservation/bps    Exclusive
1                      0                  Not configured
2                      0                  Not configured
3                      0                  Not configured
4                      0                  Not configured
5                      0                  Not configured
6                      0                  Not configured
7                      0                  Not configured
8                      20000000           Not configured
Max Reserved BW = 1500000 bps
Total Current Reservation = 20000000 bps
Guaranteed Bonus BW = 20760000 bps
Non-guaranteed Bonus BW = 9741000 bps
```

```
Subset BGs: In1/0/0:8 In1/0/0:9 In1/0/0:10 In1/0/0:11 In1/0/0:12
Superset BGs: N/A
Overlapping BGs: Wi1/0/0:8 Wi1/0/0:9 Wi1/0/0:10
Router#
```

Effective with Cisco IOS-XE Release 3.18.0SP, Capacity BW is also displayed. It is a summation of the channel capacity of the RF channels in this interface, and the capacity of OFDM channels is calculated considering the lowest profile rate.

```
Router#show cable admission-control interface wideband-Cable 2/0/0:1

Interface Wi2/0/0:1
BGID: 8194

Resource - Downstream Bandwidth
-------------------------------
App-type    Name       Reservation/bps    Maximum        Rejected
1                      4000               90%            0
2                      0                  N/A            0
3                      0                  90%            0
4                      0                  N/A            0
5                      0                  N/A            0
6                      0                  90%            0
7                      0                  N/A            0
8                      0                  87%            0
Max Reserved BW = 11424000 bps
Total Current Reservation = 4000 bps
Guaranteed Bonus BW = 884352000 bps
Non-guaranteed Bonus BW = 225904000 bps
Capacity BW = 1428000000 bps
Subset BGs: In2/0/0:0 In2/0/0:1 In2/0/0:2 In2/0/0:3 In2/0/0:4 In2/0/0:5 In2/0/0:6 In2/0/0:7
 In2/0/0:158 Wi2/0/0:0
Superset BGs: N/A
```

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 integrated-Cable 1/0/0
```

```
EIR Rebalance invoked: 450963
Adaptive CIR granted: 20
Adaptive CIR rejected: 1
Total clusters: 9
RF FlexBW
8 36376
9 36376
10 32625
......
```

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

Use the **show controllers integrated-Cable acfe cluster** command to show Per-controller statistics and clusters and checking the bandwidth information as follows:

```
Router# show controllers integrated-Cable 1/0/0 acfe cluster 0
Integrated-Cable 1/0/0 status:
Topology changed: No

========Cluster 0========
Number of RF: 2
RF FlexBW  WB  ExcessBW Quanta
0  35625   -   35438    35438
           0   187   187
1  35250   0  35250   35250

Number of BG: 2
Intf Demand CIR Max  CstrMin Alloc NBonus Ratio
WB0  1000  0  70875  35250  35437  35438  14855190400
IC0  1000  0  35625  0      35438  187    14855609600
```

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
!
```

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.

```
!
interface integrated-Cable1/0/0:0
cable bundle 1
 cable rf-bandwidth-percent 10
!
interface Wideband-Cable9/0/0:0
 cable bundle 1
  cable rf-channels channel-list 0
  bandwidth-percent 1
  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 IC interface has only 1 BE flow, then IC 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 IC interface, as it would exceed the bonus bandwidth. If the ‘max-eir-ratio’ is set to 10, then the IC 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 integrated-Cable1/0/0:0
cable bundle 1
 cable rf-bandwidth-percent 10
 cable acfe constant-eir-demand 2
!
interface Wideband-Cable9/0/0:0
 cable bundle 1
  cable rf-channels channel-list 0
  bandwidth-percent 1
  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

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

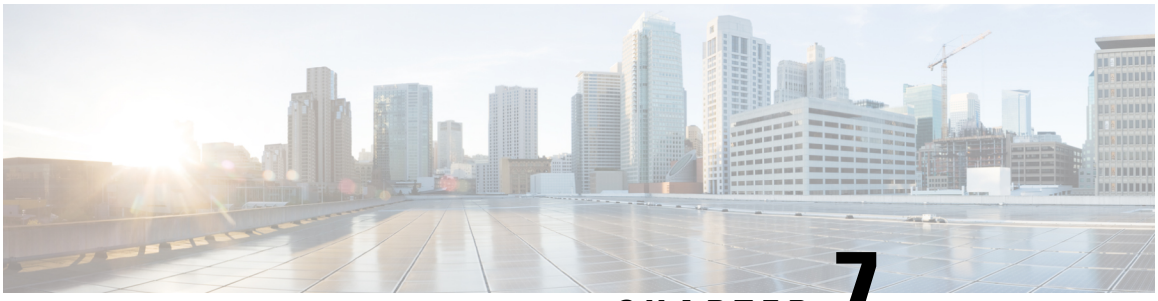
Feature Information for Fairness Across DOCSIS Interfaces

Use Cisco Feature Navigator to find information about the 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 the www.cisco.com/go/cfn link. An account on the Cisco.com page is not required.

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

Table 23: Feature Information for Downstream Interface Configuration

Feature Name	Releases	Feature Information
Fairness across DOCSIS interfaces	Cisco IOS XE Everest 16.6.1	This feature was integrated into Cisco IOS XE Everest 16.6.1 on the Cisco cBR Series Converged Broadband Routers.



CHAPTER 7

Service Group Admission Control

This document describes the Service Group Admission Control feature.

- Finding Feature Information, on page 99
- Hardware Compatibility Matrix for the Cisco cBR Series Routers, on page 99
- Restrictions for Service Group Admission Control, on page 100
- Information About Service Group Admission Control, on page 100
- How to Configure, Monitor, and Troubleshoot Service Group Admission Control, on page 102
- Configuration Examples for SGAC, on page 108
- Additional References, on page 110
- Feature Information for Service Group Admission Control, on page 111

Finding Feature Information

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

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

Hardware Compatibility Matrix for the Cisco cBR Series Routers

Note The hardware components that are introduced in a given Cisco IOS-XE Release are supported in all subsequent releases unless otherwise specified.

Table 24: Hardware Compatibility Matrix for the Cisco cBR Series Routers

Cisco CMTS Platform	Processor Engine	Interface Cards
Cisco cBR-8 Converged Broadband Router	**Cisco IOS-XE Release 16.5.1 and Later Releases** Cisco cBR-8 Supervisor: • PID—CBR-SUP-250G • PID—CBR-CCAP-SUP-160G • PID—CBR-CCAP-SUP-60G • PID—CBR-SUP-8X10G-PIC	**Cisco IOS-XE Release 16.5.1 and Later Releases** Cisco cBR-8 CCAP Line Cards: • PID—CBR-LC-8D30-16U30 • PID—CBR-LC-8D31-16U30 • PID—CBR-RF-PIC • PID—CBR-RF-PROT-PIC • PID—CBR-CCAP-LC-40G • PID—CBR-CCAP-LC-40G-R Cisco cBR-8 Downstream PHY Modules: • PID—CBR-D30-DS-MOD • PID—CBR-D31-DS-MOD Cisco cBR-8 Upstream PHY Modules: • PID—CBR-D30-US-MOD • PID—CBR-D31-US-MOD

Restrictions for Service Group Admission Control

- To configure SGAC, the Fairness Across DOCSIS Interfaces feature must be enabled.
- SGAC supports downstream only.

Information About Service Group Admission Control

Overview

Service Group Admission Control (SGAC) is a mechanism that gracefully manages service group based 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. SGAC monitors such resources constantly, and accepts or denies requests based on resource availability.

SGAC 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. SGAC reduces the impact of unpredictable traffic demands in circumstances that would otherwise produce degraded QoS for subscribers.

Note SGAC 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.

SGAC enables you to configure 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 threshold is crossed for a given resource.

For downstream (DS) channels, you can configure the bandwidth allocation with thresholds for each fiber node.

SGAC and Downstream Bandwidth Utilization

SGAC 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 SGAC 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)

All flows use 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 Downstream Bandwidth

SGAC monitors downstream bandwidth consumption using the configured maximum reserved bandwidth. It rejects service flows with a non-zero minimal rate that would make the total reserved bandwidth exceed the configured threshold.

Flexible Bandwidth Allocation

To address the issue of restricted bandwidth allocation for different application types, admission control can be applied for both normal priority and emergency voice flows. This is done by extending the threshold and assigning a group of application types in a fiber node. Each downstream service flow continues to be categorized for a single application type. However, the one-to-one mapping between an application type and a threshold no longer exists.

Each configured threshold and its associated group of application types can thus be treated as a constraint. A service flow categorized to a certain application type must pass all the constraints associated with that application type.

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. Bonding groups are created by combining multiple RF channels. A single RF channel may also be shared by multiple bonding groups.

Note Effective from Cisco IOS-XE 3.18.0SP Release, as per DOCSIS 3.1, if bonding group contains an OFDM channel, the bonding group's total bandwidth that can be reserved (its capacity), is calculated using the least efficient OFDM profile it can use.

Bonding group SGAC 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.

How to Configure, Monitor, and Troubleshoot Service Group Admission Control

Configuration procedures are optional because the default configurations are enabled by default. This section presents a sequence of procedures for non-default configurations, monitoring and debugging procedures for both the default or non-default operations of SGAC.

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.

Any one or several of these steps or commands may be used, in nearly any combination, to set or re-configure SGAC on the Cisco CMTS.

Note Application rules for SGAC are global configurations, and downstream bandwidth resources use the same sets of service flow rules.

Procedure

	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 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 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

	Command or Action	Purpose
		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.
Step 6	**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.
Step 7	**Ctrl-Z** **Example:** `Router(config)# Ctrl^Z`	Returns to Privileged EXEC mode.

Example

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 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 SGAC supports. The default bucket identifiers range from 1 to 8.

Procedure

	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.

Preempting High-Priority Emergency 911 Calls

You may configure SGAC 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. SGAC provides the command-line interface (CLI) to enable or disable this preemption ability.

SGAC 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 a 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.

Procedure

	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 SGAC 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, SGAC 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.

In each of the above calculations, SGAC 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. SGAC 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 SGAC threshold values. This value is indicated in kbps.

Enabling SGAC Check

A fiber node configured on the CMTS represents one or more matching physical fiber nodes in the HFC plant. The CMTS uses the fiber node configuration to identify the DOCSIS downstream service group (DS-SG) and DOCSIS upstream Service Group (US-SG) of the physical fiber nodes in the plant. The Service Group information is compared with MAC Domain channel configuration to automatically calculate the MAC Domain downstream and upstream service groups (MD-DS-SGs and MD-US-SGs respectively) within the MAC Domains.

Under each Fiber node, use the following procedure to enable SGAC check for an application type and any service flow of the specified application type, which is admitted to a service group.

Before you begin

Fairness Across DOCSIS Interfaces feature should always be enabled and the bandwidth percentage configured on each bonding group should be kept minimal to allow flexible adjustment of reservable bandwidth.

Restrictions

SGAC is supported only on the downstream.

Procedure

	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 fiber-node** *id* **Example:** `Router(config)# cable fiber-node 1`	Enters cable fiber-node configuration mode to configure a fiber node.
Step 4	**admission-control application-type** *n* **ds-bandwidth** *pct*	Enables SGAC checking for the specified application-type.

	Command or Action	Purpose
	Example: `Router(config-fiber-node)# admission-control application-type 1 ds-bandwidth 1`	Use the **no** form of this command to disable SGAC checking.
Step 5	Ctrl-Z **Example:** `Router(config-if)# Ctrl^Z`	Returns to Privileged EXEC mode.

What to do next

Use the **show cable admission-control fiber-node** *n* command to verify admission-control configuration.

Configuration Examples for SGAC

This section describes solutions-level examples of the SGAC feature on the Cisco CMTS. This section illustrates the functioning of SGAC in default or non-default operational configurations.

Example: SGAC Configuration Commands

In this section of configuration examples, the following SGAC 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, use:

```
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, use:

```
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
```

```
Router# show cable admission-control fiber-node 1
App-type    Name       Exclusive
1                      N/A
2                      N/A
3           Normal     10%
4                      N/A
5                      N/A
6                      N/A
7           Emergency  N/A
8                      N/A
```

```
Router#show cable admission-control interface integrated-Cable 8/0/0:0

Interface In8/0/0:0
RFID 24576

Resource - Downstream Bandwidth
-------------------------------
App-type    Name       Reservation/bps    Exclusive      Rejected
1                      0                  N/A            0
2                      0                  N/A            0
3           Normal     0                  10%            0
4                      0                  N/A            0
5                      0                  N/A            0
6                      0                  N/A            0
7           Emergency  0                  N/A            0
8                      0                  N/A            0
Max Reserved BW = 300000 bps
Total Current Reservation = 0 bps
Guaranteed Bonus BW = 21055000 bps
Non-guaranteed Bonus BW = 7744000 bps
Superset BGs: Wi8/0/0:0 Wi8/0/0:4 Wi8/0/0:6
```

```
Router#show cable admission-control interface wideband-Cable 8/0/0:0

Interface Wi8/0/0:0
BGID: 24577

Resource - Downstream Bandwidth
-------------------------------
App-type    Name       Reservation/bps    Exclusive      Rejected
1                      0                  N/A            0
2                      0                  N/A            0
3           Normal     0                  10%            0
4                      0                  N/A            0
5                      0                  N/A            0
6                      0                  N/A            0
7           Emergency  0                  N/A            0
8                      0                  N/A            0
Max Reserved BW = 600000 bps
```

```
Total Current Reservation = 0 bps
Guaranteed Bonus BW = 21055000 bps
Non-guaranteed Bonus BW = 36844000 bps
Subset BGs: In8/0/0:0 In8/0/0:1
Superset BGs: Wi8/0/0:4 Wi8/0/0:6
Overlapping BGs: N/A
```

These above configuration examples might be omitted or changed, but the remaining examples in this section presume the above configurations.

Example: SGAC 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.

The below example illustrates a sample configuration for SGAC 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.

The following command implements this configuration:

```
Router(config-fiber-node)#admission-control application-type 1 ds-bandwidth 30
```

The below example illustrates how flexible bandwidth allocation is configured. In this example, normal voice traffic (application-type 1) is associated with two thresholds. Normal voice traffic alone can use up to 40% of the service group's capacity, while normal and emergency voice traffic combined can use up to 50% of the service group's capacity. This means that emergency voice traffic can have at least 10% of the service group's capacity, even if normal voice traffic has used up its share of 40%:

```
Router(config-fiber-node)#admission-control application-type 1 ds-bandwidth 40
Router(config-fiber-node)#admission-control application-type 1-2 ds-bandwidth 50
```

where,

- 1 is normal voice application type
- 2 is emergency voice application type

Additional References

The following topics provide references related to SGAC for the Cisco CMTS.

Related Documents

Related Topic	Document Title
Cisco CMTS Cable Commands	Cisco CMTS Cable Command Reference

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	To locate and download MIBs for selected platforms, 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

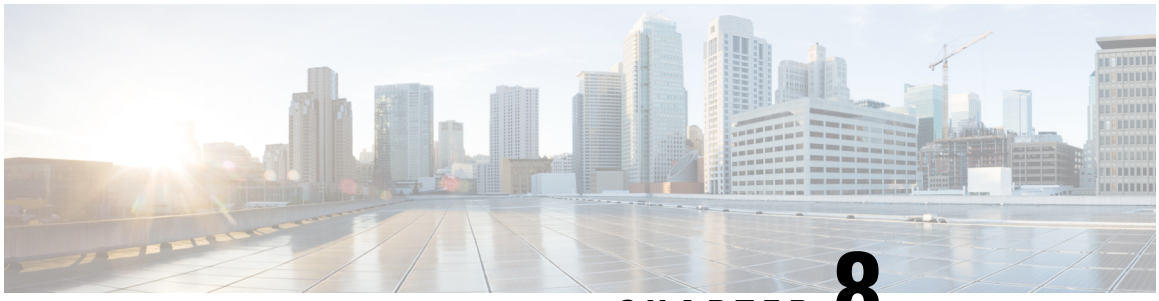
Feature Information for Service Group Admission Control

Use Cisco Feature Navigator to find information about the 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 the www.cisco.com/go/cfn link. An account on the Cisco.com page is not required.

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

Table 25: Feature Information for Service Group Admission Control

Feature Name	Releases	Feature Information
Service group admission control	Cisco IOS XE Everest 16.6.1	This feature was integrated into Cisco IOS XE Everest 16.6.1 on Cisco cBR Series Converged Broadband Routers.



CHAPTER 8

Subscriber Traffic Management

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.

Important 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 DOCSIS1.1 operations, the QoS profile should be treated as a service class.

Finding Feature Information

Your software release may not support all the features that are documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. The Feature Information Table at the end of this document provides information about the documented features and lists the releases in which each feature is supported.

- Hardware Compatibility Matrix for the Cisco cBR Series Routers, on page 114
- Restrictions for Subscriber Traffic Management on the Cisco CMTS Routers, on page 114
- Information About Subscriber Traffic Management on the Cisco CMTS Routers, on page 115
- How to Configure the Subscriber Traffic Management Feature on the Cisco CMTS Routers, on page 120
- Monitoring the Subscriber Traffic Management Feature on the Cisco CMTS Routers, on page 131
- Configuration Examples for Subscriber Traffic Management on the Cisco CMTS Routers, on page 134
- Additional References, on page 137
- Feature Information for Subscriber Traffic Management, on page 139

Hardware Compatibility Matrix for the Cisco cBR Series Routers

Note The hardware components that are introduced in a given Cisco IOS-XE Release are supported in all subsequent releases unless otherwise specified.

Table 26: Hardware Compatibility Matrix for the Cisco cBR Series Routers

Cisco CMTS Platform	Processor Engine	Interface Cards
Cisco cBR-8 Converged Broadband Router	**Cisco IOS-XE Release 16.5.1 and Later Releases** Cisco cBR-8 Supervisor: • PID—CBR-SUP-250G • PID—CBR-CCAP-SUP-160G • PID—CBR-CCAP-SUP-60G • PID—CBR-SUP-8X10G-PIC	**Cisco IOS-XE Release 16.5.1 and Later Releases** Cisco cBR-8 CCAP Line Cards: • PID—CBR-LC-8D30-16U30 • PID—CBR-LC-8D31-16U30 • PID—CBR-RF-PIC • PID—CBR-RF-PROT-PIC • PID—CBR-CCAP-LC-40G • PID—CBR-CCAP-LC-40G-R Cisco cBR-8 Downstream PHY Modules: • PID—CBR-D30-DS-MOD • PID—CBR-D31-DS-MOD Cisco cBR-8 Upstream PHY Modules: • PID—CBR-D30-US-MOD • PID—CBR-D31-US-MOD

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:

- 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 cBR series routers support a certain maximum of 40 enforce-rules. 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.
- 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 40 enforce-rules can be created on each router.
- 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 for DOCSIS1.0 cable modems. 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

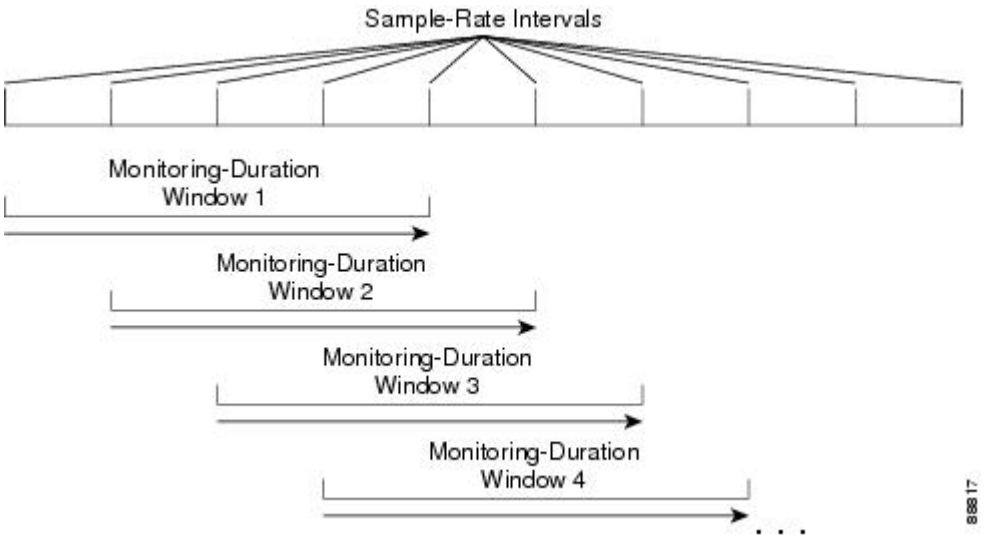
When an enforce-rule is activated, the CMTS periodically checks the bandwidth being used by subscribers to determine whether any subscribers are consuming more bandwidth than that specified by their registered QoS profiles. The CMTS keeps track of the subscribers using a sliding window that begins at 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.

STM version 1.2 supports configuration of different monitoring conditions on weekends. 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

Simple Network Management Protocol (SNMP) trap notification 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.

The following objects are used for enforce rules:

- ccqmCmtsEnfRulePenaltyEndTime
- ccqmCmtsEnfRuleWkndOff
- ccqmCmtsEnfRuleWkndMonDuration
- ccqmCmtsEnfRuleWkndAvgRate
- ccqmCmtsEnfRuleWkndSampleRate
- ccqmCmtsEnfRuleWkndFirstPeakTime
- ccqmCmtsEnfRuleWkndFirstDuration
- ccqmCmtsEnfRuleWkndFirstAvgRate
- ccqmCmtsEnfRuleWkndSecondPeakTime
- ccqmCmtsEnfRuleWkndSecondDuration
- ccqmCmtsEnfRuleWkndSecondAvgRate
- ccqmCmtsEnfRuleWkndOffPeakDuration
- ccqmCmtsEnfRuleWkndOffPeakAvgRate
- ccqmCmtsEnfRuleWkndAutoEnforce
- ccqmCmtsEnfRuleFirstPeakTimeMin
- ccqmCmtsEnfRuleSecondPeakTimeMin
- ccqmCmtsEnfRuleWkndFirstPeakTimeMin
- ccqmCmtsEnfRuleWkndSecondPeakTimeMin
- ccqmCmtsEnfRulePenaltyEndTimeMin
- ccqmCmtsEnfRuleWkPenaltyPeriod
- ccqmCmtsEnfRuleWkndPenaltyPeriod
- ccqmCmtsEnfRuleRelTimeMonitorOn

The following objects are used for enforce rule violations:

- ccqmEnfRuleViolateID
- ccqmEnfRuleViolateMacAddr
- ccqmEnfRuleViolateRuleName
- ccqmEnfRuleViolateByteCount
- ccqmEnfRuleViolateLastDetectTime
- ccqmEnfRuleViolatePenaltyExpTime
- ccqmEnfRuleViolateAvgRate

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.

Procedure

	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.

	Command or Action	Purpose
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. **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. The default is legacy and DOCSIS 1.0.
Step 5	Perform one of the following: • If you specified DOCSIS 1.0 cable modems in Step 4, on page 122, use the following commands: **a.** **qos-profile registered** *profile-id* **b.** **qos-profile enforced** *profile-id* [**no-persistence**] • If you specified DOCSIS 1.1 cable modems in Step 4, on page 122, use the **service-class** {**enforced** | **registered**} *name* command. **Example:** `Router(enforce-rule)# service-class enforced test`	• For DOCSIS 1.0 cable modems: **a.** Specifies the registered quality of service (QoS) profile that should be used for this enforce-rule. **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. **b.** Specifies the quality of service (QoS) profile that should be enforced when users violate their registered QoS profiles for DOCSIS 1.0 cable modems. • For DOCSIS 1.1 (and later) cable modems, identifies a particular service class with the specified *name* for cable modem monitoring in an enforce-rule.
Step 6	**duration** *minutes* **avg-rate** *rate* **sample-interval** *minutes*[**penalty** *minutes*] {**downstream** | **upstream**} [**enforce**] **Example:**	Specifies the time period and sample rate used for monitoring subscribers when legacy monitoring is configured (Step 4, on page 122).

	Command or Action	Purpose
	`Router(enforce-rule)# duration 10 avg-rate 500 sample-interval 10 penalty 120 downstream enforce`	

Step 7	**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 122).

Step 8	**penalty-period** *minutes* [**time-of-day** {*hour*|*hour*:*minutes*}] [**monitoring-on**] **Example:** `Router(enforce-rule)# penalty-period 10`	(Optional) Specifies the period for which an enforced QoS profile should be in effect for subscribers who violate their registered QoS profiles.
Step 9	**enabled** **Example:** `Router(enforce-rule)# enabled`	(Optional) Activates the enforce-rule and begins subscriber traffic management.
Step 10	**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
```

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 120.

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.

Procedure

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

	Command or Action	Purpose
	`Router> enable`	
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**] **Example:** `Router(enforce-rule)# weekend duration 15 avg-rate 500 sample-interval 10 penalty 120 downstream enforce`	Specifies the time period and sample rate used for monitoring subscribers on weekends.
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.

Procedure

	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 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.

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.

Procedure

	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 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).

Procedure

	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:**	Exits enforce-rule configuration mode and returns to privileged EXEC mode.

	Command or Action	Purpose
	`Router(enforce-rule)# end`	

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.

Procedure

	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.

Procedure

	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 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.

Procedure

	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.
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[2]	Title
SP-RFIv1.1-I09-020830	*Data-over-Cable Service Interface Specifications Radio Frequency Interface Specification, version 1.1* (http://www.cablemodem.com)

Standards[2]	Title
draft-ietf-ipcdn-docs-rfmibv2-06	*Radio Frequency (RF) Interface Management Information Base for DOCSIS 2.0 Compliant RF Interfaces*

[2] Not all supported standards are listed.

MIBs

MIBs[3]	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

[3] Not all supported MIBs are listed.

RFCs

RFCs[4]	Title
RFC 2233	DOCSIS OSSI Objects Support
RFC 2665	DOCSIS Ethernet MIB Objects Support
RFC 2669	Cable Device MIB

[4] 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

Use Cisco Feature Navigator to find information about the 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 the www.cisco.com/go/cfn link. An account on the Cisco.com page is not required.

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

Table 27: Feature Information for Subscriber Traffic Management

Feature Name	Releases	Feature Information
Subscriber traffic management	Cisco IOS XE Everest 16.6.1	This feature was integrated into Cisco IOS XE Everest 16.6.1 on Cisco cBR Series Converged Broadband Routers.

INDEX

C

class-map Command 15
  combining match-all and -any characteristics 15

M

match class-map Command 15
  combining match-all and -any characteristics 15
  nested class maps 15
Modular QoS Command-Line Interface 11
  description 11
MQC (modular QoS command-line interface (CLI)) 11
  comprises 11
  defined 11

N

nested traffic class 15
  typical scenario 15

T

traffic class 14
  associating multiple classes 14
traffic policies 17
  creating 17
traffic policy 15
  associating with multiple traffic classes 15