



Cisco Cable Modem Termination System Feature Guide

September 2004

Corporate 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: 408 526-4100

Text Part Number: 0L-1467-04



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

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

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

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

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

CCSP, the Cisco Square Bridge logo, Cisco Unity, Follow Me Browsing, FormShare, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, Packet, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, Registrar, ScriptShare, SlideCast, SMARTnet, StrataView Plus, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0406R)

Cisco Cable Modem Termination System Feature Guide
Copyright © 2001-2004, Cisco Systems, Inc.
All rights reserved.



Preface xv

Purpose xv

Audience xvi

Document Organization xvi

Conventions xviii

Terms and Acronyms xix

Related Documentation xix

Cisco uBR Series Documentation xix

Additional Documentation Resources xx

Obtaining Documentation xx

Cisco.com xx

Documentation CD-ROM xxi

Ordering Documentation xxi

Documentation Feedback xxi

Obtaining Technical Assistance xxi

Cisco TAC Website xxii

Opening a TAC Case xxii

TAC Case Priority Definitions xxii

Obtaining Additional Publications and Information xxiii

Cable Interface Bundling for the Cisco CMTS 1

Contents 2

Prerequisites for Cable Bundling 2

Restrictions for Cable Bundling 2

Information About Cable Bundling 3

Benefits 4

Configuring Cable Bundling 4

Monitoring Cable Interface Bundling 7

Configuration Examples for Cable Interface Bundling 9

Basic Cable Interface Bundling Example 9

Additional References 10

Related Documents 10

Standards 11

MIBs 11

RFCs	12
Technical Assistance	12

Cable Monitor and Intercept Features for the Cisco CMTS 13

Contents	14
Prerequisites for Cable Monitor and Intercept	14
Restrictions for Cable Monitor and Intercept	14
Information About Cable Monitor and Intercept	14
Overview of the cable interface Command	15
Overview of the cable monitor Command	15
Benefits	17
How to Configure for Cable Intercept and Monitoring	17
Configuring the cable intercept Command	17
Configuring the cable monitor Command	19
Monitoring the Cable Intercept and Monitor Features	21
Displaying Information About Intercepted Traffic	21
Displaying Information About Monitored Traffic	21
DOCSIS Data Packets Example	22
Timestamped Packets Example	22
Configuration Examples	23
Cable Intercept Configuration Example	23
Cable Monitor Configuration Example (MAC Address)	23
Cable Monitor Configuration Example (Ethernet, MAC-Layer, and DOCSIS-Data Packets)	24
Additional References	24
Related Documents	24
Standards	25
MIBs	25
RFCs	25
Technical Assistance	26

DHCP, ToD, and TFTP Services for the Cisco CMTS 27

Contents	28
Prerequisites for DHCP, ToD, and TFTP Services	28
Restrictions for DHCP, ToD, and TFTP Services	28
Information About DHCP, ToD, and TFTP Services	29
Feature Overview	29
Internal DHCP Server	30

External DHCP Servers	32
Time-of-Day Server	33
TFTP Server	35
Benefits	36
How to Configure DHCP, ToD, and TFTP Services	37
Configuring DHCP Service	37
Configuring Time-of-Day Service	43
Configuring TFTP Service	45
Configuring A Basic All-in-One Configuration (optional)	48
Configuring an Advanced All-in-One Configuration (optional)	49
Optimizing the Use of an External DHCP Server	49
Configuration Examples	55
DHCP Server Examples	55
ToD Server Example	57
TFTP Server Example	57
Basic All-in-One Configuration Example	58
Advanced All-in-One Configuration Example	62
Additional References	68
Related Documents	68
Standards	70
MIBs	71
RFCs	71
Technical Assistance	71
Configuring DOCSIS 1.1 on the Cisco CMTS	73
Contents	74
Prerequisites for DOCSIS 1.1 Operations	74
Restrictions for DOCSIS 1.1 Operations	75
Information about DOCSIS 1.1	78
Feature Overview	78
DOCSIS 1.1 Quality of Service	80
Benefits	86
How to Configure the Cisco CMTS for DOCSIS 1.1 Operations	87
Configuring Baseline Privacy Interface (optional)	88
Downloading the DOCSIS Root Certificate to the CMTS (required)	91
Adding a Manufacturer's Certificate as a Trusted Certificate (optional)	94
Adding a Manufacturer's or CM Certificate to the Hotlist (required)	96

Enabling Concatenation (optional)	99
Enabling DOCSIS Fragmentation (optional)	100
Monitoring DOCSIS Operations	101
Monitoring the DOCSIS Network	101
Monitoring the RF Network and Cable Interfaces	107
Monitoring BPI+ Operations	111
Command Summary	114
Configuration Examples for DOCSIS 1.1 Operations	115
DOCSIS 1.1 Configuration for Cisco uBR7246VXR Router (without BPI+)	115
DOCSIS 1.1 Configuration for Cisco uBR7246VXR Router (with BPI+)	117
DOCSIS 1.1 Configuration for Cisco uBR10012 Router (with BPI+)	121
Additional References	125
Related Documents	125
Standards	126
MIBs	127
RFCs	127
Technical Assistance	127

EtherChannel for the Cisco Cable Modem Termination System 129

Contents	130
Prerequisites for EtherChannel on the Cisco CMTS	130
Restrictions for EtherChannel on the Cisco CMTS	131
Information About EtherChannel on the Cisco CMTS	131
Introduction to EtherChannel on the Cisco CMTS	131
Cisco FastEtherChannel (FEC) and GigabitEtherChannel (GEC) on the Cisco uBR7246VXR Router	132
Cisco GigabitEtherChannel (GEC) on the Cisco uBR10012 Router	132
How to Configure EtherChannel on the Cisco CMTS	133
Configuring FEC or GEC EtherChannel on the Cisco CMTS	133
Verifying EtherChannel on the Cisco CMTS	136
Configuration Examples for EtherChannel on the Cisco CMTS	136
Additional References	140
Related Documents	140
Standards	142
MIBs	142
Technical Assistance	142
Command Reference for EtherChannel on the Cisco CMTS	143
Glossary	149

Flap List Troubleshooting for the Cisco CMTS	151
Contents	152
Prerequisites for Flap List Troubleshooting	152
Restrictions for Flap List Troubleshooting	152
Information About Flap List Troubleshooting	152
Feature Overview	153
Information in the Flap List	153
Cisco Cable Manager and Cisco Broadband Troubleshooter	154
Benefits	155
How to Configure Flap List Troubleshooting	155
Configuring Flap List Operation Using the CLI (optional)	155
Clearing the Flap List and Counters Using the CLI (optional)	157
Enabling or Disabling Power Adjustment Using the CLI (optional)	158
Configuring Flap List Operation Using SNMP (optional)	161
Clearing the Flap List and Counters Using SNMP (optional)	161
How to Monitor and Troubleshoot Using Flap Lists	162
Displaying the Flap List Using the show cable flap-list Command	162
Displaying the Flap List Using the show cable modem flap Command	166
Displaying the Flap List Using SNMP	166
Displaying Flap-List Information for Specific Cable Modems	167
Troubleshooting Suggestions	169
Configuration Examples for Flap List Troubleshooting	171
Additional References	172
Related Documents	172
Standards	173
MIBs	174
RFCs	174
Technical Assistance	174
Internal DOCSIS Configuration File Generator for the Cisco CMTS	175
Contents	175
Prerequisites for the Internal DOCSIS Configuration File Generator	176
Restrictions for the Internal DOCSIS Configuration File Generator	176
Information About the Internal DOCSIS Configuration File Generator	177
Feature Overview	177

DOCSIS Configuration File Commands	178
Benefits	179
Related Features	179
How to Use the Internal DOCSIS Configuration File Generator	179
Creating and Configuring a DOCSIS Configuration File	180
Specifying SNMP MIB Objects (Option 11)	184
Specifying Vendor-Specific Information Fields (Option 43)	191
Configuring the Router's Onboard TFTP Server	194
Configuration Examples for the Internal DOCSIS Configuration File Generator	196
Platinum.cm	196
Platinum.cm with BPI Enabled	196
Disable.cm	196
Configuration Files and DHCP Server Configuration	197
Additional References	198
Related Documents	198
Standards	198
MIBs	199
RFCs	199
Technical Assistance	199
Maximum CPE and Host Parameters for the Cisco CMTS	201
Contents	202
Information About the MAX CPE and Host Parameters	202
MAX CPE	203
MAX CPE IP	203
MAX Host	204
Interoperation of the Maximum CPE Parameters	205
Possible Conflicts Between Parameters	207
Summary of CPE Address Control	208
Benefits	208
How to Configure the MAX CPE and Host Parameters	209
Configuring the MAX CPE Parameter on the Cisco CMTS	209
Configuring the MAX Hosts Parameter for a Cable Interface	211
Configuring the MAX Hosts Parameter for a Particular Cable Modem	212
Configuration Examples for the MAX CPE and Host Parameters	213
Sample Outputs	213
Additional References	215
Related Documents	215

Standards	215
MIBs	216
Technical Assistance	216

CHAPTER 1**N+1 Redundancy for the Cisco Cable Modem Termination System 219**

Contents	221
Prerequisites	221
Restrictions and Limitations	222
General N+1 Redundancy Restrictions and Limitations	222
N+1 Redundancy Restrictions and Requirements for the Cisco uBR7246VXR Router	222
N+1 Redundancy Restrictions and Requirements for the Cisco uBR10012 Router	223
Information About N+1 Redundancy and the Cisco Universal Broadband CMTS	225
The Components and Terminology of N+1 Redundancy	225
IF Muting on the Cisco CMTS for non-SNMP-capable Upconverters	232
Cisco RF Switch Configuration Tasks for N+1 Redundancy	235
Configuring the Cisco RF Switch for N+1 Redundancy	235
Creating Cisco RF Switch Module Bitmaps	238
Cisco CMTS Configuration Tasks for N+1 Redundancy	241
Preconfiguring HCCP Protect Interfaces for N+1 Redundancy	242
Operating DHCP with the Cisco RF Switch	244
Configuring HCCP Groups for N+1 Redundancy	245
Enabling HCCP Protect Interfaces for N+1 Redundancy	247
Maintaining Online Cable Modem Service When Removing HCCP Configuration from Working HCCP Interfaces	248
Switchover Testing Tasks for N+1 Redundancy	251
Pre-testing System Check Procedures	251
Switchover Testing Procedures	255
Testing HCCP Groups with Manual Switchover	257
Using the show cable modem Command After a Manual Switchover	258
Configuration Examples for Cisco N+1 Redundancy	259
Example: Cisco 3x10 RF Switch Modules in 8+1 Mode	260
Example: Cisco 3x10 RF Switch Modules in 4+1 Mode	261
Examples: Cisco 3x10 RF Switch with Cisco uBR10012 Chassis	269
Example: Channel Switch Information from the Cisco uBR10012 Router	273
Example: Cisco 3x10 RF Switch and Cisco uBR10012 Chassis	274
Example: Cisco 3x10 RF Switches and Cisco uBR10012 Chassis	279
Example: Cisco 3x10 RF Switches and uBR7246VXR Chassis	285
Additional References	293
Related Documents	293

Standards	294
MIBs	294
Technical Assistance	294
Glossary	295

Configuring PacketCable on the Cisco CMTS 299

Contents	300
Prerequisites for PacketCable Operations	300
Restrictions for PacketCable Operations	300
Information About PacketCable Operations	301
Feature Overview	301
PacketCable Network Components	301
Dynamic Quality of Service	302
Benefits	304
How to Configure PacketCable Operations	306
Enabling PacketCable Operation	306
Disabling PacketCable Operation	307
Configuring PacketCable Operation (Optional)	308
Enabling Both PacketCable and Non-PacketCable UGS Service Flows	309
Verifying PacketCable Configuration	311
Configuring RADIUS Accounting for RKS Servers	311
Monitoring and Maintaining PacketCable Operations	314
Configuration Examples	314
Typical PacketCable Configuration	315
Additional References	318
Related Documents	318
Standards	319
MIBs	320
RFCs	320
Technical Assistance	320
Glossary	321

Point-to-Point Protocol over Ethernet Termination on the Cisco CMTS 323

Contents	324
Prerequisites for PPPoE Termination	324
Restrictions for PPPoE Termination	324
Information About PPPoE Termination	325
Feature Overview	325
Benefits	326

How to Configure the PPPoE Termination Feature	327
Enabling VPDN Operations on the Cisco CMTS	327
Configuring a Virtual Template on the Cisco CMTS	329
Configuring a VPDN Group for PPPoE Sessions	332
Configuring a VPDN Group for L2TP Tunnel Initiation on the Cisco CMTS	334
Enabling PPPoE on a Cable Interface	336
Configuring a Cisco Router as LNS	338
Clearing PPPoE Sessions	340
Enabling SNMP Traps for Active PPPoE Sessions	341
Monitoring the PPPoE Termination Feature	342
Configuration Examples for PPPoE Termination	342
PPPoE Termination on a Cisco CMTS without L2TP Tunneling	343
PPPoE Termination on a Cisco CMTS with L2TP Tunneling	344
PPPoE Client Configuration on a Cisco Router	346
PPPoE Configuration for the L2TP Network Server	346
Additional References	348
Related Documents	348
Standards	348
MIBs	349
RFCs	349
Technical Assistance	349
Glossary	350
Spectrum Management for the Cisco CMTS	353
Contents	354
Prerequisites for Spectrum Management	354
Restrictions for Spectrum Management	356
Cisco IOS Releases and Cable Interface Line Card Support	356
Cisco uBR10012 Router and Cisco IOS Release 12.2(8)BC2 Support	357
DOCSIS Cable Modem Test Analyzer	358
Dynamic Upstream Modulation	358
Fixed-Frequency Spectrum Groups with Advanced Spectrum Management	358
Limitations on Upstream Modulation Parameters for PacketCable VoIP Calls	359
HCCP 1+1 and N+1 Redundancy Support	359
Intelligent and Advanced Spectrum Management Support	360
Information About Spectrum Management	362
Spectrum Management Measurements	363
Upstream Signal Channel Overview	366
Upstream Segments and Combiner Groups	367

Frequency Management Policy	368
Guided and Scheduled Spectrum Management	370
Intelligent and Advanced Hardware-Based Spectrum Management	376
Benefits	378
How to Configure Spectrum Management	382
Guided and Scheduled Spectrum Management Configuration Tasks	382
Intelligent and Advanced Spectrum Management Configuration Tasks	396
Monitoring Spectrum Management	406
Using CLI Commands	406
Using SNMP	407
Configuration Examples	411
Upstream Traffic Shaping and Rate Limiting Examples	411
Downstream Traffic Shaping and Rate Limiting Examples	414
Spectrum Group and Combiner Group Examples	415
Other Spectrum Management Configuration Examples	417
Dynamic Upstream Modulation Examples	419
Input Power Level Example	420
Advanced Spectrum Management Configuration Examples	421
Additional References	426
Related Documents	426
Standards	427
MIBs	427
RFCs	427
Technical Assistance	428
Telco Return for the Cisco CMTS	429
Contents	429
Prerequisites for Telco Return	430
Restrictions for Telco Return	430
Information about Telco Return	431
Feature Overview	431
DOCSIS Cable Plants	431
Telco Return Operation	432
Benefits	434
How to Configure the Telco Return Feature	434
Enabling Telco Return	434
Configuring the Service Provider Descriptor Attributes	435
Configuring the Registration IP Address (optional)	438
Monitoring Telco Return Operations	439

Configuration Examples	440
Typical Telco Return Example	440
Minimal Telco Return Example	441
Minimal RADIUS Configuration	441
Additional References	441
Related Documents	441
Standards	442
MIBs	443
RFCs	443
Technical Assistance	443
Time-of-Day Server for the Cisco CMTS	445
Contents	446
Prerequisites for the Time-of-Day Server	446
Restrictions for the Time-of-Day Server	446
Information About the Time-of-Day Server	446
How to Configure the Time-of-Day Server on the Cisco CMTS	447
Enabling the Time-of-Day Server	447
Disabling the Time-of-Day Server	448
Configuration Examples for the Time-of-Day Server	449
Time-of-Day Server Configuration	449
Additional References	450
Related Documents	450
Standards	450
MIBs	451
RFCs	451
Technical Assistance	451



Preface

This preface explains the objectives, intended audience, and organization of the *Cisco Cable Modem Termination System Feature Guide* for Cisco IOS Release 12.2(8)BC2 and earlier releases. This preface also defines this document's conventions for conveying instructions and information.

- [Purpose, page xv](#)
- [Audience, page xvi](#)
- [Document Organization, page xvi](#)
- [Conventions, page xviii](#)
- [Terms and Acronyms, page xix](#)
- [Related Documentation, page xix](#)
- [Obtaining Documentation, page xx](#)
- [Obtaining Technical Assistance, page xxi](#)
- [Obtaining Additional Publications and Information, page xxiii](#)

Purpose

This feature guide describes the software features contained in the Cisco Cable Modem Termination System (CMTS). Each chapter describes a feature; the supported releases; benefits; restrictions; any supported standards, MIBs, or RFCs; any prerequisites; and the configuration tasks and examples used to set up and implement the feature.

The feature guide replaces the Cisco IOS feature modules for cable that used to describe each CMTS feature, as well as feature content found in the Cisco uBR series software configuration guides. The guide represents ongoing documentation work—more and more of the CMTS features will be added into the guide until all the features have been included. As new CMTS features are introduced, they will be included in the feature guide. Cisco IOS feature modules for the CMTS will no longer be documented. Feature content in the Cisco uBR series software configuration guides will be phased out, and users will be referred to this feature guide.

The CMTS features are used by the Cisco uBR7100 series, the Cisco uBR7200 series, and the Cisco uBR10012 universal broadband routers.

Audience

This guide is intended for CMTS system administrators, network administrators, and support engineers and technicians who configure, maintain, and troubleshoot the Cisco uBR7100 series, the Cisco uBR7200 series, and the Cisco uBR10012 router.

All users should have some experience with configuring Cisco routers and using the Cisco IOS command-line interface (CLI). A basic familiarity with Data-over-Cable Service Interface Specifications (DOCSIS) 1.0, DOCSIS 1.0+ quality of service (QoS) principles, and Simple Network Management Protocol (SNMP) is helpful.

Cable system administrators and support engineers should be acquainted with cable data networks and WAN communications protocols. Cable system technicians should be familiar with their cable plant's base operating parameters and subscriber service offerings. Network administrators should be familiar with the principles of IP routing and subnetting; some of the advanced configurations also require an understanding of access lists and how to use them.

Document Organization

Table 1 summarizes the chapters in this guide.

Table 1 *Guide Contents and Organization*

Title	Description
Cable Interface Bundling for the Cisco CMTS	Describes how to bundle cable interfaces so as to simplify interface configuration and to preserve IP address space.
Cable Monitor and Intercept Features for the Cisco CMTS	Allows an external LAN packet analyzer on the cable interface to monitor inbound and outbound data packets for specific types of traffic between the Cisco CMTS and the cable modems attached to the radio frequency (RF) line card.
Configuring PacketCable on the Cisco CMTS	Describes how to configure the Cisco uBR7200 series routers for PacketCable operations.
Configuring DOCSIS 1.1 on the Cisco CMTS	Describes how to configure the Cisco CMTS routers for DOCSIS 1.1 operations.
DHCP, ToD, and TFTP Services for the Cisco CMTS	Describes how to configure Cisco CMTS platforms so that they support onboard servers that provide Dynamic Host Configuration Protocol (DHCP), Time-of-Day (ToD), and Trivial File Transfer Protocol (TFTP) services for use in Data-over-Cable Service Interface Specifications (DOCSIS) networks. In addition, this chapter provides information about optional configurations that can be used with external DHCP servers.
EtherChannel for the Cisco Cable Modem Termination System	EtherChannel is a technology by which to configure and aggregate multiple physical Ethernet connections to form a single logical port with higher bandwidth. EtherChannel technology is currently supported on the Cisco uBR7246VXR and the Cisco uBR10012 universal broadband routers.
Flap List Troubleshooting for the Cisco CMTS	The flap list is a patented tool used to troubleshoot cable modem connectivity problems. The flap list tracks “flapping” cable modems—cable modems that have intermittent connectivity problems—that could indicate a problem with the cable modem or with the upstream or downstream portion of the cable plant.
Internal DOCSIS Configuration File Generator for the Cisco CMTS	A built-in tool on the CMTS to generate and internally store DOCSIS configuration files.

Table 1 *Guide Contents and Organization*

Title	Description
Maximum CPE and Host Parameters for the Cisco CMTS	Explanation of Cisco IOS commands used to set the maximum number of permitted customer premises equipment (CPE) devices that use the cable modem to connect to the cable network, and to synchronize the number of permitted CPE devices recognized by the CMTS and the cable modem.
N+1 Redundancy for the Cisco Cable Modem Termination System	Describes the N+1 redundancy feature that supports cable interface line card redundancy in Cisco CMTSs headends.
Point-to-Point Protocol over Ethernet Termination on the Cisco CMTS	Describes the PPPoE Termination feature, which allows service providers to extend their existing PPP dial-up provisioning systems to users on cable networks by encapsulating the PPP packets within Ethernet MAC frames.
Spectrum Management for the Cisco CMTS	A software and hardware feature provided in the CMTS so that the CMTS may sense both downstream and upstream plant impairments, report them to a management entity, and automatically mitigate them where possible.
Telco Return for the Cisco CMTS	Enables cable companies that do not support two-way radio frequency (RF) transmission or that have not upgraded their cable plants or specific service areas to offer fast downstream data services via the cable plant and upstream transmission via the PSTN over standard phone lines, as opposed to an all-cable network.
Time-of-Day Server for the Cisco CMTS	Enables the CMTS to provide a time-of-day (ToD) server to the cable modems and other customer premises equipment (CPE) devices connected to its cable interfaces. The ToD server gives the current date and time to accurately time stamp the cable modems' Simple Network Management Protocol (SNMP) messages and error log entries.
Index	Index for the entire manual.

Conventions

This guide uses the following conventions for command syntax descriptions and textual emphasis:

Table 2 *Command Syntax and Emphasis Conventions*

Convention	Description
boldface font	Commands and keywords are in boldface .
<i>italic</i> font	Arguments for which you supply values are in <i>italics</i> .
[]	Elements in square brackets are optional.
{x y z}	Alternative, mutually exclusive keywords are grouped in braces and separated by vertical bars.
[x y z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string, or the string will include the quotation marks.
screen font	Terminal sessions and information the system displays are in <code>screen font</code> .
boldface screen font	Information you must enter is in boldface screen font.
<i>italic screen</i> font	Arguments for which you supply values are in <i>italic screen</i> font.
^	The symbol ^ represents the key labeled Control—for example, the key combination ^D in a screen display means hold down the Control key while you press the D key.
< >	Nonprinting characters, such as passwords, are in angle brackets in contexts where italics are not available.
[]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.



Note

This symbol means *reader take note*. Notes contain helpful suggestions or references to material not covered in the publication.



Tip

This symbol means *the following are useful tips*.



Timesaver

This symbol means *the described action saves time*. You can save time by performing the action described in the paragraph.



Caution

This symbol means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Terms and Acronyms

To fully understand the content of this guide, you should be familiar with the following terms and acronyms:

**Note**

A complete list of terms and acronyms is available in the *Dictionary of Cisco Internetworking Terms and Acronyms* guide, available on Cisco.com and the Documentation CD-ROM.

- CoS—class of service
- CPE—customer premises equipment
- CRC—cyclic redundancy check
- CSU—channel service unit
- DCE—data communications equipment
- IPSec—IP Security Protocol
- MAC—Media Access Control
- MB—megabyte
- NVRAM—nonvolatile random-access memory
- OIR—online insertion and removal
- PPP—Point-to-Point Protocol
- QoS—quality of service
- RFI—radio frequency interference
- RIP—Routing Information Protocol
- SNMP—Simple Network Management Protocol
- TCP/IP—Transmission Control Protocol/Internet Protocol
- UBR—unspecified bit rate
- UDP—User Datagram Protocol
- UNI—User-Network Interface
- VPN—Virtual Private Network

Related Documentation

Cisco uBR Series Documentation

The procedures in this guide assume that site preparation and hardware setup are complete. Refer to the documents below as required for additional prerequisite information and reference.

**Note**

If the hypertext link to any external document does not operate, you can access the desired document by typing or pasting the full document title in the **Search** field of the Cisco.com home page. Click **Go**.

- [Cisco uBR7100 Series Universal Broadband Routers](#) documentation web page
- [Cisco uBR7200 Series Universal Broadband Routers](#) documentation web page
- [Cisco uBR10012 Universal Broadband Router](#) documentation web page

Additional Documentation Resources

For detailed information on CMTS commands, syntax, and usage, refer to the *Cisco Broadband Cable Command Reference Guide*.

For Cisco IOS software configuration information and support, refer to the configuration and command reference publications that pertain to your version of Cisco IOS software and hardware. Specifically, you should refer to the following publications:

- For procedures on configuring broadband routers using the Cisco command-line interface (CLI), refer to the *Cisco IOS Multiservice Applications Configuration Guide, Release 12.1*
- For information on setting up quality of service (QoS), refer to the *Cisco IOS Quality of Service Solutions Configuration Guide, Release 12.2* and *Cisco IOS Quality of Service Solutions Command Reference, Release 12.2* publications.
- For information on encryption, refer to the *Cisco IOS Security Configuration Guide, Release 12.2* and the *Cisco IOS Security Command Reference, Release 12.2* publications.
- For information on interfaces, refer to the *Cisco IOS Interface Configuration Guide, Release 12.2* and the *Cisco IOS Interface Command Reference, Release 12.2* publications.
- For information on IP, refer to the *Network Protocols Configuration Guide, Part 1* and the *Network Protocols Command Reference, Part 1* publications.
- For information about configuring your Cisco networking device to function as a firewall and traffic filtering capabilities with access control lists, refer to the “Traffic Filtering and Firewalls” chapter of the *Cisco IOS Security Configuration Guide, Release 12.2* on Cisco.com.

You can also refer to the Cisco IOS software release notes for the version of software you are using on your router. These Web pages on Cisco.com contain release notes for universal broadband routers:

- *Release Notes for the Cisco uBR7100 Series Universal Broadband Routers*
- *Release Notes for the Cisco uBR7200 Series Universal Broadband Routers*
- *Release Notes for the Cisco uBR10012 Universal Broadband Router*

Obtaining Documentation

Cisco provides several ways to obtain documentation, technical assistance, and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation on the World Wide Web at this URL:

<http://www.cisco.com/univercd/home/home.htm>

You can access the Cisco website at this URL:

<http://www.cisco.com>

International Cisco websites can be accessed from this URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which may have shipped with your product. The Documentation CD-ROM is updated regularly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual or quarterly subscription.

Registered Cisco.com users can order a single Documentation CD-ROM (product number DOC-CONDOCCD=) through the Cisco Ordering tool:

http://www.cisco.com/en/US/partner/ordering/ordering_place_order_ordering_tool_launch.html

All users can order annual or quarterly subscriptions through the online Subscription Store:

<http://www.cisco.com/go/subscription>

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpk/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:

<http://www.cisco.com/en/US/partner/ordering/index.shtml>

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit comments electronically on Cisco.com. On the Cisco Documentation home page, click **Feedback** at the top of the page.

You can send your comments in e-mail to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, the Cisco Technical Assistance Center (TAC) provides 24-hour, award-winning technical support services, online and over the phone. Cisco.com features the Cisco TAC website as an online starting point for technical assistance.

Cisco TAC Website

The Cisco TAC website (<http://www.cisco.com/tac>) provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The Cisco TAC website is available 24 hours a day, 365 days a year.

Accessing all the tools on the Cisco TAC website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a login ID or password, register at this URL:

<http://tools.cisco.com/RPF/register/register.do>

Opening a TAC Case

The online TAC Case Open Tool (<http://www.cisco.com/tac/caseopen>) is the fastest way to open P3 and P4 cases. (Your network is minimally impaired or you require product information). After you describe your situation, the TAC Case Open Tool automatically recommends resources for an immediate solution. If your issue is not resolved using these recommendations, your case will be assigned to a Cisco TAC engineer.

For P1 or P2 cases (your production network is down or severely degraded) or if you do not have Internet access, contact Cisco TAC by telephone. Cisco TAC engineers are assigned immediately to P1 and P2 cases to help keep your business operations running smoothly.

To open a case by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

For a complete listing of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>

TAC Case Priority Definitions

To ensure that all cases are reported in a standard format, Cisco has established case priority definitions.

Priority 1 (P1)—Your network is “down” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Priority 2 (P2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Priority 3 (P3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Priority 4 (P4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The *Cisco Product Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the *Cisco Product Catalog* at this URL:
http://www.cisco.com/en/US/products/products_catalog_links_launch.html
- Cisco Press publishes a wide range of networking publications. Cisco suggests these titles for new and experienced users: Internetworking Terms and Acronyms Dictionary, Internetworking Technology Handbook, Internetworking Troubleshooting Guide, and the Internetworking Design Guide. For current Cisco Press titles and other information, go to Cisco Press online at this URL:
<http://www.ciscopress.com>
- Packet magazine is the Cisco quarterly publication that provides the latest networking trends, technology breakthroughs, and Cisco products and solutions to help industry professionals get the most from their networking investment. Included are networking deployment and troubleshooting tips, configuration examples, customer case studies, tutorials and training, certification information, and links to numerous in-depth online resources. You can access Packet magazine at this URL:
<http://www.cisco.com/go/packet>
- iQ Magazine is the Cisco bimonthly publication that delivers the latest information about Internet business strategies for executives. You can access iQ Magazine at this URL:
<http://www.cisco.com/go/iqmagazine>
- Internet Protocol Journal is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:
http://www.cisco.com/en/US/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html
- Training—Cisco offers world-class networking training. Current offerings in network training are listed at this URL:
http://www.cisco.com/en/US/learning/le31/learning_recommended_training_list.html



Cable Interface Bundling for the Cisco CMTS

This document describes how to combine multiple cable interfaces in a Cisco Cable Modem Termination System (CMTS) universal broadband router into a single logical bundle, so as to conserve IP address space and simplify network management.

Feature History for Cable Interface Bundling

Release	Modification
12.0(7)XR	This feature was introduced on Cisco uBR7200 series routers.
12.1(5)EC1	Support for this feature was added for Cisco uBR7100 series routers.
12.2(4)BC1	Support for this feature was added for Cisco uBR10012 routers. Support for MPLS was also added for cable interface bundles on all Cisco CMTS routers.
12.1(20)EC	This feature was enhanced, so that adding an interface as a slave interface automatically removes the following Layer 3 parameters, if they are configured on that interface: IP address, IP access group, and PIM configuration.
12.2(15)BC2	This feature was enhanced, so that adding an interface as a slave interface automatically removes the following Layer 3 parameters, if they are configured on that interface: IP address, IP helper address, IP access group, PIM configuration, and IP policy-based routing. Also, creating subinterfaces on slave interfaces has been specifically prohibited. Previously, subinterfaces could be created on slave interfaces, although a warning message appeared advising users to remove the subinterface.

Finding Support Information for Platforms and Cisco IOS Software Images

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

Contents

- [Prerequisites for Cable Bundling, page 2](#)
- [Restrictions for Cable Bundling, page 2](#)
- [Information About Cable Bundling, page 3](#)
- [Configuring Cable Bundling, page 4](#)
- [Configuration Examples for Cable Interface Bundling, page 9](#)
- [Additional References, page 10](#)

Prerequisites for Cable Bundling

- The cable interfaces that make up a bundle must all be in the same Cisco CMTS chassis router. You cannot bundle cable interfaces that are in separate routers.
- All cable interfaces must continue to be configured with the required DOCSIS upstream and downstream RF parameters. In addition, the master cable interface must be configured with all of the required Layer 3 parameters, such as the IP address and any helper addresses.
- When using both cable interface bundling and loadbalancing of downstreams, we recommend that each load balance group contain only downstreams in the same cable interface bundle group.

Restrictions for Cable Bundling

- Cable interface bundling is only supported on cable interfaces. It is not supported on other interfaces.
- Cable interface bundling can be used only in two-way cable installations. It is not supported for telco-return configurations.
- Each cable bundle must have exactly one interface that is designated as the master interface. All other cable interfaces in the bundle must be slave interfaces.
- All Layer 3 configurations, such as the IP address, access lists, DHCP relay, ARP handling, and source-verify checking, must be specified on the master interface. You cannot configure these parameters on the slave interfaces in the bundle. (However, you must still configure the DOCSIS upstream and downstream parameters on each interface.)
- If using subinterfaces, create the subinterfaces only on the master interface, and configure only the subinterfaces with the Layer 3 information, such as IP addresses and access lists. (Cable modems are associated only with the master subinterfaces and not the master main interface.)

Do not create subinterfaces on a slave interface. In Cisco IOS Release 12.2(15)BC2 and later releases, this is specifically prohibited. In prior releases, a warning message appeared when trying to create a subinterface on a slave interface, but the subinterface was still created.

- When you have configured a Cisco uBR7200 series router for both N+1 redundancy and cable interface bundling, the failure of one interface in a bundle causes the failover of the entire bundle. When you have configured a Cisco uBR10012 router for both N+1 redundancy and cable interface bundling, the failure of one cable interface results only in the failover of that particular interface.
- You must configure interface bundles only by using CLI commands. You cannot use MIB objects to configure cable interface bundles through SNMP sets.

- Multicast broadcasts have the following restrictions on bundled cable interfaces:
 - For multicast addresses, the multicast MAC address points to the group of interfaces in the bundle that have received Internet Group Management Protocol (IGMP) joins.
 - Since the multicast IP to MAC mapping is not unique, multiple multicast IP address share one entry in the MAC forwarding table.
- When using bundled cable interfaces on the Cisco 7200 series routers, the input packet counters for the master interface also include the packet counts for slave interfaces, except when using a Broadband Processing Engine (BPE) cable interface (such as the Cisco uBR-MC16U/X and Cisco uBR-MC28U/X). On BPE cards and on the Cisco uBR10012 router, the input counters for master and slave cable interfaces are not combined.

Information About Cable Bundling

Cable bundling allows multiple cable interfaces to use the same IP subnet, which allows service providers to conserve their limited IP address space. Using this feature allows several physical cable interfaces to be logically bundled together into a single, Layer 3 interface.

When interfaces are bundled together, one interface is designated as the master interface, and all of the other interfaces in the bundle become the slave interfaces. You then configure only the master interface with the Layer 3 information, such as IP addresses, access lists, **cable source-verify**, and so forth. This information is then propagated to the slave interfaces.

When cable modems come online any of the interfaces in a bundle, the Cisco CMTS router creates a MAC-based forwarding table that maps each cable modem (or customer premises equipment [CPE] device) with the actual physical cable interface that it is using. The router creates this table automatically, and you do not need to reconfigure the cable modems or the routing tables on the Cisco CMTS router.

When the Cisco CMTS router receives a multicast packet on an interface bundle, it forwards it to all of the interfaces that are associated with this address in the bundle forwarding table. If the multicast MAC address is not in the bundle forwarding table, the router forwards the multicast traffic to all interfaces in the bundle.

Multicast MAC addresses are added to the bundle forwarding table in two ways:

- A static group is configured on the interface, in which case the multicast MAC address is added for all cable interfaces in the bundle. The MAC address is removed from the table when the static group configuration is removed.
- An interface receives an IGMP join request, in which case the multicast MAC address is added only for that particular interface. The MAC address is removed from the table when the interface receives an IGMP leave request.

You can add, remove, or shut down slave interfaces without affecting any of the other interfaces in the bundle. However, when you shut down or remove the master interface in a bundle, the slave interfaces remain in an online state, but no data packets are sent to any of these slave interfaces.

When the master interface is shut down, the active slave interfaces continue to receive packets, but the interfaces discard those packets as long as the master interface remains shut down. In this situation, cable modems that are connected to the slave interfaces remain online for a period of time, but they cannot renew their IP address with the DHCP server if the DHCP lease expires. Also, other cable modems cannot come online, because they cannot obtain an IP address or download a DOCSIS configuration file.

Benefits

- Cable interface bundling eliminates the need for an IP subnet for each cable interface by using only one IP subnet for each bundle of cable interfaces. This simplifies network management and conserves IP address space.
- Using cable bundling simplifies adding new cable interface line cards. When you add a new cable interface line card, you can simply assign the new interfaces to a cable bundle, without having to reassign IP addresses or create new subnets for the new set of interfaces.
- Cable bundling simplifies scalability and network management, because you can add a new cable interface line card to a bundle, and move cable modems to the new interfaces, without having to reconfigure the cable modems with new IP addresses or having to make any changes to the modem provisioning system. You can also move cable modems to other interfaces in the bundle at any time, without having to change their configuration. In particular, cable modems being assigned a static IP address can be inserted on any interface that is part of the bundle.

Configuring Cable Bundling

To create a cable bundle and to configure one cable interface to be its master interface, and one or more cable interfaces to be its slave interfaces, use the following procedure.

Prerequisites

- The master cable interface should be configured with the proper Layer 3 operational parameters, such as IP address, access lists, DHCP relay information, and so forth.
- Slave cable interfaces cannot be configured with an IP address, IP helper address, or other Layer 3 information. You must remove all Layer 3 configuration parameters from an interface before adding it to a bundle as a slave interface.

**Note**

In Cisco IOS Release 12.2(15)BC2 and later releases, configuring a cable interface as a slave interface automatically removes Layer 3 information, such as the IP address, helper address, access group, Protocol Independent Multicast (PIM) configuration, and policy-based routing.

- All cable interfaces must still be configured with the required DOCSIS RF upstream and downstream parameters.

**Note**

Attempting to configure an IP address, IP helper address, or any other Layer 3 configuration on a slave interface in a bundle produces a warning message to remove the configuration. The Layer 3 configuration information must be removed from the slave interface to ensure proper operation of the interface bundle.

Restrictions

- Configuring a cable interface to be part of a bundle automatically shuts down the interface and reenables it. This automatically forces all cable modems on that interface to go offline and to reregister with the CMTS.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface cable** *x/y/z*
4. **cable bundle** *n* **master**
5. **ip address** *ip-address subnet*
6. (any other Layer 3 configuration parameters)
7. **interface cable** *x/y/z*
8. **no ip address**
9. **cable bundle** *n*
10. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable Router#	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal Router(config)#	Enters global configuration mode.
Step 3	interface cable <i>x/y/z</i> Example: Router(config)# interface cable 5/1/0 Router(config-if)#	Enters interface configuration mode for the indicated cable interface.
Step 4	cable bundle <i>n</i> master Example: Router(config-if)# cable bundle 1 master Router(config-if)#	Configures the cable interface to be the master interface for the specified bundle group. <i>n</i> = Bundle group number. The valid range is 1 to 255, with no default.
Step 5	ip address <i>ip-address subnet</i> Example: Router(config-if)# ip address 192.168.100.1 255.255.255.0 Router(config-if)#	Assigns the specified IP address and subnet mask to the master interface for the bundle.

	Command or Action	Purpose
Step 6	<any other Layer 3 configuration parameters> Example: Router(config-if)# ip address 10.10.1.1 255.255.255.0 secondary Router(config-if)#	(Optional) Configure the master interface with any other Layer 3 configuration parameters that are necessary.
Step 7	interface cable <i>x/y/z</i> Example: Router(config-if)# interface cable 5/1/1 Router(config-if)#	Enters interface configuration mode for the indicated cable interface.
Step 8	no ip address Example: Router(config-if)# no ip address Router(config-if)#	(Optional) Removes the IP address (if any) that was previously assigned to this cable interface. This command is optional but recommended, because the show ip interface brief command reports an interface as being not OK if its configuration does not include some form of the ip address command. Specifying no ip address corrects this. Note In Cisco IOS Release 12.2(15)BC2 and later releases, configuring a cable interface as a slave interface automatically removes Layer 3 information, such as the IP address, IP helper address, IP access group, and IP policy-based routing.
Step 9	cable bundle <i>n</i> Example: Router(config-if)# cable bundle 1 Router(config-if)#	Configures the cable interface to be a slave bundle for the specified bundle group. <i>n</i> = Bundle group number. The valid range is 1 to 255, with no default. Note When you configure a cable interface to be a slave interface in a cable bundle, the router automatically removes all Layer 3 and other generic configuration information from the interface (IP address, access lists, and so forth).
Note Repeat Step 7 and Step 9 for each cable interface that is to be a member of this bundle. Repeat Step 3 through Step 9 for each cable bundle that is to be created on the router.		
Step 10	end Example: Router(config-if)# end Router#	Exits interface configuration mode and returns to privileged EXEC mode.

**Note**

To remove a cable interface from a bundle, use the **no cable bundle** command in interface configuration mode. Remember to reconfigure all of the Layer 3 IP information on the interface before attempting to bring cable modems back online the unbundled interface.

Monitoring Cable Interface Bundling

Table 1 lists the commands that are useful in monitoring the cable interface bundling feature:

Table 1 *Commands to Monitor Cable Interface Bundling*

Command	Description
show arp	Displays the entries in the router's ARP table.
show cable bundle <i>number</i> forwarding-table	Displays the MAC forwarding table for the specified bundle, showing the MAC addresses of each cable modem in a bundle and the physical cable interface that it is currently using.
show cable modem	Displays the cable modems that are online both before and after cable interface bundling has been configured.
show running-config interface cable [<i>slot/subslot</i> <i>slot/subslot/port</i>]	Displays the configuration for the specified cable interface.

show running-config interface cable Command

To display the bundles that are configured on a Cisco CMTS router, display the running configuration for each of the cable interfaces, using a command similar to the following:

```
show running-config interface cable slot/subslot
or
show running-config interface cable slot/subslot/port
```

For example, the following excerpt from a typical display shows that cable interface 3/0 is the master interface for bundle 1, and that cable interface 4/0 is a slave interface:

```
Router# show running-config interface cable 3/0
```

```
!
interface Cable3/0
 ip address 10.13.0.1 255.255.0.0 secondary
 ip address 10.12.0.1 255.255.0.0
 ip pim dense-mode
 ip igmp static-group 225.2.2.2
 no ip mroute-cache
 cable spectrum-group 5
 cable enable-trap cmonoff-notification
 cable max-hosts 2
 cable bundle 1 master
```

...

```
cable helper-address 172.22.127.2 cable-modem
cable helper-address 10.1.1.1
cable helper-address 10.2.2.2 host
no keepalive
```

```
Router# show running-config interface cable 4/0
```

```
interface Cable4/0
 no ip address
 cable bundle 1
```

...

```
cable helper-address 172.22.85.86
no keepalive
```

```
Router#
```

show cable bundle Command

Use the **show cable bundle** command to display the contents of the MAC forwarding information table for a specific cable interface bundle that has been configured on the Cisco CMTS router. This command has the following syntax:

```
show cable bundle n forwarding-table
```

The following example shows typical output for the **show cable bundle** command:

```
Router# show cable bundle 1 forwarding-table
```

MAC address	Interface	Flags	Location	link	sublink
00c0.5e01.0203	Cable8/0/0	3	64E5BF60	0	64E5BE00
00c0.5e01.0203	Cable7/0/0	3	64E5BE00	0	0
00c0.5e01.0101	Cable8/0/0	3	64E5BEE0	0	64E5BE40
00c0.5e01.0101	Cable7/0/0	3	64E5BE40	0	0
00c0.a375.cc1c	Cable8/0/0	1	64E5BEC0	0	0
00c0.0e01.a835	Cable8/0/0	1	64E5BEA0	0	0
00c0.0e01.a799	Cable8/0/0	1	64E5BDE0	0	0
00c0.0e01.a405	Cable8/0/0	1	64E5BF00	0	0
00c0.0e01.a5d1	Cable7/0/0	1	64E5BE20	0	0
00c0.0e01.a5d9	Cable8/0/0	1	64E5BE60	0	0
00c0.0e01.a5e1	Cable7/0/0	1	64E5BF40	0	0
00c0.0e01.a5f1	Cable7/0/0	1	64E5BE80	0	0
00c0.0eb4.0a41	Cable5/0/0	1	63704D1C	0	0
00c0.f03b.ed59	Cable6/1/0	1	6370427C	0	0
00c0.f03b.ed97	Cable6/1/0	1	63703F3C	0	0
00c0.0eb4.1373	Cable5/0/0	1	6370479C	0	0
00c0.f03b.edd3	Cable6/1/0	1	637042BC	0	0
00c0.7371.6df6	Cable5/0/0	1	63703DFC	0	0

```
Total = 18, sublink total = 2
```

```
Free = 1016, low_mark = 1016
```

```
Router#
```

The **show bundle** command displays the following information:

- **MAC address**—Identifies the MAC (hardware) address for a cable modem that is using an interface in the bundle.
- **Interface**—Identifies the cable interface slot and port number.
- **Flag**—Bitmask showing the current value of the flag byte for this bundle entry. The following bits can be set:
 - Bit 0 (0x01) = Bundle is active.
 - Bit 1 (0x02) = Bundle is a static multicast group.

Multiple bits can be set, so that a value of 3 indicates an active, static multicast group.

Configuration Examples for Cable Interface Bundling

This section contains the following sample configurations for the cable interface bundling feature:

- [Basic Cable Interface Bundling Example, page 9](#)

Basic Cable Interface Bundling Example

The following excerpt from a configuration file shows cable interface 4/0 being configured as the master interface for bundle 1, and interface 5/0 being configured as the first slave interface in the bundle. Note that all Layer 3 information is configured only on the master interface, but Layer 2 information, such as the DOCSIS RF configuration, is still configured on each interface.

```
!  
interface Ethernet2/0  
  ip address 172.16.135.11 255.255.255.128  
  no ip mroute-cache  
  half-duplex  
!  
  
interface Cable4/0  
  ip address 172.16.30.1 255.255.255.0  
  ip helper-address 172.16.135.20  
  no ip route-cache cef  
  no keepalive  
  cable bundle 1 master  
  cable downstream rate-limit token-bucket shaping  
  cable downstream annex B  
  cable downstream modulation 64qam  
  cable downstream interleave-depth 32  
  cable downstream frequency 555000000  
  cable upstream 0 frequency 40000000  
  cable upstream 0 power-level 0  
  no cable upstream 0 shutdown  
  cable upstream 1 shutdown  
  cable upstream 2 shutdown  
  cable upstream 3 shutdown  
  cable upstream 4 shutdown  
  cable upstream 5 shutdown  
  cable dhcp-giaddr policy  
!  
interface Cable5/0  
  no ip address  
  load-interval 30  
  no keepalive  
  cable bundle 1  
  cable downstream rate-limit token-bucket shaping  
  cable downstream annex B  
  cable downstream modulation 64qam  
  cable downstream interleave-depth 32  
  cable downstream frequency 620000000  
  cable upstream 0 frequency 25008000  
  cable upstream 0 power-level 0  
  cable upstream 0 channel-width 1600000 3200000  
  no cable upstream 0 shutdown  
  no cable upstream 1 shutdown  
  no cable upstream 2 shutdown  
  cable upstream 3 shutdown  
  cable upstream 4 shutdown  
  cable upstream 5 shutdown
```

```

cable dhcp-giaddr policy
!

```

Additional References

The following sections provide references related to the cable interface bundling feature.

Related Documents

Related Topic	Document Title
CMTS Command Reference	<i>Cisco Broadband Cable Command Reference Guide</i>, at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/cable/bbcmref/index.htm
Cisco IOS Release 12.2 Command Reference	Cisco IOS Release 12.2 Configuration Guides and Command References, at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/index.htm
Cable Features Configuration Guide	<i>Cisco CMTS Feature Guide</i>, at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/cable/cab_rout/cmtsfg/index.htm
Installing Cisco uBR7100 series routers	<i>Cisco uBR7100 Series Universal Broadband Router Hardware Installation Guide</i>
Configuring Cisco uBR7100 series routers	<i>Cisco uBR7100 Series Universal Broadband Router Software Configuration Guide</i>
Installing Cisco uBR7200 Series Routers	<i>Cisco uBR7200 Series Universal Broadband Router Hardware Installation Guide</i> <i>Cisco uBR7200 Series Universal Broadband Router Cable Modem Card Installation and Configuration publication</i> <i>Cisco uBR7200 Series Universal Broadband Router Port Adapter Installation and Configuration publication</i> <i>Cisco uBR7200 Series Universal Broadband Router 550-Watt DC-Input Power Supply Replacement Instructions</i> <i>Cisco uBR7200 Series Universal Broadband Router Subchassis and Midplane Replacement Instructions</i> <i>Cisco uBR7200 Series Rack-Mount and Cable-Management Kit Installation Instructions</i> <i>Cisco uBR7200 Series Universal Broadband Router Fan Tray Replacement Instructions</i>

Related Topic	Document Title
Configuring Cisco uBR7200 Series Routers	Cisco uBR7200 Series Universal Broadband Router Software Configuration Guide Cisco uBR7200 Series Universal Broadband Router Feature Enhancements publication
Installing Cisco uBR10012 Router	Cisco uBR10012 Series Universal Broadband Router Hardware Installation Guide 2400W AC-Input Power Shelf for the Cisco uBR10000 Series Universal Broadband Router Cable Interface Line Card Processor Hardware Installation for the Cisco uBR10000 Series Universal Broadband Router Fan Assembly Module for the Cisco uBR10000 Series Universal Broadband Router DC Power Entry Module for the Cisco uBR10000 Series Universal Broadband Router Performance Routing Engine Card Hardware Installation for the Cisco uBR10000 Series Universal Broadband Router TCC+ Card for the Cisco uBR10000 Series Universal Broadband Router
Configuring the Cisco uBR10012 Router	Cisco uBR10012 Universal Broadband Router Software Configuration Guide

Standards

Standards	Title
SP-RFiv1.1-I09-020830	Data-over-Cable Service Interface Specifications Radio Frequency Interface Specification, version 1.1
SP-RFiv2.0-I03-021218	Data-over-Cable Service Interface Specifications Radio Frequency Interface Specification, version 2.0
SP-OSSiv2.0-I03-021218	Data-over-Cable Service Interface Specifications Operations Support System Interface Specification, version 2.0
SP-BPI+-I09-020830	Data-over-Cable Service Interface Specifications Baseline Privacy Plus Interface Specification, version 2.0

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

No new or modified RFCs are supported by this feature.

Technical Assistance

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

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, TeleRouter, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0502R)



Cable Monitor and Intercept Features for the Cisco CMTS

The Cable Monitor and Intercept features for Cisco Cable Modem Termination System (CMTS) routers provide a software solution for monitoring and intercepting traffic coming from a cable network. This feature also gives service providers Lawful Intercept capabilities, such as those required by the Communications Assistance for Law Enforcement Act (CALEA).

Feature Specifications for the Cable Monitor

Feature History

Release	Modification
12.0(6)SC, 12.1(2)EC	The cable intercept command was introduced for the Cisco uBR7200 series routers.
12.1(3a)EC	The cable monitor command was introduced for Cisco uBR7200 series routers.
12.1(5)EC	Support for both commands was added for the Cisco uBR7100 series routers.
12.1(11b)EC	The cable intercept command was enhanced to allow the data collector to be more than two hops from the Cisco CMTS.
12.1(4)CX	The sid option was added to the cable monitor command for DOCSIS 1.1 support.
12.2(4)BC1	Support for these commands was added to the Release 12.2 BC train for the Cisco uBR7100 series, Cisco uBR7200 series, and Cisco uBR10012 universal broadband routers.

Supported Platforms

Cisco uBR7100 series, Cisco uBR7200 series, and Cisco uBR10012 universal broadband routers

Finding Support Information for Platforms and Cisco IOS Software Images

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



Corporate Headquarters:

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

Copyright © 2003 Cisco Systems, Inc. All rights reserved.

Contents

- [Prerequisites for Cable Monitor and Intercept, page 14](#)
- [Restrictions for Cable Monitor and Intercept, page 14](#)
- [Information About Cable Monitor and Intercept, page 14](#)
- [How to Configure for Cable Intercept and Monitoring, page 17](#)
- [Monitoring the Cable Intercept and Monitor Features, page 21](#)
- [Configuration Examples, page 23](#)
- [Additional References, page 24](#)

Prerequisites for Cable Monitor and Intercept

- The Cisco CMTS must be running Cisco IOS Release 12.1(3a)EC and later 12.1 EC releases, or Cisco 12.2(4)BC or later 12.2 BC releases.

Restrictions for Cable Monitor and Intercept

- The **cable intercept** command by itself does not fulfill the PacketCable requirements for Lawful Intercept capability. To meet these requirements, PacketCable operations must also be enabled and configured on the Cisco CMTS router (see the documents in the [“Additional References” section on page 24](#) for instructions on enabling PacketCable).
- The WAN interface on which packets are forwarded when using the **cable monitor** command should be used exclusively by the LAN analyzer. This interface must be an Ethernet, Fast Ethernet, or Gigabit Ethernet interface.
- Intercepted data from the **cable intercept** command is sent to a user-specified User Datagram Port (UDP) at a user-specified IP address. The data collector at that IP address must have exclusive use of the specified UDP port.
- The interception of customer traffic is governed by local laws and the service level agreements (SLA) with those customers. Consult the proper legal authorities before intercepting and monitoring third-party traffic. Also see the documents on CALEA and Lawful Intercept in the [“Additional References” section on page 24](#).

Information About Cable Monitor and Intercept

Cisco CMTS routers support the following two complementary commands to intercept traffic being sent or received over a cable interface:

- **cable intercept**—Forwards copies of the traffic to and from a specific MAC address to a server at a specific IP address and UDP port. This command can be used to respond to CALEA requests from law enforcement for traffic concerning a specific user.
- **cable monitor**—Forwards copies of selected packets on the cable interface to an external LAN analyzer attached to another interface on the Cisco CMTS router. This command can help in troubleshooting network and application problems.

See the following sections for more information about these commands.

**Note**

These commands do not monitor or intercept traffic for the purpose of preventing denial-of-service attacks and other types of network attacks. With both of these commands, the traffic continues on to its original destination, and only copies of the selected packets are forwarded to the CALEA server or LAN analyzer.

Overview of the cable interface Command

The **cable intercept** command forwards all traffic to and from a particular MAC address on a specific cable interface to a data collection server at a particular IP address and User Datagram Protocol (UDP) port. This command examines the source and destination MAC addresses of each Ethernet frame that is transmitted over the selected cable interface, and when a match is found, a copy of the frame is encapsulated within a UDP packet and forwarded to the specified server.

**Note**

The MAC address being intercepted is typically the MAC address of a user's CPE device (PC, Voice-over-IP phone, or so forth), not the MAC address of the cable modem.

This command can be used to comply with the United States Federal Communications Assistance for Law Enforcement Act (CALEA) and other Lawful Intercept requirements for voice communications. For specifics on CALEA Lawful Intercept, see the *PacketCable Electronic Surveillance Specification*, as listed in the [“Additional References” section on page 24](#).

This command requires that the law enforcement agency (LEA) provide a server at the specified IP address with an application that monitors the given UDP port and collects all of the data sent to that port. The choice of this application is up to the LEA. Although this application could be as simple as a packet sniffer, typically the LEA would desire a more complex application that could reconstruct the user's original data or voice traffic.

**Note**

Before Cisco IOS Release 12.1(11b)EC, the destination server had to be within two network hops of the Cisco CMTS router. This restriction was removed in Cisco IOS Release 12.1(11b)EC, 12.2(4)BC1, and all later releases.

Overview of the cable monitor Command

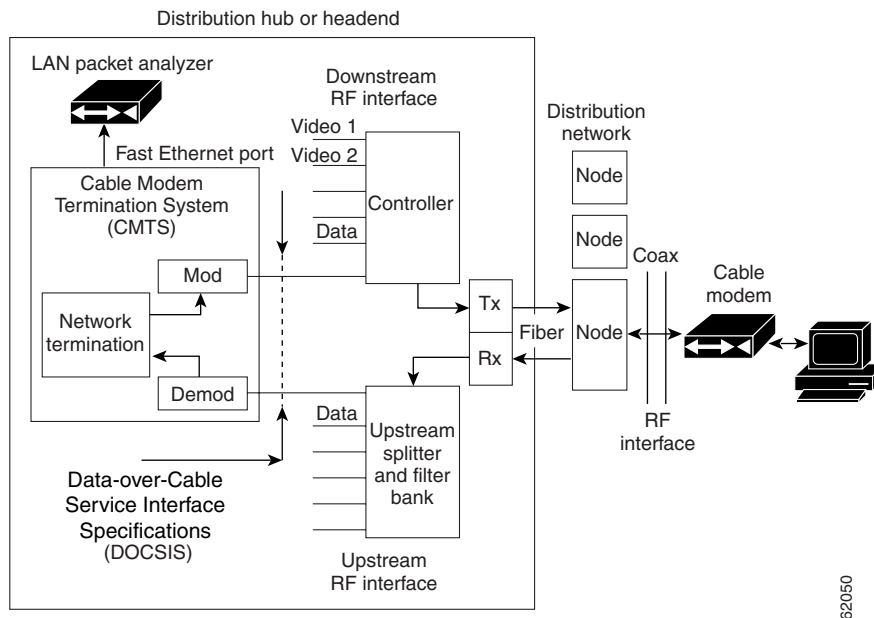
The **cable monitor** command sends copies of packets for specific types of traffic that is sent over a particular cable interface to a LAN analyzer, for use in troubleshooting network problems. This command can select packets to be forwarded using one or more of the following parameters:

- Either incoming or outbound packets
- Packets that match an IP access list
- Packets that match a specific MAC address (source and destination)
- Packets with a specific Service ID (SID)
- When monitoring a specific SID, select only specific DOCSIS MAC-layer packet types (dynamic service packets, MAP grant packets, and MAP request packets)

In addition, the **cable monitor** command can forward full DOCSIS packets, or it can strip the DOCSIS headers and forward only the Ethernet frames. Packets can also be timestamped to aid in troubleshooting. The packets are then forwarded out of the specified Ethernet or Fast Ethernet port to the LAN analyzer for additional analysis.

Figure 1 illustrates a LAN packet analyzer attached to a Fast Ethernet port in a DOCSIS two-way configuration.

Figure 1 LAN Packet Analyzer in a DOCSIS Two-Way Configuration



Note

The WAN port used for cable monitoring should be exclusively used by the LAN packet analyzer.



Tip

When you are using the **cable monitor** command, and are including the DOCSIS header along with the Ethernet frame, it is possible that the total size of the forwarded packet could exceed the maximum allowable size for an Ethernet frame (1500 bytes), if the original Ethernet frame is at or near 1500 bytes. This is because the **cable monitor** command adds the DOCSIS header to the existing Ethernet frame. If this happens, the console displays a system message similar to the following:

```
%LINK-4-TOOBIG:Interface Ethernet2/0, Output packet size of 1518 bytes too big
```

This error message is typically accompanied by a traceback display. Both the error message and traceback are informational only and can be ignored. They do not indicate a traffic flow problem with the cable modem being monitored.

Benefits

The **cable intercept** command helps the CMTS or network administrator to:

- Comply with CALEA requirements for Lawful Intercept.

- Comply with PacketCable requirements for electronic surveillance.

Monitoring upstream and downstream data packets with the **cable monitor** command helps the CMTS or network administrator to:

- Manage network variables and understand network issues that affect application performance and functionality.
- Resolve interoperability problems.

How to Configure for Cable Intercept and Monitoring

See the following sections to enable and configure the cable intercept and monitoring features.

- [Configuring the cable intercept Command, page 17](#)
- [Configuring the cable monitor Command, page 19](#)

Configuring the cable intercept Command

To enable the cable intercept feature on a particular cable interface, use the following procedure, starting in privileged EXEC mode.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface cable *x/y***
4. **cable intercept *mac-address ip-address udp-port***
5. **exit**
6. **exit**

DETAILED STEPS

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

	Command or Action	Purpose
Step 3	interface cable <i>x/y</i> Example: Router(config)# interface cable 4/0 Router(config-if)#	Enters cable interface configuration mode for the specified cable interface.
Step 4	cable intercept <i>mac-address ip-address udp-port</i> Example: Router(config-if)# cable intercept 000C.0102.0304 10.10.10.45 8132 Router(config-if)#	Enables cable interception on this cable interface with the following parameters: • <i>mac-address</i> = Specifies the MAC address for traffic that is to be intercepted. Packets with a source or destination MAC address that matches this address are forwarded. Typically, this is the MAC address of the user's CPE device (such as a PC or VoIP phone), not the MAC address of the user's cable modem. • <i>ip-address</i> = Specifies the IP address for the data collection server that is to receive copies of the forwarded traffic. • <i>udp-port</i> = Specifies the destination UDP port number at the data collection server. The valid range is 0 to 65535 with no default. This port must be unused except by the data collection server at this IP address.
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.

Configuring the cable monitor Command

To enable cable monitoring on a particular cable interface, use the following procedure, starting in privileged EXEC mode.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface cable** *x/y*
4. **cable monitor** [*incoming* | *outbound*] [*timestamp*]
interface *interface* { **access-list** {*name* | *number*} | **mac-address** *address* | **sid** *sid-number*}
[**packet-type** {*data docsis* | *data ethernet* | [*mac type type*] }]
5. **exit**

6. exit

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable Router#	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal Router(config)#	Enters global configuration mode.
Step 3	interface cable x/y Example: Router(config)# interface cable 4/0 Router(config-if)#	Enters cable interface configuration mode for the specified cable interface.

Command or Action	Purpose
Step 4 <pre> cable monitor [incoming outbound] [timestamp] interface interface {access-list {name number} mac-address address sid sid-number} [packet-type {data docsis data ethernet mac [type type]}] Example: Router(config-if)# cable monitor interface e1/2 mac-address 0123.4567.89ab packet-type data docsis Router(config-if)# </pre>	Enables cable monitoring on the cable interface with the following parameters: • incoming—(Optional) Forwards only packets being received on the upstream. • outbound—(Optional) Forwards only packets being transmitted on the downstream. • timestamp—(Optional) Appends a four-byte timestamp, in hundredths of a second, to the packets when they are forwarded to the LAN analyzer. • interface interface—Specifies the WAN interface on the router to which the LAN analyzer is connected. This interface should be used exclusively by the LAN analyzer. Identify the packets to be monitored by selecting one of the following: • access-list—Selects packets that match the specified access list. You can specify the access list by name or by number (1 to 2699). • mac-address—Specifies the MAC address for packets that should be forwarded. • sid—Selects packets with the specified service ID (SID). The valid range is 1 to 16384. You can configure the types of packets to be forwarded with the following options: • packet-type—(Optional) Selects the type of packet to be forwarded: – data docsis—Forward only data packets as full complete DOCSIS frames. – data ethernet—Forward only data packets by stripping off the DOCSIS header and forwarding only the Ethernet frame. – mac—Forwards only the MAC-layer packets. When monitoring a specific SID, you can also optionally specify the type option with one of the following MAC-layer message types: dsa, dsc, dsd, map-grant, map-req.
Note Repeat Step 4 for each type of packet or MAC address to be monitored.	
Step 5 <pre> exit Example: Router(config-if)# exit Router(config)# </pre>	Exits interface configuration mode.

	Command or Action	Purpose
Step 6	exit	Exits global configuration mode.
	Example: Router(config)# exit Router#	

Monitoring the Cable Intercept and Monitor Features

To display information about the operation of the cable intercept and cable monitor commands, use the following procedures:

- [Displaying Information About Intercepted Traffic, page 21](#)
- [Displaying Information About Monitored Traffic, page 21](#)
- [DOCSIS Data Packets Example, page 22](#)
- [Timestamped Packets Example, page 22](#)

Displaying Information About Intercepted Traffic

To display information about what traffic is being forwarded by the **cable intercept** command, use the **show interface cable intercept** command:

```
Router# show interface c6/0 intercept

          Destination  Destination
MAC Address  IP Address  UDP Port
00C0.0102.0DEF  10.10.10.131  7512

Router#
```

Displaying Information About Monitored Traffic

To display information about what traffic is being sent to the external LAN analyzer by the **cable monitor** command, use the **show interface cable monitor** command:

```
Router# show interface cable 1/0 monitor

US/  Time Outbound  Flow      Flow Type      Flow  Packet  MAC   MAC   Encap
DS   Stmp Interface Type      Identifier      Extn. Type  Extn. Type  Type
all  yes  Et1/0  mac-addr  0050.5462.008c yes  data   no    -    Ethernet
us   yes  Et1/0  acc-list  300              no    -    no    -    -
us   no   Et1/0  sid       2                yes  mac    yes  map-grant -
all  no   Et1/0  acc-list  rrr              no    -    no    -    -
all  no   Et1/0  mac-addr  0042.b013.008c yes  data   no    -    Ethernet
all  no   Et1/0  upstream  0                yes  data   no    -    docsis

Router#
```

DOCSIS Data Packets Example

This example shows sample DOCSIS packets that have been captured by the **cable monitor** command and forwarded to a LAN analyzer. The hexadecimal dump for the first packet is the following:

```
LLC: ----- LLC Header -----
      LLC:
      LLC: DSAP Address = E2, DSAP IG Bit = 01 (Group Address)
      LLC: SSAP Address = FA, SSAP CR Bit = 00 (Command)
      LLC: I frame, N(R) = 71, N(S) = 47, POLL
      LLC:
DLC: Frame padding= 43 bytes
ADDR  HEX                                     ASCII
0000:c0 00 00 1c ea 1d 00 03 fe e1 a0 54 00 03 e3 fa | .....T....
0010:5e 8f 00 0a 00 00 03 01 04 00 00 03 00 00 00 8a | ^.....
0020:4d 6e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | Mn.....
0030:00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | .....
```

The relevant DOCSIS bytes are the following:

- Byte 0x16—Control Field. A value of 03 indicates an unnumbered information frame.
- Byte 0x17—Version of the MAC management protocol. A value of 1 indicates a DOCSIS 1.0 message and a value of 2 indicates DOCSIS 1.1 message.
- Byte 0x18—MAC message type. In this example, a value of 04 indicates a Ranging Request (RNG-REQ) message.

The hexadecimal dump of the next packet is the following:

```
LLC: ----- LLC Header -----
      LLC:
      LLC: DSAP Address = FE, DSAP IG Bit = 00 (Individual Address)
      LLC: SSAP Address = E0, SSAP CR Bit = 01 (Response)
      LLC: I frame, N(R) = 42, N(S) = 80
      LLC:
DLC: Frame padding= 43 bytes
ADDR  HEX                                     ASCII
0000:c2 00 00 2b 00 00 00 03 e3 fa 5e 8f 00 03 fe e1 | ...+.....^....
0010:a0 54 00 19 00 00 03 01 05 00 00 03 01 01 04 00 | .T.....
0020:00 00 00 02 01 00 03 02 00 00 05 01 03 00 8a 4d | .....M
0030:6e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | n.....
```

This packet has a MAC message type of 05, indicating a Ranging Response (RNG-RSP) message.



Note

For complete information on the DOCSIS MAC packet format, see Chapter 6 in the DOCSIS 1.1 specification (see the [“Additional References” section on page 24](#)).

Timestamped Packets Example

The following example shows how to interpret the four-byte timestamp that is appended to packets that are forwarded by the **cable monitor** command when using the **timestamp** option. The following hexadecimal dump shows the 64-byte contents of the first MAP message packet being examined:

```
0000(0000): c302003A 00000000 01E02F00 00010008...../....
0010(0016): 0D6F4670 00260000 03010300 01380400 .oFp.&.....8..
0020(0032): 0061A1C1 0061A07C 00030004 FFFC4000 .a...a.|.....@.
0030(0048): 0189401F FFFC4042 0001C043 007EF4EA ..@...@B...C.~..
```

The relevant portions of this packet are the following:

- Byte 0—C3 indicates a MAP management message.
- Bytes 08 to 0D—Multicast address that is used to address cable modem when transmitting allocation MAP protocol data units (PDUs).
- Bytes 3C to 3F—Timestamp from the **cable monitor** command in hexadecimal (0x007EF4EA). This value is a 32-bit counter that is incremented every 10 milliseconds.

The following hexadecimal dump shows the second MAP message being forwarded:

```
0000(0000): C302003A 00000000 01E02F00 00010008 ...:...../.....
0010(0016): 0D6F4670 00260000 03010300 01380400 .oFp.&.....8..
0020(0032): 0061A5AE 0061A469 00030004 FFFC4000 .a...a.i.....@.
0030(0048): 0189401A FFFC403D 0001C03E 007EF4EF ..@...@=...>...~..
```

In this example, the timestamp is 0x007EF4EF. Subtracting the two timestamps (0x007EF4EF–0x007EF4EA) produces the time difference between the two MAP messages in hundredths of a second (which in this case is a difference of 5, for a total time difference of 50 milliseconds).

Configuration Examples

The following sections show sample configurations of the **cable intercept** and **cable monitor** commands:

- [Cable Intercept Configuration Example, page 23](#)
- [Cable Monitor Configuration Example \(MAC Address\), page 23](#)
- [Cable Monitor Configuration Example \(Ethernet, MAC-Layer, and DOCSIS-Data Packets\), page 24](#)

Cable Intercept Configuration Example

The following sample configuration shows traffic to and from MAC address 0003.e3fa.5e11 being forwarded to a data collection server at the IP address 172.18.73.189 and UDP port 9999:

```
!
interface Cable3/0
 cable intercept 0003.e3fa.5e11 172.18.73.189 9999
...
```

Cable Monitor Configuration Example (MAC Address)

The following example of the **cable monitor** command on a Cisco uBR7114 router monitors packets with the MAC address of 0002.b9ff.8c00. Both upstream and downstream packets are forwarded to a LAN analyzer on the router's Fast Ethernet interface (FE0/0).

```
!
interface cable 1/0
 cable monitor timestamp int fe0/0 mac-address 0002.b9ff.8c00 packet-type data ethernet
...
```

Cable Monitor Configuration Example (Ethernet, MAC-Layer, and DOCSIS-Data Packets)

The following example of the **cable monitor** command monitors Ethernet, MAC-layer, and DOCSIS-data packets with the MAC address of 0003.e3fa.5e8f, adding a timestamp to the packets before forwarding them to the LAN analyzer.

```
!
interface Cable 3/0
 ip address 10.100.100.1 255.255.255.0
 cable monitor timestamp int e2/0 mac-address 0003.e3fa.5e8f packet-type data ethernet
 cable monitor timestamp int e2/0 mac-address 0003.e3fa.5e8f packet-type mac
 cable monitor timestamp int e2/0 mac-address 0003.e3fa.5e8f packet-type data docsis
...
```

Additional References

For additional information related to the Cable Monitor and Intercept feature, refer to the following references:

Related Documents

Related Topic	Document Title
CMTS Command Reference	<i>Cisco Broadband Cable Command Reference Guide</i>, at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/cable/bbccmref/index.htm
Cisco IOS Release 12.2 Command Reference	Cisco IOS Release 12.2 Configuration Guides and Command References, at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/index.htm
PacketCable Configuration	<i>PacketCable for the Cisco CMTS</i>, in the Cisco CMTS Feature Guide, at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/cable/cab_rout/cmtsfg/ufg_pkcb.htm
Using the LAN analyzer	See the documentation for the LAN analyzer or other network interception software you are using for instructions on decoding DOCSIS MAC frames. Note One possible software utility you can use for this purpose is the Ethereal software, which is available for Windows and Unix systems at http://www.ethereal.com. This software supports DOCSIS MAC-layer frames with release 0.9.6 and later.

Related Topic	Document Title
CALEA Information	See the Communications Assistance for Law Enforcement Act (CALEA), which was passed by the United States Congress in 1994 and is now sections 1001 to 1010 of the United States Code Title 47 (Telegraphs, Telephones, and Radiotelegraphs). Also see the information on Cisco's web site at the following URL: http://www.cisco.com/wwl/regaffairs/lawful_intercept/index.html
Lawful Intercept	Lawful Intercept Technical Documentation at the following URL: http://www.cisco.com/en/US/tech/tk583/tk799/tech_protocol_family_home.html

Standards

Standards ¹	Title
SP-RFIV1.1-I09-020830	Data-Over-Cable Service Interface Specifications Radio Frequency Interface Specification, version 1.1 (http://www.cablemodem.com)
PKT-SP-ESP-I01-991229	PacketCable™ Electronic Surveillance Specification (http://www.packetcable.com)

1. Not all supported standards are listed.

MIBs

MIBs ¹	MIBs Link
No new or modified MIBs are supported by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

1. Not all supported MIBs are listed.

RFCs

Description	Link
No new or modified RFCs are supported by this feature.	http://www.ietf.org/rfc.html

Technical Assistance

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

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, TeleRouter, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0502R)

Copyright © 2003 Cisco Systems, Inc. All rights reserved.



DHCP, ToD, and TFTP Services for the Cisco CMTS

This chapter describes how to configure Cisco Cable Modem Termination System (CMTS) platforms so that they support onboard servers that provide Dynamic Host Configuration Protocol (DHCP), Time-of-Day (ToD), and Trivial File Transfer Protocol (TFTP) services for use in Data-over-Cable Service Interface Specifications (DOCSIS) networks. In addition, this chapter provides information about optional configurations that can be used with external DHCP servers.

Feature Specifications for DHCP, ToD, and TFTP Services

Feature History	
Release	Modification
Release 11.3 NA	The cable source-verify and ip dhcp commands were supported on the Cisco uBR7200 series routers.
Release 12.0(4)XI	The cable time-server command was introduced.
Release 12.1(2)EC1	The following commands were introduced on the Cisco IOS Release 12.1 EC train: • cable config-file • cable dhcp-giaddr • cable helper-address Also, the dhcp keyword was added to the cable source-verify command.
Release 12.1(5)EC1	Support was added for the Cisco uBR7100 series routers.
Release 12.2(4)BC1	Support for the above commands was added to Cisco IOS Release 12.2 BC for the Cisco uBR7100 series, Cisco uBR7200 series, and Cisco uBR10012 routers.
Release 12.1(11b)EC1, Release 12.2(8)BC2	The cable tftp-enforce command was introduced.
Release 12.1(13)EC, Release 12.2(11)BC1	The leasetimer keyword was added to the cable source-verify command.
Supported Platforms	
Cisco uBR7100 series, Cisco uBR7200 series, Cisco uBR10012 universal broadband routers.	

Finding Support Information for Platforms and Cisco IOS Software Images

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

Contents

- [Prerequisites for DHCP, ToD, and TFTP Services, page 28](#)
- [Restrictions for DHCP, ToD, and TFTP Services, page 28](#)
- [Information About DHCP, ToD, and TFTP Services, page 29](#)
- [How to Configure DHCP, ToD, and TFTP Services, page 37](#)
- [Configuration Examples, page 55](#)
- [Additional References, page 68](#)

Prerequisites for DHCP, ToD, and TFTP Services

- Cisco recommends the most current Cisco IOS Release 12.1 EC software release for DOCSIS 1.0 operations. For DOCSIS 1.1 operations, Cisco recommends the most current Cisco IOS Release 12.2 BC software release.
- A separate DOCSIS configuration file editor is required to build DOCSIS 1.1 configuration files, because the internal DOCSIS configuration file editor that is onboard the Cisco CMTS router supports only DOCSIS 1.0 configuration files.
- To be able to use the Cisco CMTS as the ToD server, either alone or along with other, external ToD servers, you must configure the DHCP server to provide the IP address Cisco CMTS as one of the valid ToD servers (DHCP option 4) for cable modems.

Restrictions for DHCP, ToD, and TFTP Services

- The “all-in-one” configuration should not be used as the only set of servers except for small cable plants (approximately 2,500 cable modems, lab environments, initial testing, small deployments, and troubleshooting. The “all-in-one” configuration can be used in larger networks, however, to supplement other redundant and backup servers.
- The ToD server must use the UDP protocol to conform to DOCSIS specifications.
- For proper operation of the DOCSIS network, especially a DOCSIS 1.1 network using BPI+ encryption and authentication, the system clock on the Cisco CMTS must be set accurately. You can achieve this by manually using the **set clock** command, or by configuring the CMTS to use either the Network Time Protocol (NTP) or the Simple Network Time Protocol (SNTP).
- The internal DHCP server that is onboard the Cisco CMTS router does not support the **cable source-verify** command.

Information About DHCP, ToD, and TFTP Services

This section provides the following information about the DHCP, ToD, and TFTP Services feature, and its individual components:

- [Feature Overview, page 29](#)
- [Internal DHCP Server, page 30](#)
- [External DHCP Servers, page 32](#)
- [Time-of-Day Server, page 33](#)
- [TFTP Server, page 35](#)

Feature Overview

All Cisco CMTS platforms support onboard servers that provide DHCP, ToD, and TFTP services for use in DOCSIS cable networks. These servers provide the registration services needed by DOCSIS 1.0- and 1.1-compliant cable modems:

- [Internal DHCP Server](#)—Provides the cable modem with an IP address, a subnet mask, default gateway, and other IP related parameters. The cable modem connects with the DHCP server when it initially powers on and logs on to the cable network.
- [External DHCP Servers](#)—Provides the same functionality as the onboard DHCP server, but external DHCP servers are usually part of an integrated provisioning system that is more suitable when managing large cable networks.
- [Time-of-Day Server](#)—Provides an [RFC 868](#)-compliant ToD service so that cable modems can obtain the current date and time during the registration process. The cable modem connects with the ToD server after it has obtained its IP address and other DHCP-provided IP parameters.

Although cable modems do not need to successfully complete the ToD request before coming online, this allows them to add accurate timestamps to their event logs so that these logs are coordinated to the clock used on the CMTS. In addition, having the accurate date and time is essential if the cable modem is trying to register with Baseline Privacy Interface Plus (BPI+) encryption and authentication.

- [TFTP Server](#)—Downloads the DOCSIS configuration file to the cable modem. The DOCSIS configuration file contains the operational parameters for the cable modem. The cable modem downloads its DOCSIS configuration file after connecting with the ToD server.

You can configure and use each server separately, or you can configure an “all-in-one” configuration so that the CMTS acts as a DHCP, ToD, and TFTP server. With this configuration, you do not need any additional servers, although additional servers provide redundancy, load-balancing, and scalability.



Note

You can add additional servers in a number of ways. For example, most cable operators use Cisco Network Registrar (CNR) to provide the DHCP and TFTP servers. ToD servers are freely available for most workstations and PCs. You can install the additional servers on one workstation or PC or on different workstations and PCs.

Internal DHCP Server

At power-up, DOCSIS cable modems send a broadcast message through the cable interface to find a DHCP server that can provide the information needed for IP connectivity across the network. After the cable modem comes online, the CPE devices connected to the cable modem can also make their own DHCP requests. You can configure all Cisco CMTS platforms to act as DHCP servers that provide the IP addressing and other networking information that is needed by DOCSIS cable modems and their CPE devices.

DHCP Field Options

In its DHCP request message, the cable modem identifies itself by its MAC hardware address. In reply, a DOCSIS-compatible DHCP server should provide, at minimum, the following fields when replying to cable modems that are authorized to access the cable network:

- yiaddr—IP address for the cable modem.
- Subnet Mask (option 1)—IP subnet mask for the cable modem.
- siaddr—IP address for the TFTP server that will provide the DOCSIS configuration file.
- file—Filename for the DOCSIS configuration file that the cable modem must download.
- Router Option (option 3)—IP addresses for one or more gateways that will forward the cable modem traffic.
- Time Server Option (option 4)—One or more ToD servers from which the cable modem can obtain its current date and time.
- Time Offset (option 2)—Universal Coordinated Time (UTC) that the cable modem should use in calculating local time.
- giaddr—IP address for a DHCP relay agent, if the DHCP server is on a different network from the cable modem.
- Log Server Option (option 7)—IP address for one or more SYSLOG servers that the cable modem should send error messages and other logging information (optional).
- IP Address Lease Time (option 51)—Number of seconds for which the IP address is valid, at which point the cable modem must make another DHCP request.

If you decide to also provide IP addresses to the CPE devices connected to the cable modems, the DHCP server must also provide the following information for CPE devices:

- yiaddr—IP address for the CPE device.
- Subnet Mask (option 1)—IP subnet mask for the CPE device.
- Router Option, option 3—IP addresses for one or more gateways that will forward the CPE traffic.
- Domain Name Server Option (option 6)—IP addresses for the domain name system (DNS) servers that will resolve hostnames to IP addresses for the CPE devices.
- Domain Name (option 15)—Fully-qualified domain name that the CPE devices should add to their hostnames.
- IP Address Lease Time (option 51)—Number of seconds for which the IP address is valid, at which point the CPE device must make another DHCP request.

The DHCP server on the Cisco CMTS can also provide a number of options beyond the minimum that are required for network operation. A basic configuration is suitable for small installations as well as lab and experimental networks.

You can also configure the CMTS in a more complex configuration that uses the functionality of DHCP pools. DHCP pools are configured in a hierarchical fashion, according to their network numbers. A DHCP pool with a network number that is a subset of another pool's network number inherits all of the characteristics of the larger pool.

DHCP Security Options

Because the DOCSIS specification requires cable modems to obtain their IP addresses from a DHCP server, cable networks are susceptible to certain types of configuration errors and theft-of-service attacks, including:

- Duplicate IP addresses being assigned to two or more cable modems or CPE devices
- Duplicate MAC addresses being reported by two or more cable modems or CPE devices
- Unauthorized use of a DHCP-assigned IP address as a permanent static address
- One user hijacking a valid IP address from another user and using it on a different network device
- Configuring IP addresses with network addresses that are not authorized for a cable segment
- Unauthorized ARP requests on behalf of a cable segment, typically as part of a theft-of-service attack

To help combat these attacks, the Cisco CMTS dynamically maintains a database that links the MAC and IP addresses of known CPE devices with the cable modems that are providing network access for those CPE devices. The CMTS builds this database using information from both internal and external DHCP servers:

- When using the internal DHCP server, the CMTS automatically populates the database from the DHCP requests and replies that are processed by the server.
- When using an external server, the CMTS populates the database by inspecting all broadcast DHCP transactions that are sent over a cable interface between the cable modems and CPE devices on that interface and the DHCP servers.



Note

The Cisco CMTS also monitors IP traffic coming from CPE devices to associate their IP and MAC addresses with the cable modem that is providing their Internet connection.

The CMTS can also use the DHCP Relay Agent Information option (DHCP option 82) to send particular information about a cable modem, such as its MAC address and the cable interface it is connected to. If the DHCP server cannot match the information with that belonging to a cable modem in its database, the CMTS knows that the device is a CPE device. This allows the CMTS and DHCP server to retain accurate information about which CPE devices are using which cable modems and whether the devices should be allowed network access.

Multiple DHCP Pools

You can also configure any number of DHCP pools for the DHCP server to use in assigning IP addresses. A single pool can be used for a basic configuration, or you can optionally create separate pools for cable modems and CPE devices. You can also use DHCP address pools to provide special services, such as static IP addresses, to customers who are paying for those service.

When creating multiple DHCP pools, you can configure them independently, or you can optionally create a hierarchical structure of pools that are organized according to their network numbers. A DHCP pool that has a network number that is a subset of another pool's network number inherits all of the characteristics of the larger pool. In addition to the inherited characteristics, you can further customize each pool with any number of options.

The advantage of DHCP pools is that you can create a number of different DHCP configurations for particular customers or applications, without having to repeat CLI commands for the parameters that the pools have in common. You can also change the configuration of one pool without affecting customers in other pools.

External DHCP Servers

The Cisco CMTS router provides the following optional configurations that can enhance the operation and security of external DHCP servers that you are using on the DOCSIS cable network:

- [Cable Source Verify Feature, page 32](#)
- [Smart Relay Feature, page 33](#)
- [Giaddr Field, page 33](#)

Cable Source Verify Feature

To combat theft-of-service attacks, you can enable the **cable source-verify** command on the cable interfaces on the Cisco CMTS router. This feature uses the router's internal database to verify the validity of the IP packets that the CMTS receives on the cable interfaces, and provides three levels of protection:

- At the most basic level of protection, the Cable Source Verify feature examines every IP upstream packet to prevent duplicate IP addresses from appearing on the cable network. If a conflict occurs, the CMTS recognizes only packets coming from the device that was assigned the IP address by the DHCP server. The devices with the duplicate addresses are not allowed network address. The CMTS also refuses to recognize traffic from devices with IP addresses that have network addresses that are unauthorized for that particular cable segment.
- Adding the **dhcp** option to the **cable source-verify** command provides a more comprehensive level of protection by preventing users from statically assigning currently-unused IP addresses to their devices. When the Cisco CMTS receives a packet with an unknown IP address on a cable interface, the CMTS drops the packet but also issues a DHCP LEASEQUERY message that asks the DHCP servers for any information about that device's IP and MAC addresses. If the DHCP servers do not return any information about the device, the CMTS continues to block network access for the device.
- When you use the **dhcp** option, you can also enable the **leasetimer** option, which instructs the CMTS to periodically check its internal CPE database for IP addresses whose lease times have expired. CPE devices that are using expired IP addresses are denied further access to the network until they renew their IP addresses from a valid DHCP server. This can prevent users from taking DHCP-assigned IP addresses and assigning them as static addresses to their CPE devices.

Smart Relay Feature

The Cisco CMTS supports a Smart Relay feature (the **ip dhcp smart-relay** command), which automatically switches a cable modem or CPE device to secondary DHCP servers or address pools if the primary server runs out of IP addresses or otherwise fails to respond with an IP address. The relay agent attempts to forward DHCP requests to the primary server three times. After three attempts with no successful response from the primary, the relay agent automatically switches to the secondary server.

When you are using the **cable dhcp-giaddr policy** command to specify that CPE devices should use secondary DHCP pools corresponding to the secondary addresses on a cable interface, the smart relay agent automatically rotates through the available secondary in a round robin fashion until an available pool of addresses is found. This ensures that clients are not locked out of the network because a particular pool has been exhausted.

Giaddr Field

When using separate IP address pools for cable modems and CPE devices, you can use the **cable dhcp-giaddr policy** command to specify that cable modems should use address from the primary pool and that CPE devices should use addresses from the secondary pool. The default is for the CMTS to send all DHCP requests to the primary DHCP server, and the secondary servers are used only if the primary server does not respond.

Time-of-Day Server

The Cisco CMTS can function as a ToD server that provides the current date and time to the cable modems and other customer premises equipment (CPE) devices connected to its cable interfaces. This allows the cable modems and CPE devices to accurately timestamp their Simple Network Management Protocol (SNMP) messages and error log entries, as well as ensure that all of the system clocks on the cable network are synchronized to the same system time.



Tip

The initial ToD server on the Cisco CMTS did not work with some cable modems that used an incompatible packet format. This problem was resolved in Cisco IOS Release 12.1(8)EC1 and later 12.1 EC releases, and in Cisco IOS Release 12.2(4)BC1 and later 12.2 BC releases.

The current DOCSIS 1.0 and 1.1 specifications require that all DOCSIS cable modems request the following time-related fields in the DHCP request they send during their initial power-on provisioning:

- Time Offset (option 2)—Specifies the time zone for the cable modem or CPE device, in the form of the number of seconds that the device's timestamp is offset from Greenwich Mean Time (GMT).
- Time Server Option (option 4)—Specifies one or more IP addresses for a ToD server.

After a cable modem successfully acquires a DHCP lease time, it then attempts to contact one of the ToD servers provided in the list provided by the DHCP server. If successful, the cable modem updates its system clock with the time offset and timestamp received from the ToD server.

If a ToD server cannot be reached or if it does not respond, the cable modem eventually times out, logs the failure with the CMTS, and continues on with the initialization process. The cable modem can come online without receiving a reply from a ToD server, but it must periodically continue to reach the ToD server at least once in every five-minute period until it successfully receives a ToD reply. Until it reaches a ToD server, the cable modem must initialize its system clock to midnight on January 1, 1970 GMT.

**Note**

Initial versions of the DOCSIS 1.0 specification specified that the cable device must obtain a valid response from a ToD server before continuing with the initialization process. This requirement was removed in the released DOCSIS 1.0 specification and in the DOCSIS 1.1 specifications. Cable devices running older firmware that is compliant with the initial DOCSIS 1.0 specification, however, might require receiving a reply from a ToD server before being able to come online.

Because cable modems will repeatedly retry connecting with a ToD server until they receive a successful reply, you should consider activating the ToD server on the Cisco CMTS, even if you have one or more other ToD servers at the headend. This ensures that an online cable modem will always be able to connect with the ToD server on the Cisco CMTS, even if the other servers go down or are unreachable because of network congestion, and therefore will not send repeated ToD requests.

**Tip**

To be able to use the Cisco CMTS as the ToD server, either alone or with other, external servers, you must configure the DHCP server to provide the IP address Cisco CMTS as one of the valid ToD servers (DHCP option 4) for cable modems. See [“Creating and Configuring a DHCP Address Pool for Cable Modems” section on page 37](#) for details on this configuration.

In addition, although the DOCSIS specifications do not require that a cable modem successfully obtain a response from a ToD server before coming online, not obtaining a timestamp could prevent the cable modem from coming online in the following situations:

- If DOCSIS configuration files are being timestamped, to prevent cable modems from caching the files and replaying them, the clocks on the cable modem and CMTS must be synchronized. Otherwise, the cable modem cannot determine whether a DOCSIS configuration file has the proper timestamp.
- If cable modems register using Baseline Privacy Interface Plus (BPI+) authentication and encryption, the clocks on the cable modem and CMTS must be synchronized. This is because BPI+ authorization requires that the CMTS and cable modem verify the timestamps on the digital certificates being used for authentication. If the timestamps on the CMTS and cable modem are not synchronized, the cable modem cannot come online using BPI+ encryption.

**Note**

DOCSIS cable modems must use [RFC 868](#)-compliant ToD server to obtain the current system time. They cannot use the Network Time Protocol (NTP) or Simple Network Time Protocol (SNTP) service for this purpose. However, the Cisco CMTS can use an NTP or SNTP server to set its own system clock, which can then be used by the ToD server. Otherwise, you must manually set the clock on the CMTS using the **clock set** command each time that the CMTS boots up.

**Tip**

Additional servers can be provided by workstations or PCs installed at the cable headend. UNIX and Solaris systems typically include a ToD server as part of the operating system, which can be enabled by putting the appropriate line in the `inetd.conf` file. Windows systems can use shareware servers such as Greyware and Tardis. The DOCSIS specifications require that the ToD servers use the User Datagram Protocol (UDP) protocol instead of the TCP protocol for its packets.

TFTP Server

All Cisco CMTS platforms can be configured to provide a TFTP server that can provide the following types of files to DOCSIS cable modems:

- **DOCSIS Configuration File**—After a DOCSIS cable modem has acquired a DHCP lease and attempted to contact a ToD server, the cable modem uses TFTP to download a DOCSIS configuration file from an authorized TFTP server. The DHCP server is responsible for providing the name of the DOCSIS configuration file and IP address of the TFTP server to the cable modem.
- **Software Upgrade File**—If the DOCSIS configuration file specifies that the cable modem must be running a specific version of software, and the cable modem is not already running that software, the cable modem must download that software file. For security, the cable operator can use different TFTP servers for downloading DOCSIS configuration files and for downloading new software files.
- **Cisco IOS Configuration File**—The DOCSIS configuration file for Cisco cable devices can also specify that the cable modem should download a Cisco IOS configuration file that contains command-line interface (CLI) configuration commands. Typically this is done to configure platform-specific features such as voice ports or IPsec encryption.

**Note**

Do not confuse the DOCSIS configuration file with the Cisco IOS configuration file. The DOCSIS configuration file is a binary file in the particular format that is specified by the DOCSIS specifications, and each DOCSIS cable modem must download a valid file before coming online. In contrast, the Cisco IOS configuration file is an ASCII text file that contains one or more Cisco IOS CLI configuration commands. Only Cisco cable devices can download a Cisco IOS file.

All Cisco CMTS platforms can be configured as TFTP servers that can upload these files to the cable modem. The files can reside on any valid device but typically should be copied to the Flash memory device inserted into the Flash disk slot on the Cisco CMTS.

In addition, the Cisco CMTS platform supports an internal DOCSIS configuration file editor in Cisco IOS Release 12.1(2)EC, Cisco IOS Release 12.2(4)BC1, and later releases. When you create a DOCSIS configuration file using the internal configuration file editor, the CMTS stores the configuration file in the form of CLI commands. When a cable modem requests the DOCSIS configuration file, the CMTS then dynamically creates the binary version of the file and uploads it to the cable modem.

**Note**

The internal DOCSIS configuration file editor supports only DOCSIS 1.0 configuration files. For more information, see the “*Internal DOCSIS Configurator File Generator for the Cisco CMTS*” document at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/cable/cab_rout/cmtsfg/ufgcfile.htm

To create DOCSIS 1.1 configuration files, you must use a separate configuration editor, such as the Cisco DOCSIS Configurator tool, which at the time of this document’s publication is available on Cisco.com at the following URL:

<http://www.cisco.com/cgi-bin/tablebuild.pl/cpe-conf>

For enhanced security, current versions of Cisco IOS software for Cisco CMTS platforms include a “TFTP Enforce” feature (**cable tftp-enforce** command) that allows you to require that all cable modems must attempt a TFTP download through the cable interface before being allowed to come online. This prevents a common theft-of-service attack in which hackers reconfigure their local network so that a

local TFTP server downloads an unauthorized DOCSIS configuration file to the cable modem. This ensures that cable modems download only a DOCSIS configuration file that provides the services they are authorized to use.

Benefits

- The “all-in-one” configuration allows you to set up a basic cable modem network without having to invest in additional servers and software. This configuration can also help troubleshoot plant and cable modem problems.
- The DHCP configuration can more effectively assigns and manages IP addresses from specified address pools within the CMTS to the cable modems and their CPE devices.
- The Cisco CMTS can act as a primary or backup ToD server to ensure that all cable modems are synchronized with the proper date and time before coming online. This also enables cable modems to come online more quickly because they will not have to wait for the ToD timeout period before coming online.
- The ToD server on the Cisco CMTS ensures that all devices connected to the cable network are using the same system clock, making it easier for you to troubleshoot system problems when you analyze the debugging output and error logs generated by many cable modems, CPE devices, the Cisco CMTS, and other services.
- The Cisco CMTS can act as a TFTP server for DOCSIS configuration files, software upgrade files, and Cisco IOS configuration files.
- You do not need a separate workstation or PC to create and store DOCSIS configuration files.
- The “TFTP Enforce” feature ensures that users download only an authorized DOCSIS configuration file and prevents one of the most common theft-of-service attacks.

How to Configure DHCP, ToD, and TFTP Services

See the following configuration tasks required to configure DHCP service, time-of-day service, and TFTP service on a Cisco CMTS:

- [Configuring DHCP Service, page 37](#)
- [Configuring Time-of-Day Service, page 43](#)
- [Configuring TFTP Service, page 45](#)
- [Configuring A Basic All-in-One Configuration \(optional\), page 48](#)
- [Configuring an Advanced All-in-One Configuration \(optional\), page 49](#)
- [Optimizing the Use of an External DHCP Server, page 49](#)

All procedures are required unless marked as optional (depending on the desired network configuration and applications).

Configuring DHCP Service

To configure the DHCP server on the Cisco CMTS, use the following procedures to create the required address pools for the server to use. You can create one pool for all DHCP requests (cable modems and CPE devices), or separate pools for cable modems and for CPE devices, as desired.

- [Creating and Configuring a DHCP Address Pool for Cable Modems, page 37](#)
- [Creating and Configuring a DHCP Address Pool for CPE Devices \(optional\), page 41](#)

Creating and Configuring a DHCP Address Pool for Cable Modems

To use the DHCP server on the Cisco CMTS, you must create at least one address pool that defines the IP addresses and other network parameters that are given to cable modems that make DHCP requests. To create an address pool, use the following procedure, beginning in EXEC mode. Repeat this procedure as needed to create additional address pools.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip dhcp pool** *name*
4. **network** *network-number* [*mask*]
5. **bootfile** *filename*
6. **next-server** *address* [*address2...address8*]
7. **default-router** *address* [*address2...address8*]
8. **option 2 hex** *gmt-offset*
9. **option 4 ip** *address* [*address2...address8*]
10. **option 7 ip** *address* [*address2...address8*]
11. **lease** {*days* [*hours*][*minutes*] | **infinite**}
12. **client-identifier** *unique-identifier*

13. **exit**14. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable Router#	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal Router(config)#	Enters global configuration mode.
Step 3	ip dhcp pool name Example: Router(config)# ip dhcp pool local Router(dhcp-config)#	Creates a DHCP address pool and enters DHCP pool configuration file mode. The <i>name</i> can be either an arbitrary string, such as service , or a number, such as 1 .
Step 4	network network-number [mask] Example: Router(dhcp-config)# network 10.10.10.0 255.255.0.0 Router(dhcp-config)#	Configures the address pool with the specified <i>network-number</i> and subnet <i>mask</i> , which are the DHCP <i>yiaddr</i> field and Subnet Mask (DHCP option 1) field. If you do not specify the <i>mask</i> value, it defaults to 255.255.255.255. Note To create an address pool with a single IP address, use the host command instead of network .
Step 5	bootfile filename Example: Router(dhcp-config)# bootfile platinum.cm Router(dhcp-config)#	Specifies the name of the default DOCSIS configuration file (the DHCP <i>file</i> field) for the cable modems that are assigned IP addresses from this pool. The <i>filename</i> should be the exact name (including path) that is used to request the file from the TFTP server.
Step 6	next-server address [address2...address8] Example: Router(dhcp-config)# next-server 10.10.11.1 Router(dhcp-config)#	Specifies the IP address (the DHCP <i>siaddr</i> field) for the next server in the boot process of a DHCP client. For DOCSIS cable modems, this is the IP address for the TFTP server that provides the DOCSIS configuration file. You must specify at least one IP address, and can optionally specify up to eight IP addresses, in order of preference.

	Command or Action	Purpose
Step 7	default-router <i>address</i> [<i>address2</i> ... <i>address8</i>] Example: Router(dhcp-config)# default-router 10.10.10.12 Router(dhcp-config)#	Specifies the IP address for the Router Option (DHCP option 3) field, which is the default router for the cable modems in this address pool. You must specify at least one IP address, and can optionally specify up to eight IP addresses, where the default routers are listed in their order of preference (<i>address</i> is the most preferred server, <i>address2</i> is the next most preferred, and so on). Note The first IP address must be the IP address for the cable interface that is connected to cable modems using this DHCP pool.
Step 8	option 2 hex <i>gmt-offset</i> Example: Router(dhcp-config)# option 2 hex FFFF.8F80 Router(dhcp-config)#	Specifies the Time Offset field (DHCP option 2), which is the local time zone, specified as the number of seconds, in hexadecimal, offset from Greenwich Mean Time (GMT). The following are some sample values for <i>gmt-offset</i>: FFFF.8F80 = Offset of –8 hours (–28800 seconds, Pacific Time) FFFF.9D90 = Offset of –7 hours (Mountain Time) FFFF.ABA0 = Offset of –6 hours (Central Time) FFFF.B9B0 = Offset of –5 hours (Eastern Time)
Step 9	option 4 ip <i>address</i> [<i>address2</i> ... <i>address8</i>] Example: Router(dhcp-config)# option 4 ip 10.10.10.13 10.10.11.2 Router(dhcp-config)#	Specifies the Time Server Option field (DHCP option 4), which is the IP address of the time-of-day (ToD) server from which the cable modem can obtain its current date and time. You must specify at least one IP address, and can optionally specify up to eight IP addresses, listed in their order of preference. Note If you want to use the Cisco CMTS as the ToD server, you must enter its IP address as part of this command.
Step 10	option 7 ip <i>address</i> [<i>address2</i> ... <i>address8</i>] Example: Router(dhcp-config)# option 7 ip 10.10.10.13 Router(dhcp-config)#	(Optional) Specifies the Log Server Option field (DHCP option 7), which is the IP address for a System Log (SYSLOG) server that the cable modem should send error messages and other logging information. You can optionally specify up to eight IP addresses, listed in their order of preference.

	Command or Action	Purpose
Step 11	lease {<i>days</i> [<i>hours</i>] [<i>minutes</i>] infinite} Example: Router(dhcp-config)# lease 0 12 30 Router(dhcp-config)#	Specifies the IP Address Lease Time (option 51), which is the duration of the lease for the IP address that is assigned to the cable modem. Before the lease expires, the cable modem must make another DHCP request to remain online. The default is one day. You can specify the lease time as follows: • <i>days</i> = Duration of the lease in numbers of days (0 to 365). • <i>hours</i> = Number of hours in the lease (0 to 23, optional). A <i>days</i> value must be supplied before you can configure an <i>hours</i> value. • <i>minutes</i> = Number of minutes in the lease (0 to 59, optional). A <i>days</i> value and an <i>hours</i> value must be supplied before you can configure a <i>minutes</i> value. • infinite = Unlimited lease duration. Note In most cable networks, cable modems cannot come online if the lease time is less than 3 minutes. For stability in most cable networks, the minimum lease time should be 5 minutes.
Step 12	client-identifier <i>unique-identifier</i> Example: Router(dhcp-config)# client-identifier 0100.0C01.0203.04 Router(dhcp-config)#	(Optional) Specifies the MAC address that identifies the particular cable modem that should receive the parameters from this pool. The unique-identifier is created by combining the one-byte Ethernet identifier ("01") with the six-byte MAC address for the cable modem. For example, to specify a cable modem with the MAC address of 9988.7766.5544, specify a <i>unique-identifier</i> of 0199.8877.6655.44. Note This option should be used only for DHCP pools that assign a static address to a single cable modem.
Step 13	exit Example: Router(dhcp-config)# exit Router(config)#	Exits DHCP configuration mode.
Step 14	exit Example: Router(config)# exit Router#	Exits global configuration mode.

Creating and Configuring a DHCP Address Pool for CPE Devices (optional)

In addition to providing IP addresses for cable modems, the DHCP server on the Cisco CMTS server can optionally provide IP addresses and other network parameters to the customer premises equipment (CPE) devices that are connected to the cable modems on the network. To do so, create a DHCP address pool for those CPE devices, using the following procedure, beginning in EXEC mode. Repeat this procedure as needed to create additional address pools.



Note

You can use the same address pools for cable modems and CPE devices, but it simplifies network management to maintain separate pools.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip dhcp pool** *name*
4. **network** *network-number* [*mask*]
5. **default-router** *address* [*address2...address8*]
6. **dns-server** *address* [*address2...address8*]
7. **domain-name** *domain*
8. **lease** {*days* [*hours*][*minutes*] | **infinite**}
9. **client-identifier** *unique-identifier*
10. **exit**
11. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable Router#	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal Router(config)#	Enters global configuration mode.
Step 3	ip dhcp pool <i>name</i> Example: Router(config)# ip dhcp pool local Router(dhcp-config)#	Creates a DHCP address pool and enters DHCP pool configuration file mode. The <i>name</i> can be either an arbitrary string, such as service , or a number, such as 1 .

	Command or Action	Purpose
Step 4	network <i>network-number</i> [<i>mask</i>] Example: Router(dhcp-config)# network 10.10.10.0 255.255.0.0 Router(dhcp-config)#	Configures the address pool with the specified <i>network-number</i> and subnet <i>mask</i> , which are the DHCP <i>yiaddr</i> field and Subnet Mask (DHCP option 1) field. If you do not specify the <i>mask</i> value, it defaults to 255.255.255.255. Note To create an address pool with a single IP address, use the host command instead of network .
Step 5	default-router <i>address</i> [<i>address2...address8</i>] Example: Router(dhcp-config)# default-router 10.10.10.12 Router(dhcp-config)#	Specifies the IP address for the Router Option (DHCP option 3) field, which is the default router for the cable modems and CPE devices in this address pool. You must specify at least one IP address, and can optionally specify up to eight IP addresses, where the default routers are listed in order of preference (<i>address</i> is the most preferred server, <i>address2</i> is the next most preferred, and so on).
Step 6	dns-server <i>address</i> [<i>address2...address8</i>] Example: Router(dhcp-config)# dns-server 10.10.10.13 Router(dhcp-config)#	Specifies one or more IP address for the Domain Name Server Option (DHCP option 6) field, which are the domain name system (DNS) servers that will resolve hostnames to IP addresses for the CPE devices. You must specify at least one IP address, and can optionally specify up to eight IP addresses, listed in order of preference.
Step 7	domain-name <i>domain</i> Example: Router(dhcp-config)# domain-name cisco.com Router(dhcp-config)#	Specifies the Domain Name (DHCP option 15) field, which is the fully-qualified domain name that the CPE devices should add to their hostnames. The <i>domain</i> parameter should be the domain name used by devices on the cable network.
Step 8	lease { <i>days</i> [<i>hours</i>] [<i>minutes</i>] infinite } Example: Router(dhcp-config)# lease 0 12 30 Router(dhcp-config)#	Specifies the IP Address Lease Time (option 51), which is the duration of the lease for the IP address that is assigned to the CPE device. Before the lease expires, the CPE device must make another DHCP request to remain online. The default is one day. You can specify the lease time as follows: <i>days</i> = Duration of the lease in numbers of days (0 to 365). <i>hours</i> = Number of hours in the lease (0 to 23, optional). A <i>days</i> value must be supplied before you can configure an <i>hours</i> value. <i>minutes</i> = Number of minutes in the lease (0 to 59, optional). A <i>days</i> value and an <i>hours</i> value must be supplied before you can configure a <i>minutes</i> value. infinite = Unlimited lease duration.

	Command or Action	Purpose
Step 9	client-identifier <i>unique-identifier</i> Example: Router(dhcp-config)# client-identifier 0100.0C01.0203.04 Router(dhcp-config)#	(Optional) Specifies the MAC address that identifies a particular CPE device that should receive the parameters from this pool. The unique-identifier is created by combining the one-byte Ethernet identifier (“01”) with the six-byte MAC address for the device. For example, so specify a device with the MAC address of 9988.7766.5544, specify a unique-identifier of 0199.8877.6655.44. Note This option should be used only for DHCP pools that assign a static address to a single CPE device.
Step 10	exit Example: Router(dhcp-config)# exit Router(config)#	Exits DHCP configuration mode.
Step 11	exit Example: Router(config)# exit Router#	Exits global configuration mode.

Configuring Time-of-Day Service

This section provides procedures for enabling and disabling the time-of-day (ToD) server on the Cisco CMTS routers.

Prerequisites

- To be able to use the Cisco CMTS as the ToD server, either alone or with other, external servers, you must configure the DHCP server to provide the IP address Cisco CMTS as one of the valid ToD servers (DHCP option 4) for cable modems. See [“Creating and Configuring a DHCP Address Pool for Cable Modems” section on page 37](#) for details on this configuration when using the internal DHCP server.

Enabling Time-of-Day Service

To enable the ToD server on a Cisco CMTS, use the following procedure, beginning in EXEC mode.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **service udp-small-servers max-servers no-limit**
4. **cable time-server**
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable Router#	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal Router(config)#	Enters global configuration mode.
Step 3	service udp-small-servers max-servers no-limit Example: Router(config)# service udp-small-servers max-servers no-limit Router(config)#	Enables use of minor servers that use the UDP protocol (such as ToD, echo, chargen, and discard). The max-servers no-limit option allows a large number of cable modems to obtain the ToD server at one time, in the event that a cable or power failure forces many cable modems offline. When the problem has been resolved, the cable modems can quickly reconnect.
Step 4	cable time-server Example: Router(config)# cable time-server Router(config)#	Enables the ToD server on the Cisco CMTS.
Step 5	exit Example: Router(config)# exit Router#	Exits global configuration mode.

Disabling Time-of-Day Service

To disable the ToD server, use the following procedure, beginning in EXEC mode.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **no cable time-server**
4. **no service udp-small-servers**
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable Router#	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal Router(config)#	Enters global configuration mode.
Step 3	no cable time-server Example: Router(config)# cable time-server Router(config)#	Disables the ToD server on the Cisco CMTS.
Step 4	no service udp-small-servers Example: Router(config)# no service udp-small-servers Router(config)#	(Optional) Disables the use of all minor UDP servers. Note Do not disable the minor UDP servers if you are also enabling the other DHCP or TFTP servers.
Step 5	exit Example: Router(config)# exit Router#	Exits global configuration mode.

Configuring TFTP Service

To configure TFTP service on a Cisco CMTS where the CMTS can act as a TFTP server and download a DOCSIS configuration file to cable modems, perform the following steps:

- Create the DOCSIS configuration files using the DOCSIS configuration editor of your choice. You can also use the internal DOCSIS configuration file editor on the Cisco CMTS to create DOCSIS configuration files.
- Copy all desired files (DOCSIS configuration files, software upgrade files, and Cisco IOS configuration files) to the Flash memory device on the Cisco CMTS. Typically, this is done by placing the files first on an external TFTP server, and then using TFTP commands to transfer them to the router's Flash memory.



Note If you are using the internal DOCSIS configuration editor on the Cisco CMTS to create the DOCSIS configuration files, you do not need to copy the files to a Flash memory device because they are already part of the router's configuration.

- Enable the TFTP server on the Cisco CMTS with the **tftp-server** command.

- Optionally enable the TFTP enforce feature so that cable modems must attempt a TFTP download of the DOCSIS configuration file through the cable interface with the CMTS before being allowed to come online.

Each configuration task is required unless otherwise listed as optional.

Step 1 Use the **show file systems** command to display the Flash memory cards that are available on your CMTS, along with the free space on each card and the appropriate device names to use to access each card.

Most configurations of the Cisco CMTS platforms support both linear Flash and Flash disk memory cards. Linear Flash memory is accessed using the **slot0** (or **flash**) and **slot1** device names. Flash disk memory is accessed using the **disk0** and **disk1** device names.

For example, the following command shows a Cisco uBR7200 series router that has two linear Flash memory cards installed. The cards can be accessed by the **slot0** (or **flash**) and **slot1** device names.

```
Router# show file systems
```

```
File Systems:
```

	Size(b)	Free(b)	Type	Flags	Prefixes
	48755200	48747008	flash	rw	slot0: flash:
	16384000	14284000	flash	rw	slot1:
	32768000	31232884	flash	rw	bootflash:
*	-	-	disk	rw	disk0:
	-	-	disk	rw	disk1:
	-	-	opaque	rw	system:
	-	-	opaque	rw	null:
	-	-	network	rw	tftp:
	522232	507263	nvrn	rw	nvrn:
	-	-	network	rw	rcp:
	-	-	network	rw	ftp:
	-	-	network	rw	scp:

```
Router#
```

The following example shows a Cisco uBR10012 router that has two Flash disk cards installed. These cards can be accessed by the **disk0** and **sec-disk0** device names.

```
Router# show file systems
```

```
File Systems:
```

	Size(b)	Free(b)	Type	Flags	Prefixes
	-	-	flash	rw	slot0: flash:
	-	-	flash	rw	slot1:
	32768000	29630876	flash	rw	bootflash:
*	128094208	95346688	disk	rw	disk0:
	-	-	disk	rw	disk1:
	-	-	opaque	rw	system:
	-	-	flash	rw	sec-slot0:
	-	-	flash	rw	sec-slot1:
*	128094208	95346688	disk	rw	sec-disk0:
	-	-	disk	rw	sec-disk1:
	32768000	29630876	flash	rw	sec-bootflash:
	-	-	nvrn	rw	sec-nvrn:
	-	-	opaque	rw	null:
	-	-	network	rw	tftp:
	522232	505523	nvrn	rw	nvrn:
	-	-	network	rw	rcp:
	-	-	network	rw	ftp:
	-	-	network	rw	scp:

**Tip**

Router#

The Cisco uBR10012 router supports redundant processors, a primary and a secondary, and each processor contains its own Flash memory devices. You typically do not have to copy files to the secondary Flash memory devices (which have the **sec** prefix) because the Cisco uBR10012 router synchronizes the secondary processor to the primary one.

- Step 2** Verify that the desired Flash memory card has sufficient free space for all of the files that you want to copy to the CMTS.
- Step 3** Use the **ping** command to verify that the remote TFTP server that contains the desired files is reachable. For example, the following shows a **ping** command being given to an external TFTP server with the IP address of 10.10.10.1:

Router# **ping 10.10.10.1**

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.10.10.1, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 5/6/6 ms

- Step 4** Use the **copy tftp devname** command to copy each file from the external TFTP server to the appropriate Flash memory card on the CMTS, where *devname* is the device name for the destination Flash memory card. You will then be prompted for the IP address for the external TFTP server and the filename for the file to be transferred.

The following example shows the file `docsis.cm` being transferred from the external TFTP server at IP address 10.10.10.1 to the first Flash memory disk (disk0):

Router# **copy tftp disk0**Address or name of remote host []? **10.10.10.1**Source filename []? **config-files/docsis.cm**

Destination filename [docsis.cm]?

Accessing tftp://10.10.10.1/config-file/docsis.cm.....

Loading docsis.cm from 10.10.10.1 (via Ethernet2/0): !!!

[OK - 276/4096 bytes]

276 bytes copied in 0.152 secs

Router#

- Step 5** Repeat [Step 4](#) as needed to copy all of the files from the external TFTP server to the Flash memory card on the Cisco CMTS.

- Step 6** Use the **dir** command to verify that the Flash memory card contains all of the transferred files.

Router# **dir disk0:**

Directory of disk0:/

```

 1  -rw-      10705784   May 30 2002 19:12:46  ubr10k-p6-mz.122-2.8.BC
 2  -rw-         4772   Jun 20 2002 18:12:56  running.cfg.save
 3  -rw-         241    Jul 31 2002 18:25:46  gold.cm
 4  -rw-         225    Jul 31 2002 18:25:46  silver.cm
 5  -rw-         231    Jul 31 2002 18:25:46  bronze.cm
 6  -rw-          74    Oct 11 2002 21:41:14  disable.cm
 7  -rw-      2934028   May 30 2002 11:22:12  ubr924-k8y5-mz.bin
 8  -rw-      3255196   Jun 28 2002 13:53:14  ubr925-k9v9y5-mz.bin

```

128094208 bytes total (114346688 bytes free)

Router#

- Step 7** Use the **configure terminal** command to enter global configuration mode:

```
Router# configure terminal
Router(config)#
```

- Step 8** Use the **tftp-server** command to specify which particular files can be transferred by the TFTP server that is onboard the Cisco CMTS. You can also use the **alias** option to specify a different filename that the DHCP server can use to refer to the file. For example, the following commands enable the TFTP transfer of the configuration files and software upgrade files shown in [Step 6](#):

```
Router(config)# tftp-server disk0:gold.cm alias gold.cm
Router(config)# tftp-server disk0:silver.cm alias silver.cm
Router(config)# tftp-server disk0:bronze.cm alias bronze.cm
Router(config)# tftp-server disk0:ubr924-k8y5-mz.bin alias ubr924-codefile
Router(config)# tftp-server disk0:ubr925-k9v9y5-mz.bin alias ubr925-codefile
Router(config)#
```



Note The **tftp-server** command also supports the option of specifying an access list that restricts access to the particular file to the IP addresses that match the access list.

- Step 9** (Optional) Use the following command to enable the use of the UDP small servers, and to allow an unlimited number of connections at one time. This will allow a large number of cable modems that have gone offline due to cable or power failure to rapidly come back online.

```
Router(config)# service udp-small-servers max-servers no-limit
Router(config)#
```

- Step 10** (Optional) Use the **cable tftp-enforce** command in interface configuration mode to require that each cable modem perform a TFTP download of its DOCSIS configuration file through its cable interface with the CMTS before being allowed to come online. This can prevent the most common types of theft-of-service attacks in which users configure their local networks so as to download an unauthorized configuration file to their cable modems.

```
Router(config)# interface cable x/y
Router(config-if)# cable tftp-enforce
Router(config-if)#
```

You can also specify the **mark-only** option so that cable modems can come online without attempting a TFTP download, but the cable modems are marked in the **show cable modems** command so that network administrators can investigate the situation further before taking any action.

```
Router(config)# interface cable x/y
Router(config-if)# cable tftp-enforce mark-only
Router(config-if)#
```

Configuring A Basic All-in-One Configuration (optional)

The basic all-in-one configuration requires configuring the DHCP, ToD, and TFTP servers, as described in the following sections in this document:

- [Configuring DHCP Service, page 37](#)
- [Configuring Time-of-Day Service, page 43](#)
- [Configuring TFTP Service, page 45](#)

You must also have the necessary DOCSIS configuration files available for the TFTP server. You can do this in two ways:

- Create the DOCSIS configuration files using the Cisco DOCSIS Configurator tool, and then copy them to the Flash memory device. For instructions on copying the configuration files to Flash memory, see the [“Configuring TFTP Service” section on page 45](#).
- Dynamically create the DOCSIS configuration files with the **cable config-file** command. For information on this, see the chapter [“Internal DOCSIS Configurator File Generator for the Cisco CMTS”](#) in the [Cisco CMTS Feature Guide](#).

For an example of a basic all-in-one configuration, see the [“Basic All-in-One Configuration Example” section on page 58](#).

Configuring an Advanced All-in-One Configuration (optional)

The advanced all-in-one configuration sample is identical to the basic configuration except that it uses a hierarchy of DHCP pools. Any DHCP pool with a network number that is a subset of another pool's network number inherits all the characteristics of that other pool. This saves having to repeat identical commands in the multiple DHCP pool configurations.

For information on the required tasks, see the following sections in this guide:

- [Configuring DHCP Service, page 37](#)
- [Configuring Time-of-Day Service, page 43](#)
- [Configuring TFTP Service, page 45](#)

You must also have the necessary DOCSIS configuration files available for the TFTP server. You can do this in two ways:

- Create the DOCSIS configuration files using the Cisco DOCSIS Configurator tool, and then copy them to the Flash memory device. For instructions on copying the configuration files to Flash memory, see the [“Configuring TFTP Service” section on page 45](#).
- Dynamically create the DOCSIS configuration files with the **cable config-file** command. For information on this, see the chapter [“Internal DOCSIS Configurator File Generator for the Cisco CMTS”](#) in the [Cisco CMTS Feature Guide](#). (This command creates only DOCSIS 1.0 configuration files.)

For an example of an advanced all-in-one configuration, see the [“Advanced All-in-One Configuration Example” section on page 62](#).

Optimizing the Use of an External DHCP Server

The Cisco CMTS offers a number of options that can optimize the operation of external DHCP servers on a DOCSIS cable network. See the following sections for details. All procedures are optional, depending on the needs of your network and application servers.

- [Configuring Cable Source Verify Option \(optional\), page 50](#)
- [Configuring Optional DHCP Parameters \(optional\), page 52](#)

Configuring Cable Source Verify Option (optional)

To enhance security when using external DHCP servers, you can optionally configure the Cable Source Verify feature with the following procedure, beginning in EXEC mode.

Restrictions

- The Cable Source Verify feature supports only external DHCP servers. It cannot be used with the internal DHCP server.

SUMMARY STEPS

- enable**
- configure terminal**
- interface cable *x/y***
- cable source-verify [dhcp | leasetimer *value*]**
- no cable arp**
- exit**
- ip dhcp relay information option**
- exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable Router#	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal Router(config)#	Enters global configuration mode.
Step 3	interface cable <i>x/y</i> Example: Router(config)# interface cable 4/0 Router(config-if)#	Enters cable interface configuration mode for the specified cable interface.

	Command or Action	Purpose
Step 4	Command: <code>cable source-verify [dhcp leasetimer value]</code> Example: <pre>Router(config-if)# cable source-verify dhcp Router(config-if)# cable source-verify leasetimer 30 Router(config-if)#</pre>	(Optional) Ensures that the CMTS allows network access only to those IP addresses that DHCP servers issued to devices on this cable interface. The CMTS examines DHCP packets that pass through the cable interfaces to build a database of which IP addresses are valid on which interface. • dhcp = (Optional) Drops traffic from all devices with unknown IP addresses, but the CMTS also sends a query to the DHCP servers for any information about the device. If a DHCP server informs the CMTS that the device has a valid IP address, the CMTS then allows the device on the network. • leasetimer value = (Optional) Specifies how often, in minutes, the router should check its internal CPE database for IP addresses whose lease times have expired. This can prevent users from taking DHCP-assigned IP addresses and assigning them as static addresses to their CPE devices. The valid range for value is 1 to 240 minutes, with no default. Note The leasetimer option takes effect only when the dhcp option is also used on an interface.
Step 5	Command: <code>no cable arp</code> Example: <pre>Router(config-if)# no cable arp Router(config-if)#</pre>	(Optional) Blocks Address Resolution Protocol (ARP) requests originating from devices on the cable network. Use this command, together with the cable source-verify dhcp command, to block certain types of theft-of-service attacks that attempt to hijack or spoof IP addresses.
	Note Repeat Step 3 through Step 5 for each desired cable interface.	
Step 6	Command: <code>exit</code> Example: <pre>Router(config-if)# exit Router(config)#</pre>	Exits interface configuration mode.
Step 7	Command: <code>ip dhcp relay information option</code> Example: <pre>Router(config)# ip dhcp relay information option Router(config)#</pre>	(Optional) Enables the CMTS to insert DHCP relay information (DHCP option 82) in relayed DHCP packets. This allows the DHCP server to store accurate information about which CPE devices are using which cable modems. You should use this command if you are also using the cable source-verify dhcp command. Note Cisco IOS releases before Release 12.1(2)EC1 used the cable relay-agent-option command for this purpose, but current releases should use the ip dhcp relay information option command.
Step 8	Command: <code>exit</code> Example: <pre>Router(config)# exit Router#</pre>	Exits global configuration mode.

Configuring Optional DHCP Parameters (optional)

When using an external DHCP server, the Cisco CMTS supports a number of options that can enhance operation of the cable network in certain applications. To configure these options, use the following procedure, beginning in EXEC mode.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip dhcp smart-relay**
4. **ip dhcp ping packet 0**
5. **ip dhcp relay information check**
6. **interface cable *x/y***
7. **cable helper-address *address* [cable-modem | host]**
8. **cable dhcp-giaddr policy**
9. **exit**
10. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable	Enables privileged EXEC mode. Enter your password if prompted.
	Example: Router> enable Router#	
Step 2	configure terminal	Enters global configuration mode.
	Example: Router# configure terminal Router(config)#	
Step 3	ip dhcp smart-relay	(Optional) Enables the DHCP relay agent on the CMTS to automatically switch a cable modem or CPE device to a secondary DHCP server or address pool if the primary DHCP server does not respond to three successive requests. If multiple secondary servers have been defined, the relay agent forwards DHCP requests to the secondary servers in a round robin fashion.
	Example: Router(config)# ip dhcp smart-relay Router(config)#	

	Command or Action	Purpose
Step 4	ip dhcp ping packet 0 Example: Router(config)# ip dhcp ping packet 0 Router(config)#	(Optional) Instructs the DHCP server to assign an IP address from its pool without first sending an ICMP ping to test whether a client is already currently using that IP address. Disabling the ping option can speed up address assignment when a large number of modems are trying to connect at the same time. However, disabling the ping option can also result in duplicate IP addresses being assigned if users assign unauthorized static IP addresses to their CPE devices. Note By default, the DHCP server pings a pool address twice before assigning a particular address to a requesting client. If the ping is unanswered, the DHCP server assumes that the address is not in use and assigns the address to the requesting client.
Step 5	ip dhcp relay information check Example: Router(config)# ip dhcp relay information check Router(config)#	(Optional) Configures the DHCP server to validate the relay agent information option in forwarded BOOTREPLY messages. Invalid messages are dropped. Note The ip dhcp relay information command contains several other options that might be useful for special handling of DHCP packets. See its command reference page in the Cisco IOS documentation for details.
Step 6	interface cable x/y Example: Router(config)# interface cable 4/0 Router(config-if)#	Enters cable interface configuration mode for the specified cable interface.
Step 7	cable dhcp-giaddr policy Example: Router(config-if)# cable dhcp-giaddr policy Router(config-if)#	Sets the DHCP <i>giaddr</i> field of DHCP request packets to the primary address for cable modems and the secondary address for CPE devices, allowing the use of separate address pools for the different clients. Note The cable dhcp-giaddr command also supports the primary option, but this typically is used only for EuroDOCSIS cable modems and set-top boxes.

	Command or Action	Purpose
Step 8	cable helper-address <i>address</i> [cable-modem host] Example: Router(config-if)# cable helper-address 10.10.10.13 Router(config-if)#	(Optional) Enables load-balancing of DHCP requests from cable modems and CPE devices by specifying different DHCP servers according to the cable interface or subinterface. You can also specify separate servers for cable modems and CPE devices. <i>address</i> = IP address of a DHCP server to which UDP broadcast packets will be sent via unicast packets. cable-modem = specifies this server should be used only for cable modems (optional). host = Specifies this server should be used only for CPE devices (optional). Note You must specify both the cable-modem and host options in separate commands if you decide to use them. If you specify only one option, then the other type of device (cable modem or host) will not be able to connect with a DHCP server. Tip Repeat this command to specify more than one helper address on each cable interface. You can specify more than 16 helper addresses, but the Cisco IOS software uses only the first 16 valid addresses.
	Note The ip helper-address command performs a similar function to cable helper-address, but it should be used only on non-cable interfaces. The cable helper-address command should be used on cable interfaces because it is optimized for the operation of DHCP requests on DOCSIS networks.	
	Note Repeat Step 6 through Step 8 for each desired cable interface.	
Step 9	exit Example: Router(config-if)# exit Router(config)#	Exits interface configuration mode.
Step 10	exit Example: Router(config)# exit Router#	Exits global configuration mode.

Configuration Examples

This section provides examples for the following configurations:

- [DHCP Server Examples, page 55](#)
- [ToD Server Example, page 57](#)
- [TFTP Server Example, page 57](#)
- [Basic All-in-One Configuration Example, page 58](#)
- [Advanced All-in-One Configuration Example, page 62](#)

DHCP Server Examples

The following sections gave sample configurations for configuring DHCP pools for cable modems and CPE devices:

- [DHCP Pools for Cable Modems, page 55](#)
- [DHCP Pools for Disabling Cable Modems, page 56](#)
- [DHCP Pools for CPE Devices, page 56](#)

DHCP Pools for Cable Modems

The following examples show three typical DHCP pools for cable modems. Each pool includes the following fields:

- The **dhcp pool** command defines a unique string for the pool's name, which in this case identifies the DOCSIS configuration file that is to be downloaded to the cable modem.
- The **network** command defines the range of IP addresses for each pool.
- The **bootfile** command specifies the DOCSIS configuration file to be downloaded to the cable modem. In these examples, three DOCSIS configuration files are specified (platinum.cm, gold.cm, and silver.cm).
- The **next-server** command specifies the IP address for the TFTP server.
- The **default-router** command specifies the default gateway.
- The three **option** commands specify the time offset, ToD server, and log server.
- The **lease** command specifies that the DHCP lease expires in is 7 days, 0 hours, and 10 minutes. (The cable modem will typically attempt to renew the lease at the halfway mark of approximately 3 days and 12 hours.)

```
!  
ip dhcp pool cm-platinum  
  network 10.128.4.0 255.255.255.0  
  bootfile platinum.cm  
  next-server 10.128.4.1  
  default-router 10.128.4.1  
  option 2 hex ffff.8f80  
  option 4 ip 10.1.4.1  
  option 7 ip 10.1.4.1  
  lease 7 0 10  
!  
ip dhcp pool cm-gold  
  network 10.129.4.0 255.255.255.0
```

```

bootfile gold.cm
next-server 10.129.4.1
default-router 10.129.4.1
option 2 hex ffff.8f80
option 4 ip 10.1.4.1
option 7 ip 10.1.4.1
lease 7 0 10
!
ip dhcp pool cm-silver
network 10.130.4.0 255.255.255.0
bootfile silver.cm
next-server 10.130.4.1
default-router 10.130.4.1
option 2 hex ffff.8f80
option 4 ip 10.1.4.1
option 7 ip 10.1.4.1
lease 7 0 10

```

DHCP Pools for Disabling Cable Modems

The following examples shows typical DHCP pool configurations for cable modems that disable network access for their attached CPE devices. With this configuration, the cable modem can come online and is able to communicate with the CMTS, but the CPE devices cannot access the cable network. Each pool includes the following fields:

- The DHCP pool name is a unique string that indicates the MAC address for each cable modem that should be disabled.
- The **host** option specifies a single static IP address.
- The **client-identifier** option identifies a particular cable modem to be denied access. The cable modem is identified by the combination of the Ethernet media code (“01”) plus the cable modem’s MAC address.
- The **bootfile** option specifies a DOCSIS configuration file (“disable.cm”) that disables network access.

```

!
ip dhcp pool DisabledModem(0010.aaaa.0001)
  host 10.128.1.9 255.255.255.0
  client-identifier 0100.10aa.aa00.01
  bootfile disable.cm
!
ip dhcp pool DisabledModem(0020.bbbb.0002)
  host 10.128.1.10 255.255.255.0
  client-identifier 0100.20bb.bb00.02
  bootfile disable.cm

ip dhcp pool DisabledModem(1010.9581.7f66)
  host 10.128.1.11 255.255.255.0
  client-identifier 0100.1095.817f.66
  bootfile disable.cm

```

DHCP Pools for CPE Devices

The following examples show a typical DHCP pool for CPE devices. Each pool includes the following fields:

- The **network** command defines the range of IP addresses to be assigned to the CPE devices. Typically, this command specifies a subnet in the secondary address range for the cable interface.

- The **default-router** command specifies the default gateway.
- The **dns-server** command specifies one or more IP addresses for the DNS name-resolution servers that the CPE devices should use.
- The **domain-name** command specifies the fully-qualified domain name that the CPE devices should use.
- The **lease** command specifies that the DHCP lease expires in is 7 days, 0 hours, and 10 minutes. (The CPE device will typically attempt to renew the lease at the halfway mark of approximately 3 days and 12 hours.)

```
!
ip dhcp pool hosts
  network 10.254.1.0 255.255.255.0
  default-router 10.254.1.1
  dns-server 10.254.1.1 10.128.1.1
  domain-name ExamplesDomainName.com
  lease 7 0 10
!
```

The following example shows a DHCP pool that assigns a permanent, static IP address to a particular CPE device. This example is identical to the previous pool except for the following commands:

- The **host** command is used (instead of the **network** command) to specify a single static IP address that will be assigned to the CPE device.
- The **client-identifier** command identifies the particular CPE device. The CPE device is identified by the combination of the Ethernet media code (“01”) plus the device’s MAC address (0001.dddd.0001).

```
!
ip dhcp pool staticPC(0001.dddd.0001)
  host 10.254.1.12 255.255.255.0
  client-identifier 0100.01dd.dd00.01
  default-router 10.254.1.1
  dns-server 10.254.1.1 10.128.1.1
  domain-name ExamplesDomainName.com
  lease 7 0 10
```

ToD Server Example

The following example shows a typical ToD server configuration:

```
service udp-small-servers max-servers no-limit
cable time-server
```

These are the only commands required to enable the ToD server.

TFTP Server Example

The following lines are an excerpt from a configuration that includes a TFTP server. The **cable tftp-enforce** command is optional but recommended for each cable interface. Change the files listed with the **tftp-server** command to match the specific files that are on your system.

```
! Enable the user of unlimited small servers
service udp-small-servers max-servers no-limit
!
...
```

```

! Enable the TFTP Enforce feature on all cable interfaces
interface Cable3/0
  cable tftp-enforce
interface Cable4/0
  cable tftp-enforce
interface Cable5/0
  cable tftp-enforce
!
!
...
! Enable the TFTP server and specify the files that can be
! downloaded along with their aliases
tftp-server disk0:gold.cm alias gold.cm
tftp-server disk0:silver.cm alias silver.cm
tftp-server disk0:bronze.cm alias bronze.cm
tftp-server disk0:ubr924-k8y5-mz.bin alias ubr924-codefile
tftp-server disk0:ubr925-k9v9y5-mz.bin alias ubr925-codefile

```

Basic All-in-One Configuration Example

The basic “all-in-one configuration” sample below summarizes all the components described in examples in the [“Configuration Examples” section on page 55](#). Five DOCSIS configuration files are available. The internal DOCSIS configuration file editor has been used to create four (platinum.cm, gold.cm, silver.cm, and disable.cm), and the fifth file, bronze.cm, has been loaded on to the slot0 Flash memory device. The disable.cm file disables network access for all CPE devices attached to a cable modem, and the other four files provide different levels of Quality-of-Service (QoS).

The configuration has two DHCP pools with two different address spaces. One pool provides IP addresses and platinum-level service for cable modems, and the other pool provides IP addresses for CPE devices.

```

!
version 12.1
no service pad
! provides nice timestamps on all log messages
service timestamps debug datetime msec localtime
service timestamps log uptime

! turn service password-encryption on to encrypt passwords
no service password-encryption

! provides additional space for longer configuration file
service compress-config

! supports a large number of modems / hosts attaching quickly
service udp-small-servers max-servers no-limit
!
hostname Router
!
boot system disk0:
!
no cable qos permission create
no cable qos permission update
cable qos permission modems

! permits cable modems to obtain Time of Day (TOD) from uBR7100
cable time-server

!
! High performance DOCSIS config file, additional options may be added
! 10 Mbit/sec download, 128 Kbit/sec upload speed, 10 Kbit/sec guaranteed upstream

```

```
! NOTE: cable upstream 0 admission-control 150 will prevent modems from
!   connecting after 150% of guaranteed-bandwidth has been allocated to
!   registered modems. This can be used for peek load balancing.
! max-burst 1600 prevents a modem with concatenation turned on from consuming
!   too much wire time, and interfering with VoIP traffic.
! cpe max 8 limits the modem to 8 hosts connected before the CMTS refuses
!   additional host MAC addresses.
! Timestamp option makes the config file only valid for a short period of time.
!
cable config-file platinum.cm
  service-class 1 max-upstream 128
  service-class 1 guaranteed-upstream 10
  service-class 1 max-downstream 10000
  service-class 1 max-burst 1600
  cpe max 8
  timestamp
!
! Medium performance DOCSIS config file, additional options may be added
!   5 Mbit/sec download, 128 Kbit/sec upload speed
!
cable config-file gold.cm
  service-class 1 max-upstream 64
  service-class 1 max-downstream 5000
  service-class 1 max-burst 1600
  cpe max 3
  timestamp
!
! Low performance DOCSIS config file, additional options may be added
!   1 Mbit/sec download, 64 Kbit/sec upload speed
!
cable config-file silver.cm
  service-class 1 max-upstream 64
  service-class 1 max-downstream 1000
  service-class 1 max-burst 1600
  cpe max 1
  timestamp
!
! No Access DOCSIS config file, used to correctly shut down an unused cable modem
!   1 kbit/sec download, 1 Kbit/sec upload speed, with USB/ethernet port shut down.
!
cable config-file disable.cm
  access-denied
  service-class 1 max-upstream 1
  service-class 1 max-downstream 1
  service-class 1 max-burst 1600
  cpe max 1
  timestamp
!
ip subnet-zero
! Turn on cef switching / routing, anything but process switching (no ip route-cache)
ip cef
ip cef accounting per-prefix

! Disables the finger server
no ip finger

! Prevents CMTS from looking up domain names / attempting to connect to
!   machines when mistyping commands
no ip domain-lookup

! Prevents issuance of IP address that is already in use.
ip dhcp ping packets 1

!
```

```

! DHCP reply settings for DOCSIS cable modems.
! All settings here are "default response settings" for this DHCP pool.
! DOCSIS bootfile (cable modem config-file) as defined above
! next-server = IP address of server which sends bootfile
! default-router = default gateway for cable modems, necessary to get DOCSIS files
! option 4 = TOD server IP address
! option 2 = Time offset for TOD, in seconds, HEX, from GMT, -28,000 = PST = ffff.8f80
! option 7 = Optional SYSLOG server
! Lease length, in days, hours, minutes
!
ip dhcp pool CableModems-Platinum
    network 10.128.1.0 255.255.255.0
    bootfile platinum.cm
    next-server 10.128.1.1
    default-router 10.128.1.1
    option 2 hex ffff.8f80
    option 4 ip 10.128.1.1
    option 7 ip 10.128.1.1
    lease 7 0 10

!
! DHCP reply settings for IP hosts behind DOCSIS cable modems.
! All settings here are "default response settings" for this DHCP pool.
! default-router = default gateway for cable modems, necessary to get DOCSIS files
! dns-server = IP address for DNS server, place up to 8 addresses on the same
! line as a list
! NOTE: changing the DNS-server on a Windows PC, Mac, or Unix box require
! reloading the OS, but changing it in the DHCP response is quick and easy.
! domain-name = default domain name for the host
! Lease length, in days, hours, minutes
!
ip dhcp pool hosts
    network 10.254.1.0 255.255.255.0
    default-router 10.254.1.1
    dns-server 10.254.1.1 10.128.1.1
    domain-name ExamplesDomainName.com
    lease 1 0 10

!
!
!
interface FastEthernet0/0
    ip address 10.17.123.1 255.255.255.0
    no ip mroute-cache
    no shutdown
    duplex auto
    speed auto
!
interface FastEthernet0/1
    no ip address
    no ip mroute-cache
    shutdown
    duplex auto
    speed auto
!
! Primary address is for cable modems, use only one, so make it large enough!
! Secondary addresses are for hosts, use as many as necessary
! These addresses must match the remainder of the configuration file,
! or modems won't work.
! cable downstream frequency sets the upconverter frequency
! cable down rf-power 55, sets the upconverter output power in dBmV
! each upstream interface can have a description, use it!
! All four upstreams have been set to the same default frequency, don't
! connect wire them together while on the same frequency!
! cable upstream 0 admission-control 150: limits the number of modems

```

```

! which can connect with guaranteed-bandwidth.
! NOTE: will prevent some modems from connecting once this limit is hit.
!
! High security option:
! no cable arp: prevents the uBR7100 from ever arping towards the cable modems
! for any IP-mac address pairing. Forces EVERY host to use DHCP at least
! once every time the uBR7100 is reloaded, or the arp table is cleared out.
! Forces users to use DHCP release/renew cycle on their computers if
! ARP entry is ever lost.
! Makes it impossible for an end user to type in a static IP address,
! or steal somebody else's IP address.
!
! cable-source verify dhcp: -- Forces the CMTS to populate the arp table from
! the DHCP server
! If the DHCP server does not have a valid DHCP lease for that IP / MAC combination,
! the host is unreachable.
! cable dhcp-giaddr policy: use primary IP address for modems, secondary for
! hosts behind modems
!
!
interface Cable1/0
  description Cable Downstream Interface
  ip address 10.254.1.1 255.255.255.0 secondary
  ip address 10.128.1.1 255.255.255.0
  no keepalive
  cable downstream rate-limit token-bucket shaping
  cable downstream annex B
  cable downstream modulation 64qam
  cable downstream interleave-depth 32
  cable downstream frequency 851000000
  cable down rf-power 55
  cable upstream 0 description Cable upstream interface, North
  cable upstream 0 frequency 37008000
  cable upstream 0 power-level 0
  cable upstream 0 admission-control 150
  no cable upstream 0 shutdown
  cable upstream 1 description Cable upstream interface, South
  cable upstream 1 frequency 37008000
  cable upstream 1 power-level 0
  cable upstream 1 admission-control 150
  no cable upstream 1 shutdown
  cable upstream 2 description Cable upstream interface, East
  cable upstream 2 frequency 37008000
  cable upstream 2 power-level 0
  cable upstream 2 admission-control 150
  no cable upstream 2 shutdown
  cable upstream 3 description Cable upstream interface, West
  cable upstream 3 frequency 37008000
  cable upstream 3 power-level 0
  cable upstream 3 admission-control 150
  no cable upstream 3 shutdown
  no cable arp
  cable source-verify dhcp
  cable dhcp-giaddr policy
!
!
! default route to Fast ethernet 0/0, probably best to set
! this as an IP address so interface flaps don't create route flaps.
! IP http server: enables internal http server
!
ip classless
no ip forward-protocol udp netbios-ns
ip route 0.0.0.0 0.0.0.0 FastEthernet0/0
ip http server

```

```

!
!
! Enable TFTP downloads of the silver.cm file on the Flash device
! this DOCSIS config file is built using DOCSIS CPE Configurator.
tftp-server slot0:bronze.cm alias bronze.cm
!
! Aliases for frequently used commands
!
alias exec scm show cable modem
alias exec scf show cable flap
alias exec scp show cable qos profile
!
line con 0
    exec-timeout 0 0
    transport input none
line aux 0
    speed 19200
line vty 0 4
    session-timeout 60
    login
!
ntp clock-period 17179977
ntp server 192.168.35.51
end

```

Advanced All-in-One Configuration Example

The advanced all-in-one configuration is identical to the basic configuration, except that it uses a hierarchical structure of DHCP pools to provide unique DHCP options, such as static IP addresses, to individual cable modems and CPE devices. The DHCP pools are given unique and relevant names to simplify administration, and the cable modems and CPE devices that use these pools are specified by the **client-identifier** commands.

The DHCP pools for the individual cable modems and CPE devices inherit the options from the parent pools, so you do not need to specify all of the required options for those particular pools. Instead, the new pools need to specify only those commands, such as **client-identifier**, that should be different from the parent pools.

Because the static IP addresses that are given to the cable modems and CPE devices are in the range of 10.1.4.60 and 10.1.4.70, the **ip dhcp exclude** command is used to instruct the DHCP server that it should not hand out addresses in this range to other cable modems or CPE devices.

```

!
version 12.1
no service pad
! provides nice timestamps on all log messages
service timestamps debug datetime msec localtime
service timestamps log uptime

! turn service password-encryption on to encrypt passwords
no service password-encryption

! provides additional space for longer configuration file
service compress-config

! supports a large number of modems / hosts attaching quickly
service udp-small-servers max-servers no-limit
!
hostname Router
!
boot system disk0:

```

```
!
no cable qos permission create
no cable qos permission update
cable qos permission modems

! permits cable modems to obtain Time of Day (ToD) from uBR7100
cable time-server

!
! High performance DOCSIS config file, additional options may be added
! 10 Mbit/sec download, 128 Kbit/sec upload speed, 10 Kbit/sec guaranteed upstream
! NOTE: cable upstream 0 admission-control 150 will prevent modems from
! connecting after 150% of guaranteed-bandwidth has been allocated to
! registered modems. This can be used for peak load balancing.
! max-burst 1600 prevents a modem with concatenation turned on from consuming
! too much wire time, and interfering with VoIP traffic.
! cpe max 8 limits the modem to 8 hosts connected before the CMTS refuses
! additional host MAC addresses.
! Timestamp option makes the config file only valid for a short period of time.
!
cable config-file platinum.cm
  service-class 1 max-upstream 128
  service-class 1 guaranteed-upstream 10
  service-class 1 max-downstream 10000
  service-class 1 max-burst 1600
  cpe max 8
  timestamp

!
! Medium performance DOCSIS config file, additional options may be added
! 5 Mbit/sec download, 128 Kbit/sec upload speed
!
cable config-file gold.cm
  service-class 1 max-upstream 64
  service-class 1 max-downstream 5000
  service-class 1 max-burst 1600
  cpe max 3
  timestamp

!
! Low performance DOCSIS config file, additional options may be added
! 1 Mbit/sec download, 64 Kbit/sec upload speed
!
cable config-file silver.cm
  service-class 1 max-upstream 64
  service-class 1 max-downstream 1000
  service-class 1 max-burst 1600
  cpe max 1
  timestamp

!
! No Access DOCSIS config file, used to correctly shut down an unused cable modem
! 1 kbit/sec download, 1 Kbit/sec upload speed, with USB/ethernet port shut down.
!
cable config-file disable.cm
  access-denied
  service-class 1 max-upstream 1
  service-class 1 max-downstream 1
  service-class 1 max-burst 1600
  cpe max 1
  timestamp

!
ip subnet-zero
! Turn on cef switching / routing, anything but process switching (no ip route-cache)
ip cef
ip cef accounting per-prefix
```

```

! Disables the finger server
no ip finger

! Prevents CMTS from looking up domain names / attempting to connect to
! machines when mistyping commands
no ip domain-lookup

! Prevents the issuance of IP addresses in this range, allows for use in
! static configurations.
ip dhcp excluded-address 10.128.1.60 10.128.1.70

! Prevents issuance of IP address that is already in use.
ip dhcp ping packets 1

!
! DHCP reply settings for DOCSIS cable modems.
! All settings here are "default response settings" for this DHCP pool.
! DOCSIS bootfile (cable modem config-file) as defined above
! next-server = IP address of server which sends bootfile
! default-router = default gateway for cable modems, necessary to get DOCSIS files
! option 4 = TOD server IP address
! option 2 = Time offset for TOD, in seconds, HEX, from GMT, -28,000 = PST = ffff.8f80
! option 7 = Optional SYSLOG server
! Lease length, in days, hours, minutes
!
ip dhcp pool CableModems-Platinum
    network 10.128.1.0 255.255.255.0
    bootfile platinum.cm
    next-server 10.128.1.1
    default-router 10.128.1.1
    option 2 hex ffff.8f80
    option 4 ip 10.128.1.1
    option 7 ip 10.128.1.1
    lease 7 0 10

!
! DHCP reply settings for IP hosts behind DOCSIS cable modems.
! All settings here are "default response settings" for this DHCP pool.
! default-router = default gateway for cable modems, necessary to get DOCSIS files
! dns-server = IP address for DNS server, place up to 8 addresses on the same
! line as a list
! NOTE: changing the DNS-server on a Windows PC, Mac, or Unix box require
! reloading the OS, but changing it in the DHCP response is quick and easy.
! domain-name = default domain name for the host
! Lease length, in days, hours, minutes
!
ip dhcp pool hosts
    network 10.254.1.0 255.255.255.0
    default-router 10.254.1.1
    dns-server 10.254.1.1 10.128.1.1
    domain-name ExamplesDomainName.com
    lease 1 0 10

!
! DHCP reply settings for a static IP address for a PC and cable modems
! All settings here will override "default response settings" for this DHCP pool.
! client-identifier is the ethernet MAC address of the device, preceded by 01
! Thus, the Host with an mac address of 08.00.09.af.34.e2 will ALWAYS get the
! same IP address
! Lease length, in days, hours, minutes, set to infinite.
! Use a relevant name here, as there will be lots of these entries.
!
ip dhcp pool staticPC(0800.09af.34e2)
    host 10.254.1.12 255.255.255.0

```



```

        client-identifier 0108.0009.af34.e2
        client-name staticPC(0800.09af.34e2)
        lease infinite

ip dhcp pool cm-0050.04f9.efa0cm-
  host 10.128.1.65 255.255.255.0
  client-identifier 0100.107b.ed9b.45
  bootfile disable.cm
!
ip dhcp pool cm-0030.d002.41f5
  host 10.128.1.66 255.255.255.0
  client-identifier 0100.107b.ed9b.23
  bootfile silver.cm
!
! DHCP reply settings for a cable modem, to change from default provisioning
! All settings here will override "default response settings" for this DHCP pool.
!   client-identifier is the ethernet MAC address of the device, preceded by 01
!   Thus, the modem with a mac address of 00.10.95.81.7f.66 will ALWAYS get the
!   same IP address
! This cable modem will get the gold.cm config file, and a consistent IP address
!   some IP address within the DHCP pool for the cable downstream interface is
!   required, or the reference correct config file will NOT be issued.
! Use a relevant name here, as there will be lots of these entries.
!
! WARNING: When changing config files for a modem, it is necessary to clear the
! address with "clear ip dhcp binding <ip-address>" and then reset the modem using
! "clear cable modem <mac-address> | <ip-address> reset"
!
ip dhcp pool goldmodem
  host 10.128.1.67 255.255.255.0
  client-identifier 0100.1095.817f.66
  bootfile gold.cm
!
! DHCP reply settings for a disabled cable modem.
! This will prevent this cable modem user from accessing the network.
!   client-identifier is the ethernet MAC address of the device, preceded by 01
! This cable modem will get the disable.cm config file, and a consistent IP address
!   some IP address within the DHCP pool for the cable downstream interface is
!   required, or the reference correct config file will NOT be issued.
! Use a relevant name here, as there will be lots of these entries.
!
! WARNING: When changing config files for a modem, it is necessary to clear the
! address with "clear ip dhcp binding <ip-address>" and then reset the modem using
! "clear cable modem <mac-address> | <ip-address> reset"
!
ip dhcp pool DisabledModem(0010.aaaa.0001)
  host 10.128.1.68 255.255.255.0
  client-identifier 0100.1095.817f.66
  bootfile disable.cm
!
ip dhcp pool DisabledModem(0000.bbbb.0000)
  client-identifier 0100.00bb.bb00.00
  host 10.128.1.69 255.255.255.0
  bootfile disable.cm
!
!
!
interface FastEthernet0/0
  ip address 10.17.123.1 255.255.255.0
  no ip mroute-cache
  no shutdown
  duplex auto
  speed auto
!

```

```

interface FastEthernet0/1
  no ip address
  no ip mroute-cache
  shutdown
  duplex auto
  speed auto
!
! Primary address is for cable modems, use only one, so make it large enough!
! Secondary addresses are for hosts, use as many as necessary
! These addresses must match the remainder of the configuration file,
! or modems won't work.
! cable downstream frequency sets the upconverter frequency
! cable down rf-power 55, sets the upconverter output power in dBmV
! each upstream interface can have a description, use it!
! All four upstreams have been set to the same default frequency, don't
! connect wire them together while on the same frequency!
! cable upstream 0 admission-control 150: limits the number of modems
! which can connect with guaranteed-bandwidth.
! NOTE: will prevent some modems from connecting once this limit is hit.
!
! High security option:
! no cable arp: prevents the uBR7100 from ever arping towards the cable modems
! for any IP-mac address pairing. Forces EVERY host to use DHCP at least
! once every time the uBR7100 is reloaded, or the arp table is cleared out.
! Forces users to use DHCP release/renew cycle on their computers if
! ARP entry is ever lost.
! Makes it impossible for an end user to type in a static IP address,
! or steal somebody else's IP address.
!
! cable-source verify dhcp: -- Forces the CMTS to populate the arp table from
! the DHCP server
! If the DHCP server does not have a valid DHCP lease for that IP / MAC combination,
! the host is unreachable.
! cable dhcp-giaddr policy: use primary IP address for modems, secondary for
! hosts behind modems
!
!
interface Cable1/0
  description Cable Downstream Interface
  ip address 10.254.1.1 255.255.255.0 secondary
  ip address 10.128.1.1 255.255.255.0
  no keepalive
  cable downstream rate-limit token-bucket shaping
  cable downstream annex B
  cable downstream modulation 64qam
  cable downstream interleave-depth 32
  cable downstream frequency 851000000
  cable down rf-power 55
  cable upstream 0 description Cable upstream interface, North
  cable upstream 0 frequency 37008000
  cable upstream 0 power-level 0
  cable upstream 0 admission-control 150
  no cable upstream 0 shutdown
  cable upstream 1 description Cable upstream interface, South
  cable upstream 1 frequency 37008000
  cable upstream 1 power-level 0
  cable upstream 1 admission-control 150
  no cable upstream 1 shutdown
  cable upstream 2 description Cable upstream interface, East
  cable upstream 2 frequency 37008000
  cable upstream 2 power-level 0
  cable upstream 2 admission-control 150
  no cable upstream 2 shutdown
  cable upstream 3 description Cable upstream interface, West

```

```
cable upstream 3 frequency 37008000
cable upstream 3 power-level 0
cable upstream 3 admission-control 150
no cable upstream 3 shutdown
no cable arp
cable source-verify dhcp
cable dhcp-giaddr policy
!
!
! default route to Fast ethernet 0/0, probably best to set
! this as an IP address so interface flaps don't create route flaps.
! IP http server: enables internal http server on uBR7100
!
ip classless
no ip forward-protocol udp netbios-ns
ip route 0.0.0.0 0.0.0.0 FastEthernet0/0
ip http server
!
!
! Enable TFTP downloads of the silver.cm file on the Flash device
! this DOCSIS config file is built using DOCSIS CPE Configurator.
tftp-server slot0:bronze.cm alias bronze.cm
!
! Aliases for frequently used commands
!
alias exec scm show cable modem
alias exec scf show cable flap
alias exec scp show cable qos profile
!
line con 0
    exec-timeout 0 0
    transport input none
line aux 0
    speed 19200
line vty 0 4
    session-timeout 60
    login
!
ntp clock-period 17179977
ntp server 192.168.35.51
```

Additional References

For additional information related to <module feature>, refer to the following references:

Related Documents

Related Topic	Document Title
All-In-One Configuration	For information on how to configure a Cisco CMTS that acts as a Dynamic Host Configuration Protocol (DHCP), Time-of-Day (ToD), and TFTP server in an “all-in-one configuration,” see the following URL: http://www.cisco.com/warp/customer/109/all_in_one_config.shtml
DHCP Configuration	To configure the DHCP server beyond the minimum options given in this chapter, see the “Configuring DHCP” chapter in the “IP Addressing and Services” section of the <i>Cisco IOS IP and IP Routing Configuration Guide</i>, Release 12.2 at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipr_c/index.htm For information on all DHCP commands, see the “DHCP Commands” chapter in the <i>Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services</i>, Release 12.2 at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipras_r/index.htm
TFTP Server Command	For more information about the tftp-server command, see the “Configuring Basic File-Transfer Services” section of the <i>Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2</i> at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/ffun_c/ffcp2/index.htm
NTP or SNTP Configuration	For information on configuring the Cisco CMTS to use NTP or SNTP to set its system clock, see the “Performing Basic System Management” chapter in the “System Management” section of the <i>Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2</i>, at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/ffun_c/fcfprt3/fcf012.htm
Cable Source Verify Feature	For a more detailed description of the cable source-verify command and how it can be used to prevent certain types of denial of service attacks, see the following Tech Note on Cisco.com: http://www.cisco.com/warp/public/109/source_verify.html

Related Topic	Document Title
Calculating the Hexadecimal Value for DHCP Option 2	For information on how to calculate the hexadecimal time value that is used to set the DHCP Time Offset option (DHCP option 2), see the following URL: http://www.cisco.com/warp/public/109/calculate_hexadecimal_dhcp.html
Internal DOCSIS Configuration File Editor	For information on using the internal DOCSIS configuration file editor, see the chapter “Internal DOCSIS Configurator File Generator for the Cisco CMTS” in the Cisco CMTS Feature Guide at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/cable/cab_rout/cmtsfg/ufgcfile.htm
Cisco DOCSIS Configurator Tool	For information on creating DOCSIS 1.1 configuration files, you can use the Cisco DOCSIS Configurator tool, which at the time of this document’s publication is available at the following URL: http://www.cisco.com/cgi-bin/tablebuild.pl/cpe-conf
CMTS Command Reference	<i>Cisco Broadband Cable Command Reference Guide</i>, at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/cable/bbccmref/index.htm
Cisco IOS Release 12.2 Command Reference	Cisco IOS Release 12.2 Configuration Guides and Command References, at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/index.htm
Cisco uBR7100 Series Universal Broadband Router Documentation	<i>Cisco uBR7100 Series Universal Broadband Router Hardware Installation Guide</i>, at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/cable/ubr7100/hig7100/index.htm <i>Cisco uBR7100 Series Universal Broadband Router Software Configuration Guide</i>, at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/cable/ubr7100/scg7100/index.htm

Related Topic	Document Title
Cisco uBR7200 Series Universal Broadband Router Documentation	<i>Cisco uBR7200 Series Universal Broadband Router Hardware Installation Guide</i>, at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/cable/cab_route/cr72hig/index.htm <i>Cisco uBR7200 Series Universal Broadband Router Software Configuration Guide</i>, at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/cable/cab_route/cr72scg/index.htm
Cisco uBR10012 Universal Broadband Router Documentation	<i>Cisco uBR10012 Universal Broadband Router Hardware Installation Guide</i>, at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/cable/ubr10k/ubr10012/hig/index.htm <i>Cisco uBR10012 Universal Broadband Router Software Configuration Guide</i>, at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/cable/ubr10k/ubr10012/scg/index.htm

Standards

Standards ¹	Title
ANSI/SCTE 22-1 2002 (formerly SP-RFI-C01-011119)	Data-Over-Cable Service Interface Specification DOCSIS 1.0 Radio Frequency Interface (RFI) (http://www.cablemodem.com)
SP-RFIV1.1-I08-020301	Data-over-Cable Service Interface Specifications Radio Frequency Interface Specification DOCSIS 1.1 (http://www.cablemodem.com)
SP-BPI+-I08-020301	DOCSIS Baseline Privacy Interface Plus Specification (http://www.cablemodem.com)

1. Not all supported standards are listed.

MIBs

MIBs ¹	MIBs Link
DOCS-CABLE-DEVICE-MIB (RFC 2669)	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

1. Not all supported MIBs are listed.

RFCs

RFCs ¹	Title
RFC 868	<i>Time Protocol</i>
RFC 1350	<i>The TFTP Protocol (Revision 2)</i>
RFC 2131	<i>Dynamic Host Configuration Protocol</i>
RFC 2132	<i>DCHP Options and BOOTP Vendor Extensions</i>
RFC 2349	<i>TFTP Timeout Interval and Transfer Size Options</i>
RFC 3046	<i>DHCP Relay Agent Information Option</i>

1. Not all supported RFCs are listed.

Technical Assistance

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

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, TeleRouter, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0502R)

Copyright © 2003 Cisco Systems, Inc. All rights reserved.



Configuring DOCSIS 1.1 on the Cisco CMTS

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

Feature Specifications for DOCSIS 1.1 Operations

Feature History

Release	Modification
12.1(4)CX	DOCSIS 1.1 support was introduced for Cisco uBR7200 series routers.
12.1(7)CX1	Several DOCSIS 1.1 MIBs were updated, reflecting changes in the DOCSIS 1.1 specification. The cable submgmt default command was also added, to set the default value of the attributes in DOCS-SUBMGT-MIB.
12.2(4)XF1 12.2(4)BC1	DOCSIS 1.1 support was introduced for the Cisco uBR7100 series, Cisco uBR7200 series, and Cisco uBR10012 routers on the Release 12.2 BC train.
12.2(4)BC1b	N+1 redundancy during DOCSIS 1.1 operations was supported on the Cisco uBR10012 router.
12.2(8)BC2	The show cable modem mac command was enhanced to show the DOCSIS capabilities and provisioned state of each cable modem.
12.2(11)BC1	N+1 redundancy during DOCSIS 1.1 operations was supported on the Cisco uBR7200 series router.
12.2(11)BC2	The packetcable authorize vanilla-docsis-mta command was supported to allow DOCSIS 1.1 cable modems to use UGS service flows when PacketCable operations have been enabled.

Supported Platforms

Cisco uBR7100 series, Cisco uBR7200 series, Cisco uBR10012 universal broadband routers.

Finding Support Information for Platforms and Cisco IOS Software Images

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



Corporate Headquarters:

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

Copyright © 2003 Cisco Systems, Inc. All rights reserved.

Contents

- [Prerequisites for DOCSIS 1.1 Operations, page 74](#)
- [Restrictions for DOCSIS 1.1 Operations, page 75](#)
- [Information about DOCSIS 1.1, page 78](#)
- [How to Configure the Cisco CMTS for DOCSIS 1.1 Operations, page 87](#)
- [Monitoring DOCSIS Operations, page 101](#)
- [Command Summary, page 114](#)
- [Configuration Examples for DOCSIS 1.1 Operations, page 115](#)
- [Additional References, page 125](#)

Prerequisites for DOCSIS 1.1 Operations

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

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

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

**Caution**

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

Restrictions for DOCSIS 1.1 Operations

DOCSIS 1.1 operations includes the following restrictions:

Baseline Privacy Interface Plus Requirements

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

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

**Note**

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

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

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

BPI+ Not Supported with High Availability Configurations

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

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

Cable Interface Cards

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

Cable Privacy Hotlist CLI Not Supported on Cisco uBR10012 Router

The **cable privacy hotlist** command is not supported on the Cisco uBR10012 router. To add a manufacturer's or CM certificate to the hotlist on the Cisco uBR10012 router, use SNMP commands to set the appropriate attributes in [DOCS-BPI-PLUS-MIB](#). See the [“Adding a Certificate to the Hotlist Using SNMP Commands”](#) section on page 98.

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

- [Feature Overview, page 78](#)
- [DOCSIS 1.1 Quality of Service, page 80](#)
- [Benefits, page 86](#)

Feature Overview

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, page 78](#)
- [Concatenation, page 79](#)
- [Dynamic MAC Messages, page 79](#)
- [Enhanced Quality of Service, page 79](#)
- [Fragmentation, page 80](#)
- [Interoperability, page 80](#)
- [Payload Header Suppression, page 80](#)

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.

**Note**

BPI+ is described in the [DOCSIS Baseline Privacy Interface Plus Specification](#) (SP-BPI+-I08-020301), available from the CableLabs DOCSIS web site (<http://www.cablemodem.com>).

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.

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.

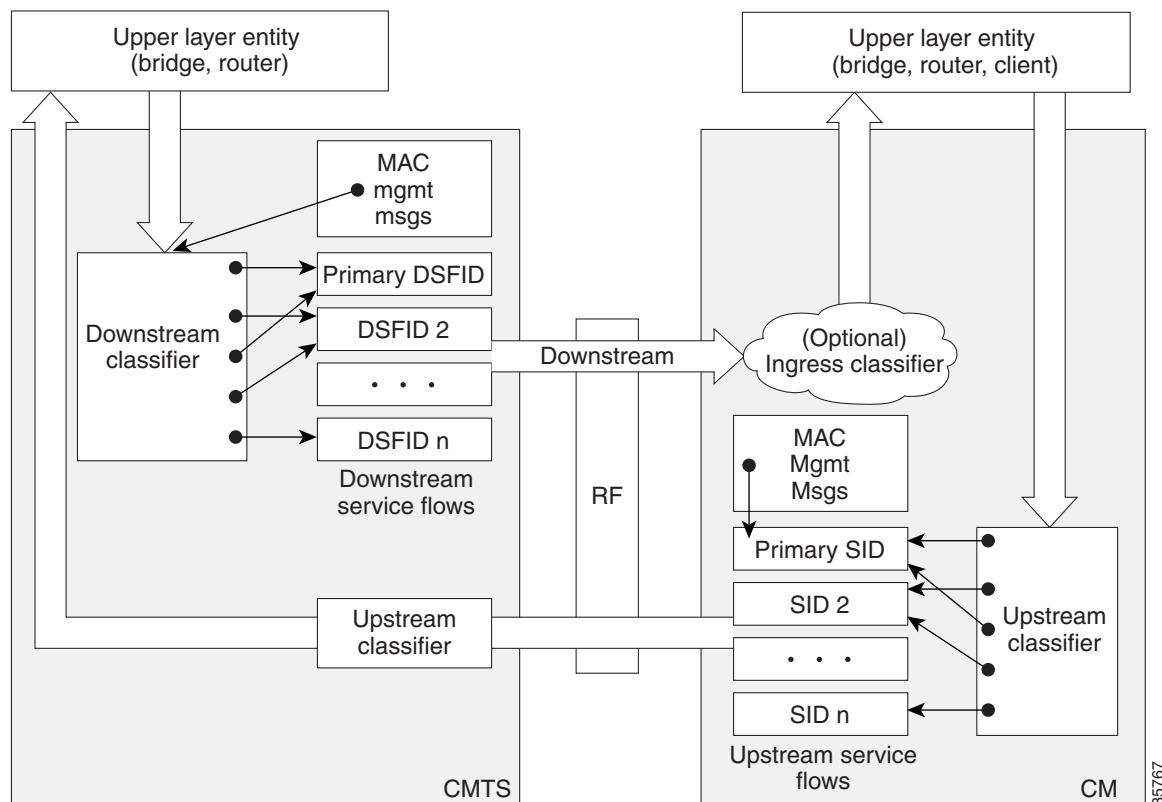
Packet Classifiers

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 2 illustrates the mapping of packet classifiers.

Figure 2 Classification Within the MAC Layer

Packet Header Suppression Rules

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

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

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

Quality of Service Comparison

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

**Note**

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

DOCSIS 1.0

DOCSIS 1.0 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 precedence type-of-service (ToS) bits.

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

DOCSIS 1.0+

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

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

- Multiple SIDs per cable modem, creating separate service flows for voice and data traffic. This allows the CMTS and cable modem to give higher priority for voice traffic, preventing the data traffic from affecting the quality of the voice calls.
- Cable modem-initiated dynamic MAC messages—Dynamic Service Addition (DSA) and Dynamic Service Deletion (DSD). These messages allow dynamic SIDs to be created and deleted on demand, so that the bandwidth required for a voice call can be allocated at the time a call is placed and then freed up for other uses when the call is over.
- Unsolicited grant service (CBR-scheduling) on the upstream—This helps provide a higher-quality channel for upstream VoIP packets from an Integrated Telephony Cable Modem (ITCM) such as the Cisco uBR925 cable access router.

- Ability to provide separate downstream rates for any given cable modem, based on the IP-precedence value in the packet. This helps separate voice signaling and data traffic that goes to the same ITCM to address rate shaping purposes.
- Concatenation allows a cable modem to send several packets in one large burst, instead of having to make a separate grant request for each.

**Caution**

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

Interoperability with Different Versions of DOCSIS Networks

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

Table 2 shows the interoperability of a DOCSIS 1.1 CMTS with different versions of cable modems.

Table 2 *DOCSIS 1.1 Interoperability*

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

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 unclassified 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.

- [Configuring Baseline Privacy Interface \(optional\), page 88](#)
- [Downloading the DOCSIS Root Certificate to the CMTS \(required\), page 91](#)
- [Adding a Manufacturer's Certificate as a Trusted Certificate \(optional\), page 94](#)
- [Adding a Manufacturer's or CM Certificate to the Hotlist \(required\), page 96](#)
- [Enabling Concatenation \(optional\), page 99](#)
- [Enabling DOCSIS Fragmentation \(optional\), page 100](#)

**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”](#) section on page 125.

Configuring Baseline Privacy Interface (optional)

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



Note

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

Prerequisites

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.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface cable *x/y***
4. **cable privacy**
5. **cable privacy 40-bit-des**
6. **cable privacy accept-self-signed-certificate**



Caution

Cisco strongly recommends that this above command remain unconfigured, 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.

7. **cable privacy authenticate-modem**
8. **cable privacy authorize-multicast**
9. **cable privacy mandatory**
10. **cable privacy oaep-support**
11. **cable privacy kek {*grace-time seconds* | *life-time seconds*}**
12. **cable privacy tek {*grace-time seconds* | *life-time seconds*}**
13. **exit**
14. **exit**

DETAILED STEPS

	Command	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 x/y Example: Router(config)# interface cable 6/0 Router(config-if)#	Enters interface configuration mode for the cable interface line card at this particular slot.
Step 4	cable privacy Example: Router(config-if)# cable privacy Router(config-if)#	(Optional) Enables BPI+ 56-bit DES encryption on the cable interface (default).
Step 5	cable privacy 40-bit-des Example: Router(config-if)# cable privacy 48-bit-des Router(config-if)#	(Optional) Enables BPI+ 40-bit DES encryption on the cable interface. Cisco does not recommend this option for production systems because 40-bit encryption is not as secure as the 56-bit DES or 168-bit 3DES encryption algorithms.
Step 6	cable privacy accept-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 Cisco strongly recommends that this command remain unconfigured, 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.

	Command	Purpose
Step 7	cable privacy authenticate-modem Example: Router(config-if)# cable privacy authenticate-modem Router(config-if)#	(Optional) Enables BPI+ encryption on the cable interface and uses the Cisco IOS Authentication, Authorization and Accounting (AAA) service together with BPI to authenticate the CMs.
Step 8	cable privacy authorize-multicast Example: Router(config-if)# cable privacy authorize-multicast Router(config-if)#	(Optional) Enables BPI+ encryption on the cable interface and uses AAA protocols to authorize all multicast stream (IGMP) join requests. Note If you use this command to authorize multicast streams, you must also use the cable privacy authenticate-modem command to enable AAA services on the cable interface.
Step 9	cable privacy mandatory Example: Router(config-if)# cable privacy mandatory Router(config-if)#	(Optional) Enables BPI+ encryption on the cable interface and requires baseline privacy for all CMs. If a CM does not enable BPI or BPI+ encryption in its DOCSIS configuration file, it will not be allowed to come online.
Step 10	cable privacy oaep-support Example: Router(config-if)# cable privacy oaep-support Router(config-if)#	(Optional) Enables BPI+ encryption on the cable interface and enables Optimal Asymmetric Encryption Padding (OAEP). This option is enabled by default. Disabling this option could have a performance impact.
Step 11	cable privacy kek {<i>grace-time seconds</i> <i>life-time seconds</i>} Example: Router(config-if)# cable privacy kek grace-time 480 Router(config-if)# cable privacy kek life-time 302400 Router(config-if)#	(Optional) Configures the grace-time and life-time values for the key encryption keys (KEKs) for BPI+ operations on all cable interfaces. • grace-time <i>seconds</i>¹—(DOCSIS 1.0 BPI only) The amount of time before the KEK key expires that the CM should begin renegotiating a new key. The valid range is 60 to 1800 seconds, with a default of 600 seconds (10 minutes). • life-time <i>seconds</i>—The maximum amount of time, in seconds, that a KEK key can be considered valid. The valid range is 300 to 604,8000, with a default of 604,800 seconds (7 days).
Step 12	cable privacy tek {<i>grace-time seconds</i> <i>life-time seconds</i>} Example: Router(config-if)# cable privacy tek grace-time 1800 Router(config-if)# cable privacy tek life-time 86400 Router(config-if)#	(Optional) Configures the grace-time and life-time values for the traffic encryption keys (TEKs) for BPI+ operations on all cable interfaces. • grace-time <i>seconds</i>¹—(DOCSIS 1.0 BPI only) The amount of time before the TEK key expires that the CM should begin renegotiating a new key. The valid range is 60 to 1800 seconds, with a default of 600 seconds (10 minutes). • life-time <i>seconds</i>—The maximum amount of time, in seconds, that a TEK key can be considered valid. The valid range is 180 to 604,8000, with a default of 43,200 seconds (12 hours).

	Command	Purpose
Step 13	exit Example: Router(config-if)# exit Router(config)#	Exits interface configuration mode. Note Repeat steps Step 3 through Step 13 for each cable interface.
Step 14	exit Example: Router(config)# exit Router#	Exits global configuration mode.

1. The KEK and TEK grace-time values apply only to DOCSIS 1.0 cable modems using BPI encryption. Cable modems that are running DOCSIS 1.1 software configure the grace-time values in their DOCSIS configuration files, and those values automatically override the CMTS settings. If a DOCSIS 1.1 configuration file does not specifically contain the grace-time values, the cable modem defaults to 600 seconds, which is the value that the CMTS then uses for the modem.

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 3 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.
Authorization Grace Timeout	The grace period for reauthorization (in seconds).
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 (required)

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. To enable the use of these digital certificates in the DOCSIS network, you must download the DOCSIS root certificate from the Verisign website and copy it to the bootflash on the Cisco CMTS router.

**Tip**

For more information about the DOCSIS root certificate provided by Verisign, see the information at the following URL:

<http://www.verisign.com/products/cable/index.html>

**Note**

The Cisco CMTS supports only one root certificate. If you load the DOCSIS root certificate, you cannot also load a EuroDOCSIS or PacketCable root certificate. EuroDOCSIS or PacketCable devices can still come online, however, if they use self-signed manufacturer's digital certificates.

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

- Step 1** Download the DOCSIS root certificate from the DOCSIS certificate signer, Verisign. At the time of this document's printing, the DOCSIS root certificate is available for download at the following URL:

<http://www.verisign.com/products/cable/root.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:

```
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):

```
Router# dir bootflash:
```

```
Directory of bootflash:/
```

```
1 -rw- 3229188 Dec 30 2002 15:53:23 ubr7200-boot-mz.122-11.BC2.bin
```

```
3407872 bytes total (250824 bytes free)
```

```
Router#
```

**Tip**

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

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

Router# **copy tftp bootflash:**

```
Address or name of remote host []? tftp-server-ip-address
Source filename []? CableLabs_DOCSIS.509
Destination filename [CableLabs_DOCSIS.509]? root-cert
Loading CableLabs_DOCSIS.509 from tftp-server-ip-address (via FastEthernet0/0): !
[OK - 996/1024 bytes]

996 bytes copied in 4.104 secs (249 bytes/sec)
Router#
```



Tip

If you are using Cisco IOS Release 12.2(4)BC1 or later software release, you can also copy the root certificate to a PCMCIA Flash Disk (disk0 or disk1). However, because Flash Disks are unsecure 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:

Router# **dir bootflash:**

Directory of bootflash:/

```
  1  -rw-      3229188  Dec 30 2002 15:53:23  ubr7200-boot-mz.122-11.BC2.bin
  2  -rw-         996   Mar 06 2002 16:03:46  root-cert
```

```
3408876 bytes total (248696 zxbytes free)
Router#
```

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



Note

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

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
```



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 (optional)

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

- [Adding a Certificate as a Trusted Certificate Using the Command Line Interface, page 94](#)
- [Adding a Certificate as a Trusted Certificate Using SNMP Commands, page 95](#)



Note

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

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

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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cable privacy add-certificate manufacturer *hex-data***
4. **exit**

DETAILED STEPS

	Command	Purpose
Step 1	enable	Enables privileged EXEC mode. Enter your password if prompted.
	Example: Router> enable Router#	
Step 2	configure terminal	Enters global configuration mode.
	Example: Router# configure terminal Router(config)#	

	Command	Purpose
Step 3	cable privacy add-certificate manufacturer <i>hex-data</i> Example: <pre>Router(config)# cable privacy add-certificate manufacturer 0001020304050CFD0E0F0A01EB02BC0304 0F019E020D230C04CD050B060A07080AF102E30405 Router(config)#</pre>	(Optional) Specifies the hexadecimal data for the manufacturer CA certificate to be added as a trusted certificate. Enter the actual certificate contents as hexadecimal data in the <i>hex-data</i> string. Enter multiple lines as needed, and use a blank line to terminate the string.
Step 4	exit Example: <pre>Router(config)# exit Router#</pre>	Exits global configuration mode.

Adding a Certificate as a Trusted Certificate Using SNMP Commands

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

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

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

- docsBpi2CmtsProvisionedCmCertStatus—Set to 4 to create the row entry.
- docsBpi2CmtsProvisionedCmCert—The hexadecimal data, as an X509Certificate value, for the actual X.509 certificate.
- docsBpi2CmtsProvisionedCmCertTrust—An Integer value from 1 to 2 specifying the certificate's trust status: 1=trusted, 2=untrusted. Specify 1 for CM certificates that should be trusted.



Tip

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

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

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

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

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



Tip

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



Note

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

Adding a Manufacturer's or CM Certificate to the Hotlist (required)

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

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

- [Adding a Certificate to the Hotlist Using the Command Line Interface, page 96](#)
- [Adding a Certificate to the Hotlist Using SNMP Commands, page 98](#)



Note

Unless you cannot use SNMP to configure the cable modem, or have a particular application that requires the use of CLI commands to add certificates, you should also use the SNMP method to add certificates to a cable modem. On the Cisco uBR10012 router, you must use the SNMP method of adding a certificate to the hotlist, because the CLI method will not actually update the hotlist on the Cisco uBR10012 router, even though the router appears to accept the CLI command.

Adding a Certificate to the Hotlist Using the Command Line Interface

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



Note

This procedure is not supported on the Cisco uBR10012 router. Use the following section, [Adding a Certificate to the Hotlist Using SNMP Commands, page 98](#), to add certificates to the hotlist on the Cisco uBR10012 router.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cable privacy hotlist cm *mac-address***

4. **cable privacy hotlist manufacturer** *certificate-serial-number*
5. **exit**

DETAILED STEPS

	Command	Purpose
Step 1	enable Example: Router> enable Router#	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal Router(config)#	Enters global configuration mode.
Step 3	cable privacy hotlist cm <i>mac-address</i> Example: Router(config)# cable privacy hotlist cm 00C0.0102.0304 Router(config)#	(Optional) Adds a CM certificate with the specified MAC address to the certificate hotlist. The <i>mac-address</i> is specified as a string of six hexadecimal digits.
Step 4	cable privacy hotlist manufacturer <i>certificate-serial-number</i> Example: Router(config)# cable privacy hotlist manufacturer 010A0BC304DFEE1CA98371 Router(config)#	Adds a manufacturer's certificate with the specified serial number to the certificate hotlist. The <i>certificate-serial-number</i> is specified as a string of hexadecimal digits. You can optionally use spaces between the digits as separators.
Step 5	exit Example: Router(config)# exit Router#	Exits global configuration mode.

Cable modems that are using a MAC address or manufacturer's certificate that matches one in the hotlist will not be allowed to register. For example, the following command will put the CM with the MAC address of 0000.0C0A.0B0C in the hotlist and prevent it from registering on any cable interface:

```
Router# config terminal
Router(config)# cable privacy hotlist cm 00 00 0C 0a 0b 0c
Oct 31 13:06:29.112: Successfully added CM hotlist 0000.0C0A.0B0C

Router#
```

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

```
Router(config)# cable privacy hotlist manufacturer 00 90 83 00 00 00 00 01
Oct 31 13:06:34.478: Successfully added MFG hotlist 00 90 83 00 00 00 00 01

Router(config)# exit
```

```
Router#
```

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

```
Router# config terminal
Router(config)# no cable privacy hotlist cm 00 00 0C 0a 0b 0c
Router(config)# no cable privacy hotlist manufacturer 00 90 83 00 00 00 00 01
Router(config)# exit
Router#
```

Adding a Certificate to the Hotlist Using SNMP Commands

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

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

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

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



Tip

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



Note

This procedure is identical to the one given for adding a certificate as a trusted certificate in the [“Adding a Certificate as a Trusted Certificate Using SNMP Commands”](#) section on page 95, 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 (optional)

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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface cable** *x/y*
4. **cable upstream** *n* **concatenation**
5. **exit**
6. **exit**

DETAILED STEPS

	Command	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 <i>x/y</i> Example: Router(config)# interface cable 6/0 Router(config-if)#	Enters interface configuration mode for the cable interface line card at this particular slot.
Step 4	cable upstream <i>n</i> 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.

	Command	Purpose
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 (optional)

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

SUMMARY STEPS

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

DETAILED STEPS

	Command	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 <i>x/y</i> Example: Router(config)# Router(config-if)#	Enters interface configuration mode for the cable interface line card at this particular slot.

	Command	Purpose
Step 4	Command <code>cable upstream n fragmentation</code> Example: <pre>Router(config-if)# cable upstream 2 fragmentation Router(config-if)# cable upstream 3 fragmentation Router(config-if)#</pre>	Enables fragmentation for the specified upstream on the cable interface. Note Repeat this command for each upstream on the interface.
Step 5	Command <code>cable upstream n unfrag-slot-jitter [limit jitter cac-enforce]</code> Example: <pre>Router(config-if)# cable upstream 0 unfrag-slot-jitter limit 2000 cac-enforce Router(config-if)#</pre>	(Optional) Specifies the amount of jitter that can be tolerated on the upstream due to unfragmentable slots. The limit option specifies the allowable <i>jitter</i> 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, <i>jitter</i> is set to a limit of 0 microseconds, and the cac-enforce option is enabled.
Step 6	Command <code>exit</code> Example: <pre>Router(config-if)# exit Router(config)#</pre>	Exits interface configuration mode.
Step 7	Command <code>exit</code> Example: <pre>Router(config)# exit Router#</pre>	Exits global configuration mode.

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, page 101](#)
- [Monitoring the RF Network and Cable Interfaces, page 107](#)
- [Monitoring BPI+ Operations, page 111](#)

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, page 102](#)
- [Displaying a Summary Report for the Cable Modems, page 104](#)
- [Displaying the Capabilities of the Cable Modems, page 105](#)
- [Displaying Detailed Information About a Particular Cable Modem, page 106](#)

**Tip**

For a complete description of the **show cable modem** command and its options, see the “Cisco Cable Modem Termination System Commands” chapter in the *Cisco Broadband Cable Command Reference Guide* (see “Additional References” section on page 125).

Displaying the Status of Cable Modems

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

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

Router#

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.

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

Router#

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

```
Router# show cable modem vendor
Vendor      MAC Address      I/F      MAC      Prim RxPwr  Timing  Num BPI
                  State          Sid  (db)    Offset  CPE  Enb
Thomson     0010.9507.01db  C5/1/0/U5 online     1      0.00   938    1    N
Ericsson    0080.37b8.e99b  C5/1/0/U5 online     2     -0.25   1268    0    N
Cisco       0002.fdfa.12ef  C6/1/0/U0 online     13      0.00   1920    1    N
Cisco       0002.fdfa.137d  C6/1/0/U0 online     16     -0.50   1920    1    N
Cisco       0003.e38f.e9ab  C6/1/0/U0 online     3     -0.25   1926    1    N
Cisco       0003.e3a6.7f69  C6/1/0/U0 online     15      0.50   1927    1    N
Cisco       0003.e3a6.816d  C6/1/0/U0 online     4      0.00   1929    1    N
Cisco       0006.28f9.8be5  C6/1/0/U0 online     12      0.75   1922    1    N
Cisco       0001.9659.519f  C6/1/1/U2 online     26      0.25   1930    1    N
Cisco       0002.b96f.fdbb  C6/1/1/U2 online     29     -0.75   1929    1    N
Cisco       0002.b96f.fdf9  C6/1/1/U2 online     39     -0.50   1931    1    N
Cisco       0002.fdfa.12e9  C6/1/1/U2 online     5     -0.25   1925    1    N
Motorola    0020.4005.3f06  C7/0/0/U0 online     2      0.00   1901    1    N
Motorola    0020.4006.b010  C7/0/0/U5 online     3      0.25   1901    1    N
```

```

Cisco      0050.7302.3d83 C7/0/0/U0 online      18      -0.25    1543    1      N
Cisco      00b0.6478.ae8d C7/0/0/U5 online      44       0.50    1920    21     N
Cisco      00d0.bad3.c0cd C7/0/0/U5 online      19       0.00    1543    1      N

```

Router#

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

Table 4 *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.
expire(pt)	The CM registered, BPI is enabled, TEK was assigned but has since expired.
Error Status Conditions	
reject(m)	The CM attempted to register but registration was refused due to a bad Message Integrity Check (MIC) value. This also could indicate that the shared secret in the DOCSIS configuration file does not match the value configured on the CMTS with the cable shared-secret command. In Cisco IOS Release 12.1(11b)EC1 and Cisco IOS Release 12.2(8)BC2 or later releases, this could also indicate that the cable tftp-enforce command has been used to require that a CM attempt a TFTP download of the DOCSIS configuration file before registering, but the CM did not do so.

Table 4 Descriptions for the MAC State Field (continued)

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

Displaying a Summary Report for the Cable Modems

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

```
Router# show cable modem summary
```

```

Interface                               Cable Modem
Total Registered Unregistered Offline
Cable5/1/0/U5      2      2      0      0
Cable6/1/0/U0     14     13      1      0
Cable6/1/1/U2     14     14      0      0
Cable7/0/0/U0      2      2      0      0
Cable7/0/0/U5      4      3      1      1

```

```
Router# show cable modem summary total
```

```

Interface                               Cable Modem
Total Registered Unregistered Offline
Cable5/1/0/U5      2      2      0      0
Cable6/1/0/U0     14     13      1      0
Cable6/1/1/U2     14     14      0      0
Cable7/0/0/U0      2      2      0      0
Cable7/0/0/U5      4      3      1      1

Total:              36     34      2      1

```


Router#

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

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

Interface	Total Modems	Active Modems	Registered Modems
Cable5/0/U0	294	272	271
Cable5/0/U1	256	248	246
Cable5/0/U2	196	194	194
Total:	746	714	711

Router# **show cable modem summary c6/1/1 c7/0/0 total**

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

Router#

Displaying the Capabilities of the Cable Modems

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

Router# **show cable modem mac**

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

Router#

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

Router# **show cable modem mac summary total**

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

```

Total:          32          1          31          25          0          25

Router#

```

Displaying Detailed Information About a Particular Cable Modem

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

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

```

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

```

```
Router#
```

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

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

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

Prim	1st time	Times	%online	Online time			Offline time		
Sid	online	Online		min	avg	max	min	avg	max
1	May 30 2000	4	99.85	48:20	11h34m	1d2h23m	00:01	00:59	03:00

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

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

```
Router#
```

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.

- [Displaying Information About the Mac Scheduler, page 107](#)
- [Displaying Information About QoS Parameter Sets, page 108](#)
- [Displaying Information About Service Flows, page 108](#)
- [Displaying Information About Service IDs, page 110](#)



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 [“Additional References” section on page 125](#)).

Displaying Information About the Mac Scheduler

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

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

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

DOCSIS 1.1 MAC scheduler for Cable3/0/U1
Queue[Rng Polls] 0/64, 0 drops
Queue[CIR Grants] 0/64, 0 drops
Queue[BE(7) Grants] 0/64, 0 drops
Queue[BE(6) Grants] 0/64, 0 drops
Queue[BE(5) Grants] 0/64, 0 drops
Queue[BE(4) Grants] 0/64, 0 drops
Queue[BE(3) Grants] 0/64, 0 drops
Queue[BE(2) Grants] 0/64, 0 drops
Queue[BE(1) Grants] 0/64, 0 drops
Queue[BE(0) Grants] 0/64, 0 drops
Req Slots 81256509, Req/Data Slots 0
Init Mtn Slots 568433, Stn Mtn Slots 68664
Short Grant Slots 2261, Long Grant Slots 2064698
Awacs Slots 0
Fragmentation count 6
Fragmentation test disabled
Avg upstream channel utilization : 1%
Avg percent contention slots : 97%
Avg percent initial ranging slots : 2%
Avg percent minislots lost on late MAPs : 0%
Sched Table Adm-State: Grants 1, Reqpolls 1, Util 20%
UGS      : 0 SIDs, Reservation-level in bps 0
UGS-AD   : 1 SIDs, Reservation-level in bps 412800
RTPS     : 0 SIDs, Reservation-level in bps 0
NRTPS    : Not Supported
BE       : 8 SIDs, Reservation-level in bps 0

Router#
```

Displaying Information About QoS Parameter Sets

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

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

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

```
Router#
```

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

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

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

```
Router#
```

Displaying Information About Service Flows

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

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

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

16	N/A	0050.7366.12fb	4	4	4	prim	DS	act	1d0h39m
15	7	0050.7366.12fb	3	3	3	prim	US	act	1d0h39m
19	N/A	0090.9607.3831	4	4	4	prim	DS	act	1d0h39m
23	10	0090.9607.3831	3	3	3	prim	US	act	1d0h39m

Router#

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

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

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

Router#

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

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

```

Sfid                               : 4
Mac Address                         : 0090.9607.3831
Type                               : Primary
Direction                         : Downstream
Current State                      : Active
Current QoS Indexes [Prov, Adm, Act] : [4, 4, 4]
Active Time                       : 21h04m
Sid                               : N/A
Traffic Priority                   : 0
Maximum Sustained rate            : 1000000 bits/sec
Maximum Burst                     : 1522 bytes
Minimum Reserved Rate             : 0 bits/sec
Admitted QoS Timeout              : 200 seconds
Active QoS Timeout                : 0 seconds
Packets                           : 130
Bytes                             : 123096
Rate Limit Delayed Grants         : 0
Rate Limit Dropped Grants         : 0
Current Throughput                : 68715 bits/sec, 9 packets/sec
Classifiers: NONE

```

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

```

Sfid                               : 19
Current State                      : Active
Sid                               : N/A
Traffic Priority                   : 0
Maximum Sustained rate            : 1000000 bits/sec
Maximum Burst                     : 1522 bytes
Minimum Reserved rate             : 50000 bits/sec
Minimum Packet Size               : 100 bytes
Admitted QoS Timeout              : 200 seconds
Active QoS Timeout                : 0 seconds
Maximum Latency                   : 20000 usecs
Current Throughput                : 68715 bits/sec, 9 packets/sec

```

Router#

Displaying Information About Service IDs

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

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

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

```
Router#
```

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

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

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

```
Router#
```

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

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

```

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

```

```

Nominal Polling Interval      : 100000 usecs
Tolerated Polling Jitter     : 2000 usecs
Unsolicited Grant Size       : 100 bytes
Grants per Interval          : 1
Request/Transmission Policy   : 0x0
IP ToS Overwrite [AND-mask, OR-mask] : 0xFF, 0x0
Current Throughput            : 863 bits/sec, 0 packets/sec

```

Router#

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, page 111](#)
- [Displaying the BPI+ Timer Values on the CMTS, page 113](#)
- [Displaying the Certificate List on the CMTS, page 113](#)

Displaying the Current BPI+ State of Cable Modems

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

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

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

```
Router# show cable modem
```

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

Router#

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

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

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

```

00d0.bad3.c0cd 144.205.151.149 C7/0/0/U5 online(pk) 19 0.25 1543 1 Y
00d0.bad3.c0cf 144.205.151.194 C7/0/0/U0 online(pt) 13 0.00 1546 1 Y
00d0.bad3.c0d5 144.205.151.133 C7/0/0/U0 reject(pt) 12 *0.50 1546 1 Y

```

Router#

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

Router# **show cable modem 00c0.abcd.ef01**

```

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

```

Router#

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

Table 5 Possible show cable modem BPI+ States

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



Tip

Other MAC states are possible. See [Table 4 on page 103](#) for a complete list.

Displaying the BPI+ Timer Values on the CMTS

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

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

```
Configured KEK lifetime value = 604800  
Configured KEK grace time value = 600
```

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

```
Configured TEK lifetime value = 60480  
Configured TEK grace time value = 600
```

```
Router#
```

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
```

```
Router#
```

Command Summary

Table 6 summarizes the commands that are used to configure and monitor the Cisco CMTS for DOCSIS 1.1 operations.

Table 6 *New or Modified Commands for DOCSIS 1.1 Operation*

Command	Description
cable dci-response	Configures how a cable interface responds to DCI-REQ messages for cable modems on that interface.
cable dci-upstream-disable	Configures a cable interface so that it transmits a DOCSIS 1.1 Upstream Transmitter Disable (UP-DIS) message to a particular cable modem (CM).
cable service class	Sets parameters for a cable service class.
cable service flow inactivity-threshold	Sets the inactivity threshold value for service flows using Unsolicited Grant Service with Activity Detection (UGS-AD).
cable submgmt default	Sets the default values for attributes in the Subscriber Management MIB (DOCS-SUBMGT-MIB), so that those default values persist over restarts.
cable upstream fragmentation	Enables DOCSIS 1.1 fragmentation on a cable interface.
cable upstream unfrag-slot-jitter	Controls how much jitter can be tolerated on the corresponding upstream due to unfragmentable slots.
debug cable dci	Displays information about DOCSIS 1.1 Device Class Identification (DCI) messages.
debug cable mac-scheduler	Displays information about the MAC scheduler's admission control activities.
debug cable phs	Displays the activities of the payload header suppression (PHS) driver.
debug cable tlvs	Displays the TLVs parsed by the DOCSIS 1.1 TLV parser/encoder, including the TLVs for service flow encodings, classifier encodings, and PHS rules.
show cable modem	Displays information for the registered and unregistered cable modems.
show cable service-class	Displays the parameters for a DOCSIS 1.1 cable service class.
show interface cable downstream	Displays the downstream packet queuing and the scheduling state.
show interface cable mac-scheduler	Displays the current time-slot scheduling state and statistics.
show interface cable qos paramset	Displays the attributes of the service flow QoS parameter set.
show interface cable service-flow	Displays the attributes of DOCSIS service flows on a given cable interface.

The following commands have been obsoleted and not used for DOCSIS 1.1 operations:

- **cable qos [profile | permission]**
- **cable service-flow inactivity-timeout**
- **show cable qos profile**

Configuration Examples for DOCSIS 1.1 Operations

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

- [DOCSIS 1.1 Configuration for Cisco uBR7246VXR Router \(without BPI+\), page 115](#)
- [DOCSIS 1.1 Configuration for Cisco uBR7246VXR Router \(with BPI+\), page 117](#)
- [DOCSIS 1.1 Configuration for Cisco uBR10012 Router \(with BPI+\), page 121](#)

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

```
version 12.2
no service pad
service timestamps log datetime localtime
service password-encryption
service udp-small-servers max-servers no-limit
!
hostname 7246VXR
!
enable password 7 030A69CE09
!
cable qos profile 8
cable qos profile 10
cable qos profile 10 grant-size 1500
cable qos profile 12 guaranteed-upstream 100000
no cable qos permission create
no cable qos permission update
cable qos permission modems
cable timeserver
!
cable config-file disable.cm
access-denied
service-class 1 max-upstream 1
service-class 1 max-downstream 1600
cpe max 1
timestamp
!
cable config-file platinum.cm
service-class 1 max-upstream 128
service-class 1 guaranteed-upstream 10
service-class 1 max-downstream 10000
service-class 1 max-burst 1600
cpe max 10
timestamp
!
clock timezone PDT -8
clock summer-time PDT recurring
clock calendar-valid
ip subnet-zero
ip cef
ip cef accounting per-prefix
no ip finger
ip tcp synwait-time 5
no ip domain-lookup
ip host vxr 192.100.168.103
ip domain-name cisco.com
ip name-server 192.100.168.70
ip name-server 192.100.168.132
ip name-server 192.100.168.250
no ip dhcp relay information check
```

```

!
!
!
ip dhcp pool cm-platinum
network 10.10.4.0 255.255.255.0
    bootfile platinum.cm
    next-server 10.10.4.1
    default-router 10.10.4.1
    option 7 ip 10.10.4.1
    option 4 ip 10.10.4.1
    option 2 hex ffff.8f80
    lease 7 0 10
!
ip dhcp pool pcs-c4
network 192.100.168.0 255.255.255.224
next-server 192.100.168.1
default-router 192.100.168.1
dns-server 192.100.168.2
domain-name cisco.com
lease 7 0 10
!
!
interface Ethernet2/0
ip address 192.100.168.4 255.255.255.192
no ip mroute-cache
half-duplex
!
interface Cable4/0
ip address 192.100.168.1 255.255.255.224 secondary
ip address 10.10.4.1 255.255.255.0
no ip route-cache cef
no keepalive
cable downstream rate-limit token-bucket shaping
cable downstream annex B
cable downstream modulation 64qam
cable downstream interleave-depth 32
cable downstream frequency 555000000
cable upstream 0 frequency 40000000
cable upstream 0 power-level 0
no cable upstream 0 shutdown
cable upstream 1 shutdown
cable upstream 2 shutdown
cable upstream 3 shutdown
cable upstream 4 shutdown
cable upstream 5 shutdown
cable dhcp-giaddr policy
!
!
router eigrp 202
redistribute connected
redistribute static
network 10.0.0.0
network 192.100.168.0
no auto-summary
no eigrp log-neighbor-changes
!
router rip
version 2
redistribute connected
redistribute static
network 10.0.0.0
network 192.100.168.0
no auto-summary
!

```

```

ip default-gateway 192.100.168.1
ip classless
ip route 0.0.0.0 0.0.0.0 192.100.168.1
ip route 192.100.168.0 255.255.255.0 Ethernet2/0
ip http server
ip http authentication local
!
snmp-server engineID local 00000009020000E01ED77E40
snmp-server community public RO
snmp-server community private RW
tftp-server server
  tftp-server slot0:silver.cm alias silver.cm
!
line con 0
  exec-timeout 0 0
  transport input none
line aux 0
  speed 19200
line vty 0 4
  session-timeout 60
  login
!
ntp clock-period 17179977
ntp server 192.100.168.51
end

```

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

```

version 12.2
no service pad
service password-encryption
service compress-config
!
hostname uBR7246VXR
!
logging queue-limit 100
enable password 7 03085A09
!
clock summer-time EDT recurring
clock calendar-valid
cable flap-list insertion-time 120
cable flap-list power-adjust threshold 5
cable flap-list aging 1440
cable modem max-cpe 2
cable modulation-profile 2 request 0 16 2 8 qpsk scrambler 152 no-diff 64 fixed uw8
cable modulation-profile 2 initial 5 34 0 48 qpsk scrambler 152 no-diff 128 fixed uw16
cable modulation-profile 2 station 5 34 0 48 qpsk scrambler 152 no-diff 128 fixed uw16
cable modulation-profile 2 short 5 91 14 8 qpsk scrambler 152 no-diff 72 shortened uw8
cable modulation-profile 2 long 8 239 0 8 qpsk scrambler 152 no-diff 80 shortened uw8
cable modulation-profile 3 request 0 16 2 8 qpsk scrambler 152 no-diff 64 fixed uw8
cable modulation-profile 3 initial 5 34 0 48 qpsk scrambler 152 no-diff 128 fixed uw16
cable modulation-profile 3 station 5 34 0 48 qpsk scrambler 152 no-diff 128 fixed uw16
cable modulation-profile 3 short 8 85 14 8 qpsk scrambler 152 no-diff 72 shortened uw8
cable modulation-profile 3 long 10 235 0 8 qpsk scrambler 152 no-diff 80 shortened uw8
cable modulation-profile 4 request 0 16 2 8 qpsk scrambler 152 no-diff 64 fixed uw8
cable modulation-profile 4 initial 5 34 0 48 qpsk scrambler 152 no-diff 128 fixed uw16
cable modulation-profile 4 station 5 34 0 48 qpsk scrambler 152 no-diff 128 fixed uw16
cable modulation-profile 4 short 10 8 6 8 8 16qam scrambler 152 no-diff 144 shortened uw16
cable modulation-profile 4 long 10 235 0 8 16qam scrambler 152 no-diff 160 shortened uw16
no cable qos permission create
no cable qos permission update
cable qos permission modems

```

```

cable logging badips source 2000000
cable time-server
!
!
ip subnet-zero
no ip source-route
!
!
ip cef
ip domain name sampleclient.com
ip dhcp smart-relay
ip dhcp relay information option
no ip dhcp relay information check
!
crypto ca trustpoint DOCSIS-ROOT-CERT
!
crypto ca certificate chain DOCSIS-ROOT-CERT
certificate ca 00A07300000000002
308202B7 30820220 A0030201 02020800 A0730000 00000230 0D06092A 864886F7
0D010105 05003081 9D310B30 09060355 04061302 5553310E 300C0603 55040A13
05436F6D 3231310F 300D0603 55040B13 06444F43 53495331 36303406 0355040B
132D4C4F 43303030 332C2037 35302054 61736D61 6E204472 6976652C 204D696C
70697461 732C2043 41203935 30333531 35303306 03550403 132C436F 6D323120
4361626C 65204D6F 64656D20 526F6F74 20436572 74696669 63617465 20417574
686F7269 7479301E 170D3030 30353038 30373030 30305A17 0D323530 35303830
37303030 305A3081 9D310B30 09060355 04061302 5553310E 300C0603 55040A13
05436F6D 3231310F 300D0603 55040B13 06444F43 53495331 36303406 0355040B
132D4C4F 43303030 332C2037 35302054 61736D61 6E204472 6976652C 204D696C
70697461 732C2043 41203935 30333531 35303306 03550403 132C436F 6D323120
4361626C 65204D6F 64656D20 526F6F74 20436572 74696669 63617465 20417574
686F7269 74793081 9F300D06 092A8648 86F70D01 01010500 03818D00 30818902
818100D9 C1A4199A 47D4FFAD B43F573C D1232742 748D2C91 B89E9FE9 94277008
FBA544C8 5CC4FE3F 754BA64B AEE5A362 32A41BFE B9FD03C2 99242D95 0508DC45
1A007021 FEC688F9 E57D9161 DE43E4EC 29379E9E 3AEB3563 455AF3B6 2C345A31
70F4FCF6 FB39FC6E 815F05CF EC6E618A 52562F26 098C5BE1 48FD46DE E07078A9
DD962902 03010001 300D0609 2A864886 F70D0101 05050003 8181001B DFAF32FD
38FF13E8 CD5063C6 4663D00A 2F3132FB 25D9F6DF 1CC67C1B 5CDB5F02 825F2DD2
72C07A3C 7EB0B138 F217E0BA CCBCF712 19AB117E 76193E86 3E7C8532 B44228A1
0E19643A B44D66B6 15F8F142 9ECF54F6 AFCA093E A6D59067 E3F9306C 5696BF5F
C34999A5 5F36F368 EAFAA8DD BAD93942 8620C59C 879EB625 88C3A1
quit
!
!
!
key chain ubr7246-rip
key 1
key-string 7 0600066C594C1B4F0E574345460133
!
!
interface FastEthernet0/0
ip address 192.168.10.130 255.255.255.0
duplex half
tag-switching ip
no cdp enable
!
interface Ethernet1/0
ip address 10.10.0.1 255.255.0.0
no ip redirects
no ip proxy-arp
ip pim dense-mode
no ip mroute-cache
duplex half
no keepalive
no cdp enable

```

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

```

cable upstream 4 minislots-size 4
cable upstream 4 modulation-profile 2
no cable upstream 4 shutdown
cable upstream 5 frequency 20000000
cable upstream 5 power-level 0
cable upstream 5 channel-width 1600000 1600000
cable upstream 5 minislots-size 4
cable upstream 5 modulation-profile 2
no cable upstream 5 shutdown
cable dhcp-giaddr policy
cable privacy accept-self-signed-certificate
cable privacy authenticate-modem
cable privacy authorize-multicast
cable privacy kek life-time 300
cable privacy tek life-time 180
no keepalive
!
interface Cable4/0
ip address 192.168.10.55 255.255.255.0
ip mask-reply
no ip redirects
no ip proxy-arp
ip multicast ttl-threshold 5
ip multicast boundary 15
ip route-cache flow
no ip mroute-cache
cable map-advance dynamic 400 1000
cable insertion-interval automatic 25 500
cable bundle 1
cable downstream annex B
cable downstream modulation 64qam
cable downstream interleave-depth 32
cable downstream channel-id 1
cable upstream 0 frequency 30000000
cable upstream 0 power-level 0
cable upstream 0 channel-width 1600000 1600000
cable upstream 0 minislots-size 4
cable upstream 0 modulation-profile 3
no cable upstream 0 shutdown
cable upstream 1 frequency 31008000
cable upstream 1 power-level 0
cable upstream 1 channel-width 1600000 1600000
cable upstream 1 minislots-size 4
cable upstream 1 modulation-profile 3
no cable upstream 1 shutdown
cable upstream 2 frequency 32000000
cable upstream 2 power-level 0
cable upstream 2 channel-width 1600000 1600000
cable upstream 2 minislots-size 4
cable upstream 2 modulation-profile 3
no cable upstream 2 shutdown
cable upstream 3 frequency 33008000
cable upstream 3 power-level 0
cable upstream 3 channel-width 1600000 1600000
cable upstream 3 minislots-size 4
no cable upstream 3 shutdown
cable upstream 4 frequency 34000000
cable upstream 4 power-level 0
cable upstream 4 channel-width 1600000 1600000
cable upstream 4 minislots-size 4
cable upstream 4 modulation-profile 3
no cable upstream 4 shutdown
cable upstream 5 frequency 35008000
cable upstream 5 power-level 0

```



```
cable upstream 5 channel-width 1600000 1600000
cable upstream 5 minislot-size 4
cable upstream 5 modulation-profile 3
no cable upstream 5 shutdown
cable source-verify leasetimer 5
cable dhcp-giaddr policy
cable privacy accept-self-signed-certificate
cable privacy authenticate-modem
cable privacy authorize-multicast
cable privacy kek life-time 300
cable privacy tek life-time 180
no keepalive
!
!
router rip
version 2
redistribute bgp 222 metric transparent
network 10.10.0.0
no auto-summary
!
!
ip default-gateway 192.168.100.1
ip classless
no ip forward-protocol udp netbios-ns
no ip forward-protocol udp netbios-dgm
no ip http server
no ip http secure-server
!
!
!
!
snmp-server community private RW
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps config
snmp-server enable traps cable
snmp-server enable traps docsis-cmts
snmp-server enable traps syslog
!
line con 0
exec-timeout 0 0
password 7 070C285F4D06
stopbits 1
line vty 0 4
session-timeout 60
exec-timeout 0 0
password 7 0703204E
line vty 5 15
!
scheduler allocate 4000 200
end
```

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

```
version 12.2
service timestamps log datetime msec localtime
service password-encryption
!
hostname uBR10012
!
redundancy
main-cpu
auto-sync standard
```

```

logging queue-limit 100
no logging buffered
no logging rate-limit
enable password my-enable-password
!
ipc cache 5000
card 1/1 2cable-tccplus
card 2/0 1gigetheretnet-1
card 2/1 2cable-tccplus
card 3/0 1gigetheretnet-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 cv_su
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 ool_cm
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 unreachable
 no ip proxy-arp
 load-interval 30
 negotiation auto
 no cdp enable
!
interface GigabitEthernet3/0/0
 no ip address
 ip pim sparse-mode
 no ip route-cache cef
 load-interval 30
 shutdown
 negotiation auto
 no cdp enable
!
interface POS4/0/0
 no ip address
 crc 32
 no cdp enable
 pos ais-shut
!
!
interface Cable8/0/0
 ip address 10.10.10.28 255.255.255.0
 ip helper-address 1.10.10.133
 cable bundle 2 master
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream frequency 669000000
 cable downstream channel-id 0
 no cable downstream rf-shutdown
 cable downstream rf-power 45
 cable upstream 0 connector 0
 cable upstream 0 spectrum-group 32
 cable upstream 0 power-level 0
 cable upstream 0 channel-width 1600000
 cable upstream 0 minislot-size 4
 cable upstream 0 range-backoff 3 6
 cable upstream 0 data-backoff 0 6
 cable upstream 0 modulation-profile 23
 no cable upstream 0 rate-limit
 no cable upstream 0 shutdown
 cable upstream 1 connector 1
 cable upstream 1 spectrum-group 32
 cable upstream 1 power-level 0
 cable upstream 1 channel-width 1600000
 cable upstream 1 minislot-size 4
 cable upstream 1 data-backoff 0 6
 cable upstream 1 modulation-profile 23
 no cable upstream 1 shutdown
 cable upstream 2 connector 2
 cable upstream 2 spectrum-group 32
 cable upstream 2 power-level 0
 cable upstream 2 channel-width 1600000
```

```

cable upstream 2 minislot-size 4
cable upstream 2 data-backoff 3 6
cable upstream 2 modulation-profile 23
no cable upstream 2 shutdown
cable upstream 3 connector 3
cable upstream 3 spectrum-group 32
cable upstream 3 channel-width 1600000
cable upstream 3 minislot-size 4
cable upstream 3 modulation-profile 21
no cable upstream 3 shutdown
cable source-verify
cable privacy kek life-time 300
cable privacy tek life-time 180
no keepalive
!
interface Cable8/0/1
ip address 10.10.11.121
cable bundle 2
cable downstream annex B
cable downstream modulation 64qam
cable downstream interleave-depth 32
cable downstream frequency 453000000
cable downstream channel-id 0
no cable downstream rf-shutdown
cable upstream max-ports 6
cable upstream 0 connector 4
cable upstream 0 spectrum-group 2
cable upstream 0 power-level 0
cable upstream 0 channel-width 1600000
cable upstream 0 minislot-size 4
cable upstream 0 range-backoff 3 6
cable upstream 0 data-backoff 0 6
cable upstream 0 modulation-profile 23 21
no cable upstream 0 rate-limit
cable upstream 0 shutdown
cable upstream 1 connector 5
cable upstream 1 channel-width 1600000
cable upstream 1 minislot-size 4
cable upstream 1 modulation-profile 21
cable upstream 1 shutdown
cable upstream 2 connector 6
cable upstream 2 channel-width 1600000
cable upstream 2 minislot-size 4
cable upstream 2 modulation-profile 21
cable upstream 2 shutdown
cable upstream 3 connector 7
cable upstream 3 channel-width 1600000
cable upstream 3 minislot-size 4
cable upstream 3 modulation-profile 21
cable upstream 3 shutdown
cable upstream 4 channel-width 1600000
cable upstream 4 minislot-size 4
cable upstream 4 modulation-profile 21
cable upstream 4 shutdown
cable upstream 5 channel-width 1600000
cable upstream 5 minislot-size 4
cable upstream 5 modulation-profile 21
cable upstream 5 shutdown
cable source-verify
cable privacy kek life-time 300
cable privacy tek life-time 180
no keepalive
!
!
```

```

ip classless
ip http server
no ip http secure-server
!
!
no cdp run
snmp-server community public RW
snmp-server community private RW
snmp-server enable traps cable
!
line con 0
  exec-timeout 0 0
line aux 0
line vty 0 4
  exec-timeout 0 0
  password my-telnet-password
  login
  length 0
!
end

```

Additional References

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

Related Documents

Related Topic	Document Title
Cable Command Reference Guide	For syntax and usage information on the cable-specific commands used in this chapter, see the “Cisco Cable Modem Termination System Commands” chapter of the <i>Cisco Broadband Cable Command Reference Guide</i> at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/cable/bbccmref/bbcmts.htm
DHCP Configuration	To configure the DHCP server onboard the Cisco CMTS, see the “Configuring DHCP” chapter in the “IP Addressing and Services” section of the <i>Cisco IOS IP and IP Routing Configuration Guide</i>, Release 12.2T at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipr_c/index.htm For information on all DHCP commands, see the “DHCP Commands” chapter in the <i>Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services</i>, Release 12.2T at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipras_r/index.htm

Related Topic	Document Title
HCCP N+1 Configuration	To configure the Cisco CMTS for N+1 redundancy, see the <i>N+1 Redundancy for the Cisco Cable Modem Termination System</i> chapter in the Cisco CMTS Feature Guide at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/cable/cab_rout/mtsfg/ufgnpls1.htm
NTP or SNTP Configuration	For information on configuring the Cisco CMTS to use Network Time Protocol (NTP) or Simple Network Time Protocol (SNTP) to set its system clock, see the “Performing Basic System Management” chapter in the “System Management” section of the <i>Cisco IOS Configuration Fundamentals Configuration Guide</i> , Release 12.2T, at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/ffun_c/fcfprt3/fcf012.htm
Software Configuration Guides	For information on configuring the CMTS router for cable operations, see the appropriate software configuration guide for your router. These guides are available for each router at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/cable/index.htm

Standards

Standards ¹	Title
SP-RFIV1.1-I08-020301	<i>Data-over-Cable Service Interface Specifications Radio Frequency Interface Specification</i>
SP-BPI+-I08-020301	<i>DOCSIS Baseline Privacy Interface Plus Specification</i>

1. Not all supported standards are listed.

MIBs

MIBs ¹	MIBs Link
- DOCS-BPI-PLUS-MIB - DOCS-CABLE-DEVICE-MIB (RFC 2669) - DOCS-CABLE-DEVICE-TRAP-MIB - DOCS-IF-EXT-MIB - DOCS-IF-MIB (RFC 2670) - DOCS-QOS-MIB - DOCS-SUBMGT-MIB - IGMP-STD-MIB (RFC 2933)	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

1. Not all supported MIBs are listed.

RFCs

RFCs ¹	Title
RFC 2669	DOCS-CABLE-DEVICE-MIB
RFC 2670	DOCS-IF-MIB
RFC 2933	IGMP-STD-MIB

1. Not all supported RFCs are listed.

Technical Assistance

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

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, TeleRouter, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0502R)

Copyright © 2003 Cisco Systems, Inc. All rights reserved.



EtherChannel for the Cisco Cable Modem Termination System

This document describes the features, benefits and configuration of Cisco EtherChannel technology on the Cisco Cable Modem Termination System (CMTS).

EtherChannel is a technology by which to configure and aggregate multiple physical Ethernet connections to form a single logical port with higher bandwidth. The first EtherChannel port configured on the Cisco CMTS serves as the EtherChannel bundle master by default, and each slave interface interacts with the network using the MAC address of the EtherChannel bundle master.

EtherChannel ports reside on a routing or bridging end-point. The router or switch uses EtherChannel to increase bandwidth utilization in either half- or full-duplex mode, and load balances the traffic across the multiple physical connections.

EtherChannel on the Cisco CMTS supports inter-VLAN routing with multiple devices and standards, and supports FastEtherChannel (FEC) and Gigabit EtherChannel (GEC) on the Cisco CMTS depending on the router and associated processing modules in the chassis.

Feature History for EtherChannel on the Cisco CMTS

Release	Modification
12.2(11)BC3	FEC and GEC support was introduced on the Cisco uBR7246VXR router with the NPE-G1 network processing engine required for GEC.
12.2(9a)BC	GEC support was introduced on the Cisco uBR10012 universal broadband router with the Cisco uBR10012 PRE2 performance routing engine.

Finding Support Information for Platforms and Cisco IOS Software Images

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



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

Copyright © 2004 Cisco Systems, Inc. All rights reserved.

Contents

- [Prerequisites for EtherChannel on the Cisco CMTS](#)
- [Restrictions for EtherChannel on the Cisco CMTS](#)
- [Information About EtherChannel on the Cisco CMTS](#)
- [How to Configure EtherChannel on the Cisco CMTS](#)
- [Additional References](#)
- [Command Reference for EtherChannel on the Cisco CMTS](#)
- [Glossary](#)

Prerequisites for EtherChannel on the Cisco CMTS

The Cisco uBR10012 universal broadband router has the following prerequisites to support GEC and 802.1Q encapsulation for inter-VLAN trunking, also summarized in [Table 1](#):

- Cisco IOS Release 12.2(9a)BC or a later BC release.
- The Cisco uBR10012 router supports only GEC with PRE2 performance routing engine modules.

The Cisco uBR7246VXR universal broadband router has the following prerequisites to support FEC or GEC and 802.1Q encapsulation for inter-VLAN trunking:

- Cisco IOS Release 12.2(11)BC3 or a later BC release.
- The Cisco uBR7246VXR router supports FEC on Fast Ethernet channels with the Cisco NPE-225 or Cisco NPE-400 network processing engines.
- The Cisco uBR7246VXR router supports GEC on Gigabit Ethernet channels using the Cisco uBR7200-NPE-G1 network processing engine.

Table 7 *Supported Interfaces and Encapsulations for EtherChannel on the Cisco CMTS*

Cisco CMTS	Full Duplex Supported	Encapsulation Supported	Cisco IOS Release
Cisco uBR7246VXR	Fast Ethernet with the Cisco NPE-225 or Cisco NPE-400	IEEE 802.1Q	12.2(11)BC3
	GigabitEthernet with the Cisco uBR7200-NPE-G1	IEEE 802.1Q	12.2(9a)BC
Cisco uBR10012	Gigabit Ethernet with the PRE2 Module	IEEE 802.1Q	12.2(9a)BC

Restrictions for EtherChannel on the Cisco CMTS

The following restrictions apply to both the Cisco uBR10012 and Cisco uBR7246VXR routers with Cisco IOS Release 12.2(9a)BC and earlier supported releases:

- EtherChannel on the Cisco CMTS is limited to Network Layer 3 functions, and does not support Data-Link Layer 2 EtherChannel functions as with certain other Cisco product platforms.
- The Port Aggregation Protocol (PAgP) is not supported on the Cisco CMTS as with other Cisco product platforms (such as the CatOS switch).
- Only the IEEE 802.1Q trunking protocol is supported on the Cisco CMTS. ATM trunking is not supported on the Cisco uBR10012 or Cisco uBR7246VXR routers as of this release.

Information About EtherChannel on the Cisco CMTS

Several Cisco product platforms currently support EtherChannel, such as the Cisco 7200 Series and Cisco Catalyst Switches. This document describes EtherChannel on the following Cisco CMTS router platforms:

- [Introduction to EtherChannel on the Cisco CMTS, page 131](#)
- [Cisco FastEtherChannel \(FEC\) and GigabitEtherChannel \(GEC\) on the Cisco uBR7246VXR Router, page 132](#)
- [Cisco GigabitEtherChannel \(GEC\) on the Cisco uBR10012 Router, page 132](#)

Introduction to EtherChannel on the Cisco CMTS

EtherChannel is based on proven industry-standard technology. The Cisco CMTS supports EtherChannel with several benefits, including the following:

- EtherChannel on the Cisco CMTS supports subsecond convergence times.
- EtherChannel can be used to connect two switch devices together, or to connect a router with a switch.
- A single EtherChannel connection supports a higher bandwidth between the two devices.
- The logical port channels on either Cisco CMTS platform provide fault-tolerant, high-speed links between routers, switches, and servers.
- EtherChannel offers redundancy and high availability on the Cisco CMTS. Failure of one connection causes a switch or router to use load balancing across the other connections in the EtherChannel.
- Load balancing on the Cisco CMTS supports dynamic link addition and removal without traffic interruption.
- EtherChannel supports inter-VLAN trunking. Trunking carries traffic from several VLANs over a point-to-point link between the two devices. The network provides inter-VLAN communication with trunking between the Cisco CMTS router and one or more switches. In a campus network, trunking is configured over an EtherChannel link to carry the multiple VLAN information over a high-bandwidth channel.

Cisco FastEtherChannel (FEC) and GigabitEtherChannel (GEC) on the Cisco uBR7246VXR Router

Cisco's Fast EtherChannel (FEC) technology builds upon standards-based 802.3 full-duplex Fast Ethernet to provide a reliable high-speed solution for network managers who require higher bandwidth between servers, routers, and switches than single-link Ethernet technology can provide.

Fast EtherChannel provides bandwidth scalability within the network backbone by providing increments from 200 Mbps to 800 Mbps with multi-gigabit capacity available on an increasing number of platforms.

Fast EtherChannel technology solves the immediate problem of scaling bandwidth within the network backbone, and can be applied to support Gigabit EtherChannels.

Cisco IOS Release 12.2(11)BC3 introduced support for Cisco EtherChannel technology for the Cisco uBR7246VXR router, and support continues with Cisco IOS Release 12.2(9a)BC. FEC on the Cisco uBR7246VXR router includes the following EtherChannel capabilities:

- Supports a maximum of four physical ports to be combined into one logical FEC or GEC link.
- Supports bandwidth up to 800 Mbps FEC (Fast EtherChannel full duplex) on the Cisco uBR7246VXR router.
- Supports bandwidth up to 4 Gbps GEC (Gigabit EtherChannel—half-duplex) for a combined total of up to 8 Gbps (full-duplex) with the Cisco uBR7200-NPE-G1 processor.

The Cisco uBR7200-NPE-G1 processor includes three onboard Gigabit Ethernet interfaces. If you want to use these interfaces to replace the Fast Ethernet interfaces on the existing I/O controller, you will have to configure the new interfaces before they can be used to access the network. If you are also removing the existing I/O controller, you remove the configuration for its Fast Ethernet interfaces.

The Cisco uBR7200-NPE-G1 contains its own onboard I/O controller, which includes the boot flash memory and NVRAM memory. After you install the Cisco uBR7200-NPE-G1 in a chassis, you can no longer access the boot flash and NVRAM memory on the I/O controller. You must therefore copy the Cisco IOS software image and configuration file to the memory on the Cisco uBR7200-NPE-G1.

Cisco GigabitEtherChannel (GEC) on the Cisco uBR10012 Router

Cisco GigabitEtherChannel (GEC) is high-performance Ethernet technology that provides gigabit-per-second transmission rates. It provides flexible, scalable bandwidth with resiliency and load sharing across links for switches, router interfaces, and servers.

Cisco IOS Release 12.2(9a)BC supports GigabitEtherChannel on the Cisco uBR10012 router with the following EtherChannel capabilities:

- Supports IEEE 802.1Q encapsulation for inter-VLAN networking.
- Supports a maximum of four physical Ethernet ports to be combined as one logical EtherChannel link.
- Supports bandwidth up to 4 Gbps GEC (Gigabit EtherChannel—half duplex) for a combined total of up to 8 Gbps (full duplex) on the Cisco uBR10012 router with PRE2 performance routing engine modules.

How to Configure EtherChannel on the Cisco CMTS

Refer to the following procedures to configure EtherChannel on the Cisco CMTS:

- [Cisco FastEtherChannel \(FEC\) and GigabitEtherChannel \(GEC\) on the Cisco uBR7246VXR Router, page 132](#)
- [“Verifying EtherChannel on the Cisco CMTS” section on page 136](#)
- [“Configuration Examples for EtherChannel on the Cisco CMTS” section on page 136](#)

Configuring FEC or GEC EtherChannel on the Cisco CMTS

This procedure describes and illustrates the configuration of EtherChannel FEC or GEC on the Cisco uBR7246VXR or Cisco uBR10012 routers, as described in [Table 7 on page 130](#).

Prerequisites

- Cisco IOS 12.2(9a)BC is installed or upgraded on either the Cisco uBR10012 or Cisco uBR7246VXR universal broadband router.
- Fast Ethernet or Gigabit Ethernet modules and interfaces are installed on the Cisco uBR7246VXR chassis as described in the [“Cisco FastEtherChannel \(FEC\) and GigabitEtherChannel \(GEC\) on the Cisco uBR7246VXR Router” section on page 4](#).
- PRE2 modules are installed in the Cisco uBR10012 router chassis as described in the [“Cisco GigabitEtherChannel \(GEC\) on the Cisco uBR10012 Router” section on page 132](#).
- Fast Ethernet or Gigabit Ethernet cabling is completed and the ports are operational on the router and network.
- LAN interfaces are configured and operational on the router and network, with IP addresses and subnet masks.

Restrictions

- The Cisco uBR7246VXR and Cisco uBR10012 routers support up to four physical connectors to be configured as one logical FEC or GEC port.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface port-channel** *number*
4. **exit**
5. **interface gigabitethernet** *slot/{subslot}/port*
or
6. **interface fastethernet** *slot/{subslot}/port*
7. **shutdown**
8. **channel-group** *number*
9. **no shutdown**
10. **Ctrl-Z**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	interface port-channel <i>n</i> Example: Router(config)# interface port-channel 1	Creates an EtherChannel interface. The first EtherChannel interface configured becomes the bundle master for all ports in the EtherChannel group. The MAC address of the first EtherChannel interface is the MAC address for all EtherChannel interfaces in the group. <i>n</i>—EtherChannel port number for the specified port. The EtherChannel port number may range from 1 to 64. To remove an EtherChannel interface from the EtherChannel group, use the no form of this command. For illustration, the example at left names the interface Port-channel11 . If the first EtherChannel interface in the group is later removed, the second EtherChannel interface in the group becomes the bundle master by default. Repeat this step on every EtherChannel port to be bundled into a FEC or GEC group. This configuration must be present on all EtherChannel interfaces before the EtherChannel group can be configured.
Step 4	exit Example: Router(config-if)# exit	Exits interface configuration mode for Port-channel11 and returns to global configuration mode.
Step 5	interface gigabitethernet slot/{subslot}/port Example: Router# interface gigabitethernet 1/0/0	(Gigabit Ethernet interface only) Selects the Gigabit Ethernet interface that you wish to add as a member EtherChannel link in the EtherChannel bundle, and enters interface configuration mode. The Cisco CMTS Cisco uBR10012 and Cisco uBR7246VXR routers differ in slot selection as follows: <i>slot/subslot/port</i>—Cisco uBR10012 router <i>slot/port</i>—Cisco uBR7246VXR router Note Cisco recommends that the link being added to the Cisco CMTS EtherChannel be shut down prior to configuring it as a member of the EtherChannel. Use the shutdown command in interface configuration mode immediately before completing the following steps in this procedure.

	Command or Action	Purpose
Step 6	interface fastethernet <i>slot/(subslot)port</i> Example: Router# interface fastethernet 3/0	(Fast Ethernet interface only) Selects a Fast Ethernet interface and enters interface configuration mode. Note The Cisco CMTS Cisco uBR10012 and Cisco uBR7246VXR routers differ in slot selection as follows: – <i>slot/subslot/port</i>—Cisco uBR10012 router – <i>slot/port</i>—Cisco uBR7246VXR router
Step 7	shutdown Example: Router(config-if)# shutdown	Shuts down the interface selected in Step 5 or Step 6 above prior to configuring it as a member of the EtherChannel. Note Cisco recommends that the link being added to the Cisco CMTS EtherChannel be shut down prior to configuring it as a member of the EtherChannel.
Step 8	channel-group <i>number</i> Example: Router(config-if)# channel-group 1	Adds the current interface (Gigabit Ethernet or Fast Ethernet) to the EtherChannel Group, associating that interface with an EtherChannel link. • <i>number</i>—The identifying number for the EtherChannel group with which to associate this interface. An EtherChannel group can be identified in the range of 1 to 64, and each group can have up to four interfaces, only one of which is the master. To remove an EtherChannel group and the associated ports from the Cisco CMTS, use the no form of this command.
Step 9	no shutdown Example:	Enables the interface on which EtherChannel is configured.
Step 10	Ctrl-Z Example: Router(config)# Ctrl-z	Returns to privileged EXEC mode. IP traffic should be visible on the network with completion of the above steps.

Examples

See [Configuration Examples for EtherChannel on the Cisco CMTS, page 8](#).

Troubleshooting Tips

Once interface operations are confirmed (prior to this procedure), and EtherChannel configurations have been verified (next procedure), any difficulty experienced through the EtherChannel links may pertain to inter-VLAN or IP routing on the network, or perhaps very high bandwidth consumption.

See the “[Additional References](#)” section on [page 10](#) for further resources in troubleshooting these and additional configurations.

What to Do Next

Additional IP, access list, inter-VLAN or load balancing configurations may be made to the Cisco CMTS and these changes will be supported in the running EtherChannel configuration without service disruption from EtherChannel. Refer to the “[Additional References](#)” section on [page 11](#) for more information.

Verifying EtherChannel on the Cisco CMTS

Links can be added or removed from an EtherChannel interface without traffic interruption. If an Ethernet link in an EtherChannel interface fails, traffic previously carried over the failed link switches to the remaining links within the EtherChannel. There are a number of events that can cause a link to be added or removed including adding or removing a link using Cisco IOS commands and simulating link failure and recovery (as with (no)shutdown links).

Cisco EtherChannel supports online insertion and removal (OIR) of field-replaceable units (FRUs) in the Cisco CMTS chassis. Ports that remain active during OIR of one FRU will take over and support the traffic bandwidth requirements without service disruption. However, OIR is not described in this procedure. Refer to the “[Additional References](#)” section on [page 10](#) for complete OIR procedures and guidelines for the respective FRU.

SUMMARY STEPS

- 1. enable
- 2. show interface port-channel channel-id

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	show interface port-channel n Example: Router# show interface port-channel 1	Verifies the EtherChannel configuration on the Cisco CMTS for the selected EtherChannel group. • <i>n</i>—The identifying number for the Port Channel group to display.

Configuration Examples for EtherChannel on the Cisco CMTS

The sequential configuration example and commands in [Table 2](#) illustrate the configuration of Etherchannel on a Cisco uBR7246VXR router with a five-port sensor:

The following example illustrates Gigabit EtherChannel (GEC) information for the port-channel interface of 2 as configured on a Cisco uBR10012 router with the PRE2 performance routing engine model.

This configuration is comprised of three GEC port channels as follows:

- Member 0 is the GEC interface bundle master.
- Member 2 is the final slave interface in this GEC group.
- These three port-channel interfaces (members) comprise one GEC group that is set up with a GEC peer on the network.

Router# show interface port-channel 2


```

Port-channel2 is up, line protocol is up
  Hardware is GEChannel, address is 8888.8888.8888 (bia 0000.0000.0000)
  Internet address is 101.101.101.1/16
  MTU 1500 bytes, BW 3000000 Kbit, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
    No. of members in this channel: 3
    No. of configured members in this channel: 3
    No. of passive members in this channel: 0
    No. of active members in this channel: 3
      Member 0 : GigabitEthernet1/0/0 , Full-duplex, 1000Mb/s
      Member 1 : GigabitEthernet3/0/0 , Full-duplex, 1000Mb/s
      Member 2 : GigabitEthernet2/0/0 , Full-duplex, 1000Mb/s
    No. of Non-active members in this channel: 0
  Last input 00:00:02, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/225/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/120 (size/max)
  30 second input rate 17292000 bits/sec, 9948 packets/sec
  30 second output rate 17315000 bits/sec, 9935 packets/sec
    866398790 packets input, 3324942446 bytes, 0 no buffer
    Received 2 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    0 watchdog, 0 multicast, 0 pause input
    0 input packets with dribble condition detected
    866394055 packets output, 3323914794 bytes, 0 underruns
    0 output errors, 0 collisions, 0 interface resets
    0 babbles, 0 late collision, 0 deferred
    0 lost carrier, 0 no carrier, 0 pause output
    0 output buffer failures, 0 output buffers swapped out

```

The following example illustrates GEC information for the port-channel interface of 2 as configured on a Cisco uBR7246VXR router.

This configuration is comprised of three port-channel interfaces (members) as follows:

- Member 0 is the GEC interface bundle master.
- Member 2 is the final slave interface in this GEC group.
- These three port-channel interfaces (members) comprise one GEC group that is set up with a GEC peer on the network.

```

Router# show interfaces port-channel 2
Port-channel2 is up, line protocol is up
  Hardware is GEChannel, address is 000b.bf7d.9c01 (bia 000b.bf7d.9c00)
  Internet address is 101.101.101.2/16
  MTU 1500 bytes, BW 3000000 Kbit, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
    No. of members in this channel: 3
    No. of configured members in this channel: 3
    No. of passive members in this channel: 0
    No. of active members in this channel: 3
      Member 0 : GigabitEthernet0/3 , Full-duplex, 1000Mb/s
      Member 1 : GigabitEthernet0/2 , Full-duplex, 1000Mb/s
      Member 2 : GigabitEthernet0/1 , Full-duplex, 1000Mb/s
    No. of Non-active members in this channel: 0
  Last input 00:13:48, output never, output hang never
  Last clearing of "show interface" counters never

```

```

Input queue: 0/225/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/120 (size/max)
30 second input rate 17358000 bits/sec, 9999 packets/sec
30 second output rate 17359000 bits/sec, 10000 packets/sec
  868633935 packets input, 3809968911 bytes, 0 no buffer
  Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
  0 watchdog, 0 multicast, 0 pause input
  0 input packets with dribble condition detected
  868642883 packets output, 3811242413 bytes, 0 underruns
  2 output errors, 0 collisions, 0 interface resets
  0 babbles, 0 late collision, 0 deferred
  2 lost carrier, 0 no carrier, 0 pause output
  0 output buffer failures, 0 output buffers swapped out

```

The following example illustrates FastEtherChannel (FEC) information for the port channel interface of 1 as configured on a Cisco uBR7246VXR router.

This configuration is comprised of four port channel interfaces (members) as follows:

- Member 0
- Member 0 is the GEC interface bundle master.
- Member 3 is the final slave interface in this FEC group.
- These four port-channel interfaces (members) comprise one FEC group that is set up with an FEC peer on the network.

```

Router# show interfaces port-channel 1
Port-channel1 is up, line protocol is up
  Hardware is FEChannel, address is 000b.bf7d.9c1c (bia 000b.bf7d.9c00)
  Description: test
  Internet address is 100.100.100.1/24
  MTU 1500 bytes, BW 400000 Kbit, DLY 100 usec,
    reliability 255/255, txload 11/255, rxload 11/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
    No. of members in this channel: 4
    No. of configured members in this channel: 4
    No. of passive members in this channel: 0
    No. of active members in this channel: 4
      Member 0 : FastEthernet2/1 , Full-duplex, 100Mb/s
      Member 1 : FastEthernet2/0 , Full-duplex, 100Mb/s
      Member 2 : FastEthernet1/1 , Full-duplex, 100Mb/s
      Member 3 : FastEthernet1/0 , Full-duplex, 100Mb/s
    No. of Non-active members in this channel: 0
  Last input 00:14:48, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/300/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/160 (size/max)
  30 second input rate 17358000 bits/sec, 9998 packets/sec
  30 second output rate 17357000 bits/sec, 9998 packets/sec
    869366601 packets input, 3968956491 bytes
    Received 3 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    0 watchdog
    0 input packets with dribble condition detected
    868944538 packets output, 3876736548 bytes, 0 underruns
    0 output errors, 0 collisions, 0 interface resets
    0 babbles, 0 late collision, 0 deferred
    0 lost carrier, 0 no carrier

```

0 output buffer failures, 0 output buffers swapped out

Additional References

The following additional references are available for Cisco EtherChannel for the Cisco Cable Modem Termination System.

Related Documents

Related Topic	Document Title
EtherChannel for Cisco Products	• <i>Cisco EtherChannel</i> home page http://www.cisco.com/en/US/tech/tk389/tk213/tech_protocol_family_home.html • <i>Cisco EtherChannel Technology</i> white paper http://www.cisco.com/en/US/tech/tk389/tk213/technologies_white_paper09186a0080092944.shtml • <i>Fast EtherChannel</i> web page http://www.cisco.com/en/US/tech/tk389/tk213/tk225/tech_protocol_home.html • <i>Gigabit EtherChannel</i> web page http://www.cisco.com/en/US/tech/tk389/tk213/tk276/tech_protocol_home.html
Cisco uBR10012 Universal Broadband Router	• <i>Cisco uBR10012 Universal Broadband Router Hardware Installation Guide</i> http://www.cisco.com/univercd/cc/td/doc/product/cable/ubr10k/ubr10012/hig/index.htm • <i>Cisco uBR10012 Universal Broadband Router Performance Routing Engine Module</i> http://lbj.cisco.com/targets/ucdit/cc/td/doc/product/cable/ubr10k/ubr10012/frus/pre5096.htm • <i>Cisco uBR10012 OC-48 DPT/POS Interface Module (Installation and Configuration)</i> http://www.cisco.com/univercd/cc/td/doc/product/cable/ubr10k/ubr10012/frus/ub_oc48.htm http://www.cisco.com/univercd/cc/td/doc/product/cable/ubr10k/ubr10012/ub10ksw/oc48pre2.htm
Cisco uBR7246VXR Universal Broadband Router	• <i>Cisco uBR7200 Series Universal Broadband Router Hardware Installation Guide</i> http://www.cisco.com/univercd/cc/td/doc/product/cable/cab_rout/cr72hig/index.htm • <i>Cisco uBR7200-NPE-G1 Network Processing Engine</i> (Read Me First and White Paper) http://www.cisco.com/univercd/cc/td/doc/product/cable/cab_rout/cfig_nts/15066r.htm http://www.cisco.com/en/US/products/hw/modules/ps4917/products_white_paper09186a0080113728.shtml

Related Topic	Document Title
WAN and Inter-VLAN Routing with the Cisco CMTS	• “<i>Configuring LAN Interfaces</i>” chapter in the <i>Cisco IOS Interface Configuration Guide</i>, Release 12.2 http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/finter_c/icflanin.htm • <i>Transparent LAN Service (TLS) over Cable</i> Describes how to map a service ID (SID) to an ATM permanent virtual connection (PVC) or to an IEEE 802.1Q VLAN. http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122bc/122bc_11/sidatmpv.htm • <i>Cisco IOS Wide-Area Networking Configuration Guide</i>, Release 12.3 http://www.cisco.com/en/US/products/sw/iosswrel/ps5187/prod_configuration_guide09186a008017d137.html • <i>Point-to-Point Protocol over Ethernet Support on the Cisco CMTS</i> http://www.cisco.com/en/US/products/hw/cable/ps2217/products_feature_guide_chapter09186a008019b6ae.html • <i>Cisco IOS IEEE 802.1Q Support</i> http://www.cisco.com/en/US/products/sw/iosswrel/ps1830/products_feature_guide09186a008008742b.html • <i>ATM Multilink PPP Support on Multiple Virtual Circuits (VCs)</i> http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftatmmlt.htm • <i>Cisco New Virtual Circuit (VC) Configuration</i> http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113t/113t_2/pvcmgmt/vcconfig.htm • <i>Cisco IOS IP Configuration Guide</i>, Release 12.3 http://www.cisco.com/en/US/products/sw/iosswrel/ps5187/prod_configuration_guide09186a008017d581.html
Configuring Additional Devices for EtherChannel	• <i>Configuring EtherChannel and 802.1Q Trunking Between a Catalyst 2950 and a Router (inter-VLAN Routing)</i> http://www.cisco.com/en/US/products/hw/switches/ps628/products_configuration_example09186a00800ef797.shtml • <i>Configuring EtherChannel and 802.1Q Trunking Between Catalyst 2900XL/3500XL and Catalyst 2940, 2950/2955, and 2970 Switches</i> http://www.cisco.com/en/US/products/hw/switches/ps607/products_configuration_example09186a0080094789.shtml

Standards

Standards	Title
IEEE Std 802.1Q, 2003 Edition	IEEE Std 802.1Q, 2003 Edition (Incorporates IEEE Std 802.1Q-1998, IEEE Std 802.1u-2001, IEEE Std 802.1v-2001, and IEEE Std 802.1s-2002) http://ieeexplore.ieee.org/xpl/tocresult.jsp?isNumber=27089

MIBs

For additional information about MIBs for the Cisco CMTS, refer to the following resources on Cisco.com:

- *Cisco CMTS Universal Broadband Router MIB Specifications Guide*
<http://www.cisco.com/univercd/cc/td/doc/product/cable/cmtsmib/>
- *SNMP Object Navigator*
<http://www.cisco.com/cgi-bin/Support/Mibbrowser/unity.pl>

Technical Assistance

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

Command Reference for EtherChannel on the Cisco CMTS

This section describes the following Cisco IOS Software commands for Cisco IOS Release 12.2(9a)BC, as supported by the Cisco uBR10012 router or the Cisco uBR7246VXR routers:

- [channel-group](#)
- [interface port-channel](#)
- [show interface port-channel](#)

channel-group

To add an interface (Gigabit Ethernet or Fast Ethernet) to an EtherChannel Group, and to associate that interface with an EtherChannel link, use the **channel-group** command in interface configuration mode.

To remove an EtherChannel interface from the EtherChannel group, use the **no** form of this command.

channel-group *n*
no channel-group *n*

Syntax Description	<i>n</i>	The identifying number for the EtherChannel group with which to associate this interface. An EtherChannel group can be identified in the range of 1 to 64, and each group can have up to four interfaces, only one of which is the master.

Defaults	By default, the channel-group command has the following behaviors: - EtherChannel groups and ports are not defined. - EtherChannel groups and ports are disabled (off mode) once configured, and must be enabled. - The first port assigned to an EtherChannel group is the bundle master.

Command Modes	Interface configuration

Command History	Release	Modification
	12.2(11)BC3	This command was introduced on the Cisco uBR7246VXR router.
	12.2(9a)BC	This command was introduced on the Cisco uBR10012 router.

Usage Guidelines	The no form of this command also removes the associated EtherChannel ports within the EtherChannel group.

Examples	The following example creates an EtherChannel link with a channel group identifier of 1 on the specified port. If this is the first port assigned to EtherChannel group 1, it becomes the master in that EtherChannel group. <pre>Router(config-if)# channel-group etherchannel 1</pre>

Related Commands	Command	Description
	show interface port-channel	Displays the EtherChannel interfaces and channel identifiers, with their mode and operational status.

interface port-channel

To create an EtherChannel interface on the Cisco Cable Modem Termination System (CMTS), use the **interface port-channel** command in global configuration mode. To remove this EtherChannel port from the Cisco CMTS, use the **no** form of this command.

interface port-channel *n*

no interface port-channel *n*

Syntax Description

<i>number</i>	Identifying port channel number for this interface (EtherChannel port). The range is 1 to 64.

Defaults

By default, EtherChannel groups and ports are not defined, and they are disabled (**off** mode) configured.

Command Modes

Global configuration

Command History

Release	Modification
12.2(11)BC3	This command was introduced on the Cisco uBR7246VXR router.
12.2(9a)BC	This command was introduced on the Cisco uBR10012 router.

Usage Guidelines

The first EtherChannel interface configured becomes the bundle master for all EtherChannel interfaces in the group. That is, the MAC address of the first EtherChannel interface is the MAC address for all EtherChannel interfaces in the group. If the first EtherChannel interface is later removed, the second EtherChannel interface to be configured becomes the bundled master by default.

Repeat this configuration on every EtherChannel port to be bundled into a FastEtherChannel (FEC) or GigabitEtherChannel (GEC) group. This configuration must be present on all EtherChannel interfaces before the EtherChannel group can be configured.

Examples

The following example configures the port to have an EtherChannel port number of 1 within its EtherChannel group. The EtherChannel group is defined with the **channel-group** command.

```
Router(config-if)# interface port-channel 1
```

Related Commands

Command	Description
channel-group	Assigns an EtherChannel port to an EtherChannel group.
show interface port-channel	Displays the EtherChannel interfaces and channel identifiers, with their mode and operational status.

show interface port-channel

To display the EtherChannel interfaces and channel identifiers, with their mode and operational status, use the **show interface port-channel** command in privileged EXEC mode.

```
show interface port-channel {number}
```

Syntax Description	<i>number</i>	Optional value enables the display of information for one port channel interface number. The range is from 1 to 64.

Defaults	No default behaviors or values.

Command Modes	Privileged EXEC

Command History	Release	Modification
	12.2(11)BC3	This command was introduced on the Cisco uBR7246VXR router.
	12.2(9a)BC	This command was introduced on the Cisco uBR10012 router.

The following example illustrates Gigabit EtherChannel (GEC) information for the port-channel interface of 2 as configured on a Cisco uBR10012 router with the PRE2 performance routing engine model.

This configuration is comprised of three GEC port channels as follows:

- Member 0 is the GEC interface bundle master.
- Member 2 is the final slave interface in this GEC group.
- These three port-channel interfaces (members) comprise one GEC group that is set up with a GEC peer on the network.

```
Router# show interface port-channel 2
Port-channel2 is up, line protocol is up
  Hardware is GEChannel, address is 8888.8888.8888 (bia 0000.0000.0000)
  Internet address is 101.101.101.1/16
  MTU 1500 bytes, BW 3000000 Kbit, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
    No. of members in this channel: 3
    No. of configured members in this channel: 3
    No. of passive members in this channel: 0
    No. of active members in this channel: 3
      Member 0 : GigabitEthernet1/0/0 , Full-duplex, 1000Mb/s
      Member 1 : GigabitEthernet3/0/0 , Full-duplex, 1000Mb/s
      Member 2 : GigabitEthernet2/0/0 , Full-duplex, 1000Mb/s
    No. of Non-active members in this channel: 0
  Last input 00:00:02, output never, output hang never
  Last clearing of "show interface" counters never
```

```

Input queue: 0/225/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/120 (size/max)
30 second input rate 17292000 bits/sec, 9948 packets/sec
30 second output rate 17315000 bits/sec, 9935 packets/sec
 866398790 packets input, 3324942446 bytes, 0 no buffer
Received 2 broadcasts, 0 runts, 0 giants, 0 throttles
 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
 0 watchdog, 0 multicast, 0 pause input
 0 input packets with dribble condition detected
866394055 packets output, 3323914794 bytes, 0 underruns
 0 output errors, 0 collisions, 0 interface resets
 0 babbles, 0 late collision, 0 deferred
 0 lost carrier, 0 no carrier, 0 pause output
 0 output buffer failures, 0 output buffers swapped out

```

The following example illustrates GEC information for the port-channel interface of 2 as configured on a Cisco uBR7246VXR router.

This configuration is comprised of three port-channel interfaces (members) as follows:

- Member 0 is the GEC interface bundle master.
- Member 2 is the final slave interface in this GEC group.
- These three port-channel interfaces (members) comprise one GEC group that is set up with a GEC peer on the network.

```

Router# show interfaces port-channel 2
Port-channel2 is up, line protocol is up
  Hardware is GEChannel, address is 000b.bf7d.9c01 (bia 000b.bf7d.9c00)
  Internet address is 101.101.101.2/16
  MTU 1500 bytes, BW 3000000 Kbit, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
    No. of members in this channel: 3
    No. of configured members in this channel: 3
    No. of passive members in this channel: 0
    No. of active members in this channel: 3
      Member 0 : GigabitEthernet0/3 , Full-duplex, 1000Mb/s
      Member 1 : GigabitEthernet0/2 , Full-duplex, 1000Mb/s
      Member 2 : GigabitEthernet0/1 , Full-duplex, 1000Mb/s
    No. of Non-active members in this channel: 0
  Last input 00:13:48, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/225/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/120 (size/max)
 30 second input rate 17358000 bits/sec, 9999 packets/sec
 30 second output rate 17359000 bits/sec, 10000 packets/sec
 868633935 packets input, 3809968911 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
 0 watchdog, 0 multicast, 0 pause input
 0 input packets with dribble condition detected
868642883 packets output, 3811242413 bytes, 0 underruns
 2 output errors, 0 collisions, 0 interface resets
 0 babbles, 0 late collision, 0 deferred
 2 lost carrier, 0 no carrier, 0 pause output
 0 output buffer failures, 0 output buffers swapped out

```

The following example illustrates FastEtherChannel (FEC) information for the specified port channel interface as configured on a Cisco uBR7246VXR router.

This configuration is comprised of four port channel interfaces (members) as follows:

- Member 0
- Member 0 is the GEC interface bundle master.
- Member 3 is the final slave interface in this FEC group.
- These four port-channel interfaces (members) comprise one FEC group that is set up with an FEC peer on the network.

```
Router# show interfaces port-channel 1
Port-channel1 is up, line protocol is up
  Hardware is FEChannel, address is 000b.bf7d.9c1c (bia 000b.bf7d.9c00)
  Description: test
  Internet address is 100.100.100.1/24
  MTU 1500 bytes, BW 400000 Kbit, DLY 100 usec,
    reliability 255/255, txload 11/255, rxload 11/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
    No. of members in this channel: 4
    No. of configured members in this channel: 4
    No. of passive members in this channel: 0
    No. of active members in this channel: 4
      Member 0 : FastEthernet2/1 , Full-duplex, 100Mb/s
      Member 1 : FastEthernet2/0 , Full-duplex, 100Mb/s
      Member 2 : FastEthernet1/1 , Full-duplex, 100Mb/s
      Member 3 : FastEthernet1/0 , Full-duplex, 100Mb/s
    No. of Non-active members in this channel: 0
  Last input 00:14:48, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/300/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/160 (size/max)
  30 second input rate 17358000 bits/sec, 9998 packets/sec
  30 second output rate 17357000 bits/sec, 9998 packets/sec
    869366601 packets input, 3968956491 bytes
    Received 3 broadcasts, 0 runs, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    0 watchdog
    0 input packets with dribble condition detected
    868944538 packets output, 3876736548 bytes, 0 underruns
    0 output errors, 0 collisions, 0 interface resets
    0 babbles, 0 late collision, 0 deferred
    0 lost carrier, 0 no carrier
    0 output buffer failures, 0 output buffers swapped out
```

Related Commands

Command	Description
channel-group	Creates an EtherChannel group and link, through which all port-channel interfaces interoperate with the network.
interface port-channel	Creates an EtherChannel interface on the Cisco CMTS.

Glossary

ACL

Access Control List. A list kept by routers to control access to or from the router for a number of services (for example, to prevent packets with a certain IP address from leaving a particular interface on the router).

CLI

command-line interface. An interface that allows the user to interact with the operating system by entering commands and optional arguments. The UNIX operating system and DOS provide CLIs.

EtherChannel

Developed and copyrighted by Cisco Systems. Logical aggregation of multiple Ethernet interfaces used to form a single higher bandwidth routing or bridging endpoint.

ICMP

Internet Control Message Protocol. Network layer Internet protocol that reports errors and provides other information relevant to IP packet processing. Documented in RFC 792.

MTU

maximum transmission unit. Maximum packet size, in bytes, that a particular interface can handle.

NMS

network management system. System responsible for managing at least part of a network. An NMS is generally a reasonably powerful and well-equipped computer, such as an engineering workstation. NMSs communicate with agents to help keep track of network statistics and resources.

OIR

online insertion and removal. Feature that permits the addition, the replacement, or the removal of cards without interrupting the system power, entering console commands, or causing other software or interfaces to shutdown.

RPF

Reverse Path Forwarding. Multicasting technique in which a multicast datagram is forwarded out of all but the receiving interface if the receiving interface is the one used to forward unicast datagrams to the source of the multicast datagram.

SNMP

Simple Network Management Protocol. Network management protocol used almost exclusively in TCP/IP networks. SNMP provides a means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security.

VLAN

virtual local area network (LAN). Group of devices on one or more LANs that are configured (using management software) so that they can communicate as if they were attached to the same wire, when in fact they are located on a number of different LAN segments. Because VLANs are based on logical instead of physical connections, they are extremely flexible.

VPN

virtual private network. Enables IP traffic to travel securely over a public TCP/IP network by encrypting all traffic from one network to another. A VPN uses "tunneling" to encrypt all information at the IP level.

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, TeleRouter, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0502R)

Copyright © 2004 Cisco Systems, Inc. All rights reserved.



Flap List Troubleshooting for the Cisco CMTS

This document describes how to configure and use the Flap List Troubleshooting feature on the Cisco Cable Modem Termination System (CMTS) routers. The flap list is a patented tool for the Cisco CMTS routers to diagnose potential problems with a particular cable modem or with a particular cable interface. The flap list tracks “flapping” cable modems, which are cable modems that have intermittent connectivity problems. Excessive flapping could indicate a problem with a particular cable modem or with the upstream or downstream portion of the cable plant.

Feature Specifications for Flap List Troubleshooting

Feature History

Release	Modification
Release 11.3 NA	This feature was introduced on the Cisco uBR7200 series routers.
Release 12.0(4)XA	The <i>days</i> parameter was removed from the cable flap-list aging command.
Release 12.0(7)XR, 12.1(2)EC	The output of show cable flap-list command was enhanced to show when the Cisco uBR7200 series router has detected an unstable return path for a particular CM and has made an automated power adjustment.
Release 12.1(5)EC	This feature was supported on the Cisco uBR7100 series routers.
Release 12.1(7)CX	The ccsFlapClearAll attribute was added to the ccsFlapTable table in the CISCO-CABLE-SPECTRUM-MIB MIB.
12.2(4)BC1	This feature was supported on the Release 12.2 BC train for all Cisco CMTS platforms. The show cable modem flap command was also introduced to display flap-list information for individual cable modems.

Supported Platforms

Cisco uBR7100 series, Cisco uBR7200 series, Cisco uBR10012 universal broadband routers.

Finding Support Information for Platforms and Cisco IOS Software Images

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

Contents

- [Prerequisites for Flap List Troubleshooting, page 152](#)
- [Restrictions for Flap List Troubleshooting, page 152](#)
- [Information About Flap List Troubleshooting, page 152](#)
- [How to Configure Flap List Troubleshooting, page 155](#)
- [How to Monitor and Troubleshoot Using Flap Lists, page 162](#)
- [Configuration Examples for Flap List Troubleshooting, page 171](#)
- [Additional References, page 172](#)

Prerequisites for Flap List Troubleshooting

- To configure and access the flap list using SNMP commands, you must be using an SNMPv3 manager and have configured the Cisco CMTS router for SNMP operations.

Restrictions for Flap List Troubleshooting

- The Cisco CMTS should be running the latest Cisco IOS Release 12.1 EC or Cisco IOS Release 12.2 EC, or later, release.
- The Flap List Troubleshooting feature can be used only with two-way cable modems. The flap-list does not support telco-return cable modems or set-top boxes.

**Note**

Since the cable flap list was originally developed, polling mechanisms have been enhanced to have an increased rate of 1/sec when polls are missed. Cable modems can go offline faster than the frequency hop period, which can cause the frequency to stay fixed while cable modems go offline. To compensate for this, reduce the hop period to 10 seconds.

Information About Flap List Troubleshooting

This section describes the following information about the Flap List Troubleshooting feature:

- [Feature Overview, page 153](#)
- [Information in the Flap List, page 153](#)
- [Cisco Cable Manager and Cisco Broadband Troubleshooter, page 154](#)
- [Benefits, page 155](#)

Feature Overview

The Flap List Troubleshooting is a patented tool that is incorporated in the Cisco IOS software for the Cisco Cable Modem Termination System (CMTS) universal broadband routers. The flap list tracks “flapping” cable modems, which are cable modems that have intermittent connectivity problems. A flapping cable modem can indicate either a problem with that particular cable modem, or it could indicate an RF noise problem with the upstream or downstream portion of the cable plant.

The flap-list feature supports any cable modem that conforms to the Data-over-Cable Service Interface Specifications (DOCSIS) because it does not use any special messaging to poll cable modems or to request any special information from them. Instead, this feature monitors the normal registration and station maintenance activity that is already performed over a DOCSIS cable network.

This allows the Cisco CMTS to collect the flap-list data without generating additional packet overhead and without impacting network throughput and performance. It also means that although the Flap List Troubleshooting feature is a proprietary feature for Cisco CMTS routers, it is compatible with all DOCSIS-compliant cable modems. In addition, unlike other monitoring methods that use the Simple Network Management Protocol (SNMP), the flap list uses zero bandwidth.

Information in the Flap List

The Flap List Troubleshooting feature tracks the following situations:

- **Reinsertions**—A reinsertion occurs when the cable modem re-registers more frequently than the user-specified insertion time. A pattern of reinsertions can indicate either potential problems in the downstream or that the cable modem is being improperly provisioned.
- **Hits and Misses**—A hit occurs when a cable modem successfully responds to the station maintenance messages (MAC-layer “keepalive” messages) that the Cisco CMTS sends out to conform to the DOCSIS standard. A miss occurs when the cable modem does not respond to the request within the user-specified timeout period. A pattern of misses can indicate a potential problem in either the downstream or upstream path, or that a problem can be occurring in the registration process.
- **Power Adjustments**—DOCSIS cable modems can adjust their upstream transmission power levels to adjust to unstable cable plant signal levels, up to a maximum allowable power level. Repeated power adjustments usually indicate a problem with an amplifier in the upstream return path.

The flap-list feature is automatically enabled, but to use the flap list effectively, the cable system administrator should also typically do the following:

- Set up a script to periodically poll the flap list, for example, every 15 minutes.
- Examine the resulting data and perform trend analysis to identify cable modems that are consistently in the flap list.
- Query the billing and administrative database for cable modem MAC address-to-street address translation and generate a report. The reports can be given to the customer service department or the cable plant’s operations and maintenance department. Using these reports, maintenance personnel can quickly discern how characteristic patterns of flapping cable modems, street addresses, and flap statistics indicate which amplifier or feeder lines are faulty. The reports also help to quickly discern whether problems exist in your downstream or upstream path and whether the problem is ingress noise or equipment related.

The flap list provides a quick way to quickly diagnose a number of possible problems. For example, if a subscriber reports a problem, but the flap list for the cable interface that is providing services to them shows little or no flap-list activity, the cable technician can assume that the Cisco CMTS and cable plant are communicating reliably. The problem, therefore, is probably in the subscriber's computer equipment or in the local connection to the cable modem.

Similarly, a cable technician can use the pattern of reinsertions, hits and misses, and power adjustments to quickly troubleshoot the following types of problems:

- If a subscriber's cable modem shows a lot of flap-list activity, it is having some kind of communication problem. Either the cable modem's hardware is faulty, its installation is faulty, the coaxial cable being used is faulty, or some portion of the cable plant that services this cable modem is faulty.
- Focus on the top 10 percent of cable modems that are most active in the flap list, since these are the most likely to indicate consistent and pervasive plant or equipment problems that will continue to disrupt communication with the headend.
- Cable modems with more than 50 power adjustments per day have a suspect upstream path.
- Cable modems with approximately the same number of hits and misses and with a lot of insertions have a suspect downstream path (for example, low level into the cable modem).
- All cable modems incrementing the insertion at the same time indicates a problem with the provisioning servers.
- Cable modems with high cyclic redundancy check (CRC) errors have bad upstream paths or in-home wiring problems.
- Correlating cable modems on the same physical upstream port with similar flap-list statistics can quickly resolve outside plant problems to a particular node or geography.

In addition, the cable network administrators can use the flap list to collect quality control and upstream performance data. Typically, the network operations center (NOC) saves the flap list to a database on a local computer on a daily basis, providing the ability to generate reports that track upstream performance and installation quality control, as well as to provide trend reports on cable plant problems.



Tip

The system supports automatic power adjustments. The **show cable flap-list** and **show cable modem** commands indicate when the headend cable router has detected an unstable return path for a particular modem and has compensated with a power adjustment. An asterisk (*) appears in the power-adjustment field for a modem when a power adjustment has been made; an exclamation point (!) appears when the modem has reached its maximum power-transmit level and cannot increase its power level any further.

Cisco Cable Manager and Cisco Broadband Troubleshooter

The Flap List Troubleshooting feature is supported by Cisco Cable Manager (CCM), Release 2.0 or later, which is a UNIX-based software suite that manages routers and DOCSIS-compliant cable modems, generates performance reports, troubleshoots connectivity problems, views the network graphically, and edits DOCSIS configuration files. You can access the CCM locally from the CCM server console or remotely from a UNIX workstation or a PC.

The Flap List Troubleshooting feature also works together with the Cisco Broadband Troubleshooter (CBT), which is a graphical-based application to manage and diagnose problems on the hybrid fiber-coaxial (HFC) network. Radio frequency (RF) technicians can quickly isolate plant and provisioning problems and characterize upstream and downstream trouble patterns, including analyzing flapping modems.

Benefits

The Flap List Troubleshooting feature is a proactive way to manage and troubleshoot problems on an HFC network. Its use of passive monitoring is more scalable and efficient than techniques that send special messages to cable modems or that regularly poll the cable modems using Simple Network Management Protocol (SNMP) commands. Because it uses mechanisms that already exist in a DOCSIS network, it can be used with any DOCSIS-certified cable modem or set-top box.

The flap list provides a cable technician with both real-time and historical cable health statistics for quick, accurate problem isolation and network diagnosis. Using the flap list, a cable technician is able to do the following:

- Quickly learn how to characterize trouble patterns in the hybrid fiber-coaxial (HFC) network.
- Determine which amplifier or feeder line is faulty.
- Distinguish an upstream path problem from a downstream one.
- Isolate an ingress noise problem from a plant equipment problem.

How to Configure Flap List Troubleshooting

This section describes how to configure the flap list operation on the Cisco CMTS. You can use either the command-line interface (CLI) commands or Simple Network Management Protocol (SNMP) commands to configure the flap list, to remove a cable modem from the list, or to clear the flap-list counters.

- [Configuring Flap List Operation Using the CLI \(optional\), page 155](#)
- [Clearing the Flap List and Counters Using the CLI \(optional\), page 157](#)
- [Enabling or Disabling Power Adjustment Using the CLI \(optional\), page 158](#)
- [Configuring Flap List Operation Using SNMP \(optional\), page 161](#)
- [Clearing the Flap List and Counters Using SNMP \(optional\), page 161](#)

Configuring Flap List Operation Using the CLI (optional)

To configure the operation of the flap list, use the following procedure, beginning in EXEC mode. This procedure is optional, unless you want to change the default values for the flap list.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cable flap-list insertion-time** *seconds*
4. **cable flap-list power-adjust threshold** *db*
5. **cable flap-list miss-threshold** *misses*
6. **cable flap-list aging** *minutes*
7. **cable flap-list size** *number*
8. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable Router#	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal Router(config)#	Enters global configuration mode.
Step 3	 cable flap-list insertion-time <i>seconds</i> Example: Router(config)# cable flap-list insertion-time 3600 Router(config)#	(Optional) Specifies the minimum insertion (registration) time interval in seconds. Any cable modem that makes a registration request more frequently than this period of time is placed in the flap list. The valid range is from 60 to 86400 seconds, with a default of 180 seconds.
Step 4	 cable flap-list power-adjust threshold <i>db</i> Example: Router(config)# cable flap-list power-adjust threshold 5 Router(config)#	(Optional) Specifies the minimum power adjustment, in dB, that constitutes a flap-list event. The valid range is from 1 to 10 dB, with a default of 2 dB. (See the “Enabling or Disabling Power Adjustment Using the CLI (optional)” section on page 158.) Note A threshold of less than 2 dB can cause excessive flap-list event recording. If you need to change this parameter from its default, Cisco recommends setting it to 3 dB or higher.
Step 5	 cable flap-list miss-threshold <i>misses</i> Example: Router(config)# cable flap-list miss-threshold 10 Router(config)#	(Optional) Specifies the number of MAC-layer station maintenance (keepalive) messages that can be missed in succession before the CMTS places the cable modem in the flap list. The valid range is 1 to 12, with a default of 6. Note A high miss rate indicates potential plant problems, such as intermittent upstream problems, fiber laser clipping, or common-path distortion.
Step 6	 cable flap-list aging <i>minutes</i> Example: Router(config)# cable flap-list aging 20160 Router(config)#	(Optional) Specifies how long, in minutes, the Cisco CMTS should keep information for cable modems in the flap list. The valid range is from 1 to 86400 minutes, with a default of 10080 minutes (1 week).

	Command or Action	Purpose
Step 7	command <code>flap-list size number</code> Example: Router(config)# <code>cable flap-list size 4000</code> Router(config)#	Specifies the maximum number of cable modems that can be kept in the flap list. The valid range is from 1 to 8191 cable modems, with a default of 100 cable modems. Tip To avoid wasting processor memory, do not set this value beyond the actual number of cable modems being serviced by the Cisco CMTS.
Step 8	command <code>exit</code> Example: Router(config)# <code>exit</code> Router#	Exits global configuration mode.

Clearing the Flap List and Counters Using the CLI (optional)

To clear one or more cable modems from the flap list, or to clear the flap list counters for one or more cable modems (while still keeping the modems in the flap list), use the following procedure, beginning in EXEC mode.

SUMMARY STEPS

1. **enable**
2. **clear cable flap-list** {*mac-addr* | **all**} [**save-counters**]
3. **clear cable modem** {*mac-addr* | *ip-addr* | [**cable slot/port**] {**all** | *oui string* | **reject**} } **counters**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable Router#	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	clear cable flap-list { <i>mac-addr</i> all } [save-counters] Example: Router# clear cable flap-list 0102.0304.0506 save-counters Router# clear cable flap-list 000C.0102.0304 Router#	Clears one or all cable modems from the flap list: • <i>mac-addr</i> = Removes the cable modem with this specific MAC address from the flap-list table. • all = Removes all CMs from the flap-list table. • save-counters = (Optional) Preserves the flap-list counters that are displayed by the show cable flap-list command and by SNMP commands that access the CISCO-CABLE-SPECTRUM-MIB MIB.
Step 3	clear cable modem { <i>mac-addr</i> <i>ip-addr</i> [cable interface] { all <i>oui string</i> reject } } counters Example: Router# clear cable modem 172.12.23.45 counters Router# clear cable modem oui Cisco counters Router# clear cable modem reject counters Router# clear cable modem c4/0 counters Router#	Sets the flap-list counters to zero for one or more CMs: • <i>mac-addr</i> = Resets the counters for the CM with this specific MAC address. • <i>ip-addr</i> = Resets the counters for the CM with this specific IP address. • cable interface = Resets the counters for all CMs on this specific cable interface. • all = Resets the counters for all CMs. • oui string = Resets the counters for all CMs that match the specified Organization Unique Identifier (OUI). The <i>string</i> parameter can be either the three byte hexadecimal string (such as 00.00.0C) or a vendor name that has been defined using the cable modem vendor command. • reject = Resets the flapping counters for all CMs that are currently in one of the reject states (see the show cable modem command).

Enabling or Disabling Power Adjustment Using the CLI (optional)

The Cisco CMTS can automatically monitor a cable modem's power adjustments and determine whether a particular cable modem requires a change in the power adjustment method. To enable a cable interface to make automatic power adjustments, and to set the frequency threshold for when those adjustments are made, use the following procedure, beginning in EXEC mode.

SUMMARY STEPS

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

3. **interface cable** *x/y*
4. **cable upstream** *n* **power-adjust**
{**continue** *pwr-level* | **noise** *perc-pwr-adj* | **threshold** *value*}
5. **cable upstream** *n* **freq-adj averaging** *percent*
6. **exit**
7. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable Router#	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal Router(config)#	Enters global configuration mode.
Step 3	interface cable <i>x/y</i> Example: Router(config)# interface cable 4/0 Router(config-if)#	Enters cable interface configuration mode for the specified cable interface.
Step 4	cable upstream <i>n</i> power-adjust { continue <i>pwr-level</i> noise <i>perc-pwr-adj</i> threshold <i>value</i> } Example: Router(config-if)# cable upstream 0 power-adjust threshold 2 Router(config-if)# cable upstream 0 power-adjust noise 50 Router(config-if)#	Enables automatic power adjustment on an upstream port for this cable interface: <i>n</i> = Specifies the upstream port number. Valid values start with 0 for the first upstream port on the cable interface line card. continue <i>pwr-level</i> = Specifies the power threshold value that determines the value of the Ranging Status field in the Ranging Response (RNG-RSP) messages that the CMTS sends to the CM. The valid range is from 2 to 15 dB, with a default of 2 dB. threshold <i>value</i> = Specifies the power adjustment threshold. The threshold range is from 0 to 10 dB, with a default of 1 dB. noise <i>perc-pwr-adj</i> = Specifies the percentage of power adjustment packets that is required to enable automatic power adjustments, which use an averaging algorithm to smooth out wide jumps in the power level. The valid range is 10 to 100 percent, with a default of 30 percent.

Note Repeat [Step 4](#) for each upstream port on the cable interface.

	Command or Action	Purpose
Step 5	cable upstream <i>n</i> freq-adj averaging <i>percent</i> Example: Router(config-if)# cable upstream 0 freq-adj averaging 50 Router(config-if)#	Specifies the percentage of frequency adjustment packets needed to change the adjustment method from the regular power-adjustment method to the automatic power adjustment method: <i>n</i> = Specifies the upstream port number. Valid values start with 0 for the first upstream port on the cable interface line card. <i>percent</i> = Specifies the percentage of frequency-adjustment packets required to switch from the regular power-adjustment method to the noise power-adjustment method. The valid range is from 10 to 100 percent.
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.

**Caution**

The default settings are adequate for system operation. Amplitude averaging is an automatic procedure. In general, Cisco does not recommend that you adjust values. Cisco does recommend, however, that you clean up your cable plant should you encounter flapping cable modems.

**Note**

In some instances, you might adjust certain values for the **cable upstream power-adjust** command:

If CMs cannot complete ranging because they have reached maximum power levels, increase the **continue pwr-level** parameter beyond the default value of 2 dB. Values larger than 10 dB on “C” versions of cable interface line cards, or 5 dB on FPGA versions, are not recommended.

If the flap list shows CMs with a large number of power adjustments, but the CMs are not detected as “noisy,” decrease the **noise perc-pwr-adj** value. If too many CMs are unnecessarily detected as “noisy,” increase the percentage.

Configuring Flap List Operation Using SNMP (optional)

To configure the Flap List Troubleshooting feature on the Cisco CMTS using SNMP, set the appropriate `cssFlapObjects` attributes in the `CISCO-CABLE-SPECTRUM-MIB`. [Table 8](#) lists each of the configurable attributes:

Table 8 *Flap-List Configuration Attributes*

Attribute	Type	Range	Description
<code>ccsFlapListMaxSize</code>	Integer32	1 to 65536 ¹	The maximum number of modems that a flap list can support. The default is 100.
<code>ccsFlapListCurrentSize</code>	Integer32	1 to 65536 ¹	The current number of modems in the flap list.
<code>ccsFlapAging</code>	Integer32	1 to 86400	The flap entry aging threshold in minutes. The default is 10080 minutes (180 hours or 7 days).
<code>ccsFlapInsertionTime</code>	Integer32	60 to 86400	The worst-case insertion time, in seconds. If a cable modem has not completed the registration stage within this interval, the cable modem is inserted into the flap list. The default value is 90 seconds.
<code>ccsFlapPowerAdjustThreshold</code>	Integer32	1 to 10	When the power of the modem is adjusted beyond the power adjust threshold, the modem is inserted into the flap list.
<code>ccsFlapMissThreshold</code>	Unsigned32	1 to 12	When a cable modem does not acknowledge this number of consecutive MAC-layer station maintenance (keepalive) messages, the cable modem is placed in the flap list.

1. The allowable range when using SNMP for these parameters is 1 to 65536 (a 32-bit value), but the valid operational range is 1 to 8191.

Clearing the Flap List and Counters Using SNMP (optional)

To remove a cable modem from the flap list or to clear one or all of the flap-list counters, set the appropriate `cssFlapObjects` attributes in the `CISCO-CABLE-SPECTRUM-MIB`. [Table 9](#) lists the attributes that clear the SNMP counters.

Table 9 *Attributes to Clear the Flap List*

Attribute	Type	Description
<code>ccsFlapResetAll</code>	Boolean	Setting this object to True (1) resets all flap-list counters to zero.
<code>ccsFlapClearAll</code>	Boolean	Setting this object to True (1) removes all cable modems from the flap list, and destroys all entries in the <code>ccsFlapTable</code> . If a modem keeps flapping, the modem is added again into the flap list as a new entry.



Note

The `ccsFlapLastClearTime` attribute contains the date and time that the entries in the `ccsFlapTable` table were last cleared.

How to Monitor and Troubleshoot Using Flap Lists

- [Displaying the Flap List Using the show cable flap-list Command, page 162](#)
- [Displaying the Flap List Using the show cable modem flap Command, page 166](#)
- [Displaying the Flap List Using SNMP, page 166](#)
- [Displaying Flap-List Information for Specific Cable Modems, page 167](#)
- [Troubleshooting Suggestions, page 169](#)

Displaying the Flap List Using the show cable flap-list Command

To display the current contents of the flap list, use the **show cable flap-list** command in privileged EXEC mode. This command has the following syntax:

- **show cable flap-list** = Displays the complete flap list.
- **show cable flap-list sort-interface** = Displays the complete flap list sorted by cable interface.
- **show cable flap-list cable interface [upstream port]** = Displays the flap list for a specific cable interface, or for a specific upstream port on that cable interface.

To change the way the output is sorted, add one of the following optional keywords:

- **sort-flap** = Sorts the output by the number of times that the cable modem has flapped.
- **sort-time** = Sorts the output by the most recent time that the cable modem flapped.

The following example shows typical output of the **show cable flap-list** command.

```
uBR7100# show cable flap-list
Mac Addr          CableIF Ins  Hit   Miss   CRC   P-Adj  Flap   Time
0010.9500.461f C1/0 U1 56 18857 887    0      1    116 Jun 1 14:09:12
0010.9500.446e C1/0 U1 38 18686 2935   0      1     80 Jun 2 19:03:57
0010.9500.38ec C1/0 U2 63 18932 1040   0      8    138 Jun 2 23:50:53
0010.9500.4474 C1/0 U2 65 18913 1053   0      3    137 Jun 2 09:30:09
0010.9500.4672 C1/0 U2 56 18990 2327   0      6    124 Jun 2 10:44:14
0010.9500.38f0 C1/0 U2 50 18964 2083   0      5    111 Jun 2 20:46:56
0010.9500.e8cb C1/0 U2 0 6537 183    0      1     5 Jun 2 22:35:48
0010.9500.38f6 C1/0 U3 50 19016 2511   0      2    104 Jun 2 07:46:31
0010.9500.4671 C1/0 U3 43 18755 3212   1      1     89 Jun 1 19:36:20
0010.9500.38eb C1/0 U0 57 36133 1608   0      6    126 Jun 2 20:04:58
0010.9500.3ce2 C1/0 U0 44 35315 1907   0      4     99 Jun 2 16:42:47
0010.9500.e8d0 C1/0 U2 0 13213 246    0      1     5 Jun 3 04:15:30
0010.9500.4674 C1/0 U2 56 36037 2379   0      4    121 Jun 3 00:34:12
0010.9500.4677 C1/0 U2 40 35781 2381   0      4     91 Jun 2 12:14:38
0010.9500.4614 C1/0 U2 40 21810 2362   0    502   586 Jun 2 21:43:02
0010.9500.3be9 C1/0 U2 63 22862 969    0      0    128 Jun 1 14:09:03
0010.9500.4609 C1/0 U2 55 22723 2127   0      0    112 Jun 1 14:08:02
0010.9500.3cb8 C1/0 U2 49 22607 1378   0      0    102 Jun 1 14:08:58
0010.9500.460d C1/0 U3 46 22477 2967   0      2     96 Jun 2 17:03:48
0010.9500.3cba C1/0 U3 39 22343 3058   0      0     81 Jun 1 14:13:16
0010.9500.3cb4 C1/0 U3 38 22238 2936   0      0     79 Jun 1 14:09:26
0010.9500.4612 C1/0 U3 38 22306 2928   0      0     79 Jun 1 14:09:29
```

Router#

Table 10 describes each field show by the **show cable flap-list** command:

Table 10 *show cable flap-list Command Field Descriptions*

Field	Description
Mac Addr	The MAC address for the CM.
CableIF	The cable interface line card, including upstream, for this CM.
Ins	The number of times the CM comes up and inserts itself into the network. This counter is indicates the number of times the RF link was abnormally reestablished into the network. This counter is increased when the time between initial link establishment and a reestablishment was less than the threshold parameter configured using the cable flap-list insertion-time command. Normal modem activity uses the following sequence: • Initial link insertion is followed by a station maintenance message between the CMTS and cable modem. • Power on • Initial maintenance • Station maintenance • Power off When the link is broken, initial maintenance is repeated to reestablish the link. • Initial maintenance @ Time T1 • Station maintenance • Initial maintenance @ Time T2 The Ins and Flap counters in the flap list are incremented whenever $T2 - T1 < N$ where N is the insertion-time parameter configured in the cable flap-list insertion-time command. This count may indicate intermittent downstream synchronization loss or DHCP or modem registration problems. In the latter case, the Ins count tends to track the Flap count. If the downstream is unstable (levels move outside the modem's range occasionally), insertions can occur. If the modem cannot provision correctly, many insertions occur. If link reestablishment happens too frequently, the modem usually has a registration problem. To check for this potential problem, check to see if the insertion counter is the same order of magnitude as the Flap counter.
Hit	The number of times the CM responds to MAC-layer station maintenance (keepalive) messages. (The minimum hit rate is once per 30 seconds. It can indicate intermittent upstream, laser clipping, or common-path distortion.
Miss	The number of times the CM misses and does not respond to a MAC-layer station maintenance (keepalive) message. An 8 percent miss rate is normal for the Cisco cable interface line cards. It can indicate intermittent upstream, laser clipping, or common-path distortion.

Table 10 *show cable flap-list Command Field Descriptions (continued)*

Field	Description
Note	The Hit and Miss columns are keepalive polling statistics between the CMTS and the cable modem. The station maintenance process occurs for every modem approximately every 25 seconds. When the CMTS receives a response from the modem, the event is counted as a hit. If the CMTS does not receive a response from the cable modem, the event is counted as a miss. Ideally, the hit count should be much greater than the miss count. If a modem has a hit count much less than its miss count, then registration is failing. Noisy links cause the miss or hit ratio to deviate from a nominal 10 percent or less. High miss counts can indicate: – Intermittent upstream possibly due to noise – Laser clipping – Common-path distortion – Ingress or interference – Too much or too little upstream attenuation A cable modem fails to respond either because of noise or if it is down. Modems that log only misses and zero hits are assumed to be powered off. If noise caused a poll to be missed, then the transition from miss to hit is detected as a flap condition. The poll rate is increased to 1 per second whenever the modem misses a poll. This is used to accelerate the offline state detection and decrease station maintenance overhead. Misses are not desirable, because they usually indicate a return path problem; however, having a small number of misses is normal. After 16 misses, the modem is assumed to have powered off and the link is broken. The flap count is incremented if there are <i>M</i> consecutive misses, where <i>M</i> is configured in the cable flap miss-threshold command. The parameter value ranges from 1 to 12, with a default of 6. Hit and miss analysis could be done after the Ins count stops incrementing. In general, if the hit and miss counts are about the same order of magnitude, and the CRC count is low or nonexistent, then the upstream is experiencing noise. If the miss count is greater, then the modem is probably experiencing common-path distortion and is dropping out frequently or not completing registration. Check grounding connections and if you see noise disappear after breaking a cable connection, but build back up again later, check the end-of-line terminators. You may be using a substandard frequency translator instead of a Digital Signal Processor. If the line is simply noisy, but not too noisy, you see an increase in the percentage of misses. If it is very noisy, then more than 80% of the ranging responses (RNG-RSP) are missed and the modem has many insertions.
CRC	The number of cyclic redundancy check (CRC) errors from this CM. CRC errors usually indicate downstream signal interruption or interference noise on a plant. Some CRC errors can be expected on the older FPGA line cards. Many CRC errors mean that the plant technicians should be looking for poorly performing forward components. A low count can always be expected, but a high CRC number calls for some plant troubleshooting. The CRC counter indicates: • Intermittent upstream • Laser clipping • Common-path distortion • Impulsive noise or interference

Table 10 *show cable flap-list Command Field Descriptions (continued)*

Field	Description
P-Adj	The number of times the headend instructed the CM to adjust transmit (TX) power more than 3 dB. It can indicate amplifier degradation, poor connections, or thermal sensitivity. * means the noise power-adjustment method is active for this modem. ! means the modem has reached its maximum transmit power. The station maintenance poll in the CMTS constantly adjusts the modem transmit power, frequency, and timing. The power-adjustment (P-Adj) column indicates the number of times the modem's power adjustment exceeded the threshold value. The power adjustment threshold may be set using the cable flap-list power-adjust threshold command with a value range of 0 to 10 dB and a default value of 2 dB. Tuning this threshold is recommended to decrease irrelevant entries in the flap list. Power-adjustment values of 2 dB and below continuously increment the P-Adj counter. The modem transmitter step size is 1.5 dB, whereas the headend may command 0.25 dB step sizes. Power-adjustment flap strongly suggests upstream plant problems such as: • Amplifier degradation • Poor connections • Thermal sensitivity • Attenuation problem The P-Adj column is often watched as an indicator of plant stability. It may give a forewarning of a future plant outage. If the upstream path contains too much or too little loss, the modem is undergoing many power adjustments.
Flap	The total number of times a modem has flapped, which is the sum of P-Adj and Ins values. This counter is incremented when one of the following events is detected: • Unusual modem insertion or re-registration attempts. The Flap and the Ins counters are incremented when the modem tries to reestablish the RF link with the CMTS within a period of time that is less than the user-configured insertion interval value. • Abnormal miss or hit ratio. The Flap counter is incremented when <i>N</i> consecutive misses are detected after a hit where <i>N</i> can be user-configured with a default value of 6. • Unusual power adjustment. The Flap and P-Adj counters are incremented when the modem's upstream power is adjusted beyond a user-configured power level.
Time	Time is the most recent time that the modem dropped the connection or flapped. The value is based on the clock configured on the local CMTS. If no time is configured, this value is based on the current uptime of the CMTS. When a cable modem meets one of the three flap-list criteria, the Flap counter is incremental and Time is set to the current time.

Displaying the Flap List Using the show cable modem flap Command

To display the contents of the flap list for a specific cable modem, use the **show cable modem flap** command in privileged EXEC mode. This command has the following syntax:

- **show cable modem** [*ip-address* | *mac-address*] **flap** = Displays the flap list for a specific cable modem, as identified by its IP address or MAC address.
- **show cable modem cable interface** [*upstream port*] **flap** = Displays the flap list for all cable modems on a specific cable interface.



Note

The **show cable modem flap** command displays information similar to that shown by the **show cable flap-list** command, except it displays this information on a per-modem basis.

The following example shows sample output for the **show cable modem flap** command for a particular cable modem:

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

MAC Address	I/F	Ins	Hit	Miss	CRC	P-Adj	Flap	Time
0010.7bb3.fcd1	C5/0/U5	0	36278	92	0	369	372	Jun 1 13:05:23

```
Router#
```

The following example shows sample output for the **show cable modem flap** command for all cable modems on a specific cable interface:

```
Router# show cable modem c8/1/0 flap
```

MAC Address	I/F	Ins	Hit	Miss	CRC	P-Adj	Flap	Time
0050.7366.1243	C8/1/0/U1	6	29770	79	0	0	11	Apr 28 13:08:06
0002.b970.0027	C8/1/0/U4	6	29737	109	0	1	14	Apr 28 13:08:44
0006.5314.858d	C8/1/0/U4	2	29635	41	0	0	4	Apr 28 13:09:21

```
Router#
```

See [Table 10 on page 163](#) for a description of the fields shown by this command.

Displaying the Flap List Using SNMP

To display the contents of the flap list using SNMP, query the `ccsFlapTable` table in the `CISCO-CABLE-SPECTRUM-MIB`. This table contains an entry for each cable modem. [Table 11](#) briefly describes each attribute in this table.

Table 11 *ccsFlapTable Attributes*

Attribute	Type	Description
ccsFlapMacAddr	MacAddress	MAC address of the cable modem's cable interface. Identifies a flap-list entry for a flapping cable modem.
ccsFlapUpstreamIfIndex	InterfaceIndex	Upstream being used by the flapping cable modem.
ccsFlapDownstreamIfIndex	InterfaceIndex	Downstream being used by the flapping cable modem.
ccsFlapLastFlapTime	DateAndTime	Time stamp for the last time the cable modem flapped.
ccsFlapCreateTime	DateAndTime	Time stamp that this entry was added to the table.

Table 11 *cssFlapTable Attributes (continued)*

Attribute	Type	Description
ccsFlapRowStatus	RowStatus	Control attribute for the status of this entry.
ccsFlapInsertionFailNum	Unsigned32	Number of times the CM comes up and inserts itself into the network. This counter is increased when the time between initial link establishment and a reestablishment was less than the threshold parameter configured using the cable flap-list insertion-time command or ccsFlapInsertionTime attribute. When the cable modem cannot finish registration within the insertion time (ccsFlapInsertionTime), it resends the Initial Maintenance packet. When the CMTS receives the packet sooner than expected, the CMTS increments this counter.
ccsFlapHitNum	Unsigned32	Number of times the CM responds to MAC-layer station maintenance (keepalive) messages. (The minimum hit rate is once per 30 seconds.)
ccsFlapMissNum	Unsigned32	Number of times the CM misses and does not respond to a MAC-layer station maintenance (keepalive) message. An 8 percent miss rate is normal for the Cisco cable interface line cards. If the CMTS misses a ranging request within 25 msec, then the miss number is incremented.
ccsFlapCrcErrorNum	Unsigned32	Number of times the CMTS upstream receiver flagged a packet with a CRC error. A high value indicates that the cable upstream may have a high noise level. The modem may not be flapping yet, but this could become a possible problem.
ccsFlapPowerAdjustmentNum	Unsigned32	Number of times the cable modem upstream transmit power is adjusted during station maintenance. When the adjustment is greater than the power-adjustment threshold, the number is incremented.
ccsFlapTotalNum	Unsigned32	Number of times a modem has flapped, which is the sum of the following: • When ccsFlapInsertionFailNum is increased • When the CMTS receives a miss followed by a hit • When ccsFlapPowerAdjustmentNum is increased
ccsFlapResetNow	Boolean	Setting this object to True (1) resets all flap-list counters to zero.
ccsFlapLastResetTime	DateAndTime	Time stamp for when all the counters for this particular entry were reset to zero.

Displaying Flap-List Information for Specific Cable Modems

To use SNMP requests to display flap-list information for a specific cable modem, use the cable modem's MAC address as the index to retrieve entries from the ccsFlapTable. Use the following procedure to retrieve flap-list entries for a particular cable modem.

DETAILED STEPS

- Step 1** Convert the cable modem's MAC address into a dotted decimal string. For example, the MAC address 000C.64ff.eb95 would become 0.12.100.255.235.149.

Step 2 Use the dotted decimal version of the MAC address as the instance for requesting information from the `ccsFlapTable`. For example, to retrieve the `ccsFlapHits`, `ccsFlapMisses`, and `ccsFlapPowerAdjustments` values for this cable modem, you would make an SNMP request for the following objects:

- `ccsFlapHits.0.12.100.255.235.149`
- `ccsFlapMisses.0.12.100.255.235.149`
- `ccsFlapPowerAdjustments.0.12.100.255.235.149`

Example

Assume that you want to retrieve the same flap-list information as the **show cable flap-list** command for a cable modem with the MAC address of 000C.64ff.eb95:

```
Router# show cable flap-list
```

```
MAC Address      Upstream      Ins   Hit   Miss  CRC   P-Adj  Flap  Time
000C.64ff.eb95  Cable3/0/U4   3314  55605 50460 0      *42175 47533 Jan 27 02:49:10
```

```
Router#
```

Use an SNMP tool to retrieve the `ccsFlapTable` and filter it by the decimal MAC address. For example, using the standard Unix **getone** command, you would give the following command:

```
csh% getmany -v2c 192.168.100.121 public ccsFlapTable | grep 0.12.100.255.235.149
```

```
ccsFlapUpstreamIfIndex.0.12.100.255.235.149 = 15
ccsFlapDownstreamIfIndex.0.12.100.255.235.149 = 17
ccsFlapInsertionFails.0.12.100.255.235.149 = 3315
ccsFlapHits.0.12.100.255.235.149 = 55608
ccsFlapMisses.0.12.100.255.235.149 = 50460
ccsFlapCrcErrors.0.12.100.255.235.149 = 0
ccsFlapPowerAdjustments.0.12.100.255.235.149 = 42175
ccsFlapTotal.0.12.100.255.235.149 = 47534
ccsFlapLastFlapTime.0.12.100.255.235.149 = 07 d4 01 1b 02 33 1a 00
ccsFlapCreateTime.0.12.100.255.235.149 = 07 d4 01 16 03 23 22 00
ccsFlapRowStatus.0.12.100.255.235.149 = active(1)
ccsFlapInsertionFailNum.0.12.100.255.235.149 = 3315
ccsFlapHitNum.0.12.100.255.235.149 = 55608
ccsFlapMissNum.0.12.100.255.235.149 = 50460
ccsFlapCrcErrorNum.0.12.100.255.235.149 = 0
ccsFlapPowerAdjustmentNum.0.12.100.255.235.149 = 42175
ccsFlapTotalNum.0.12.100.255.235.149 = 47534
ccsFlapResetNow.0.12.100.255.235.149 = false(2)
ccsFlapLastResetTime.0.12.100.255.235.149 = 07 d4 01 16 03 20 18 00
```

```
csh%
```

To request just one particular value, use the decimal MAC address as the instance for that object:

```
csh% getone -v2c 172.22.85.7 public ccsFlapMisses.0.12.100.255.235.149
```

```
ccsFlapMisses.0.12.100.255.235.149 = 50736
```

```
csh %
```


Troubleshooting Suggestions

This section provides tips on how to interpret the flap-list counters, as well as how to determine the optimum power level for a flapping cable modem.

- [Troubleshooting Tips, page 169](#)
- [Performing Amplitude Averaging, page 169](#)
- [Using Other Related Commands, page 170](#)

Troubleshooting Tips

This section includes suggestions on how to interpret different network conditions based on the flap-list statistics:

- **Condition 1:** Low miss or hit ratio (< 2 percent for a Cisco uBR-MC16 card), low insertion, low P-Adj, low flap counter, and old time stamp.
Analysis: This exhibits an optimal network situation.
- **Condition 2:** High ratio of misses over hits (> 10 percent).
Analysis: Hit and miss analysis should be done after the Ins count stops incrementing. In general, if the hit and miss counts are about the same order of magnitude, the upstream can be experiencing noise. If the miss count is greater, then the modem is probably dropping out frequently and not completing registration. The upstream or downstream might not be stable enough for reliable link establishment. Very low hits and miss counters and high insertion counters indicate provisioning problems.
- **Condition 3:** Relatively high power-adjustment counter.
Analysis: Indicates that the power-adjustment threshold is probably set at default value of 2 dB. The modem transmitter step size is 1.5 dB, but the headend can command 0.25 dB step sizes. Tuning your power threshold to 6 dB is recommended to decrease irrelevant entries in the flap list. The power-adjustment threshold can be set using *cable flap power threshold <0-10 dB>* in the Cisco IOS global configuration mode. A properly operating HFC network with short amplifier cascades can use a 2 to 3 dB threshold.
- **Condition 4:** High P-Adj and CRC errors.
Analysis: This condition can indicate that the fiber node is clipping the upstream return laser. Evaluate the modems with the highest CRC count first. If the modems are not going offline (Ins = 0), this is not noticed by subscribers. However, they could receive slower service due to dropped IP packets in the upstream. This condition also results in input errors on the Cisco uBR7100 series router cable interface.
- **Condition 5:** High insertion rate.
Analysis: If link reestablishment happens too frequently, the modem is usually having a registration problem. This is indicated by a high Ins counter, which tracks the Flap counter.

Performing Amplitude Averaging

The CMTS uses an averaging algorithm to determine the optimum power level for a cable modem with low carrier-to-noise ratio that is making excessive power adjustments—known as flapping. To avoid dropping flapping cable modems, the CMTS averages a configurable number of RNG-REQ messages before it makes power adjustments. By compensating for a potentially unstable return path, the CMTS maintains connectivity with affected cable modems. You can interpret these power adjustments, however, as indicating unstable return path connections.

The **show cable flap-list** and **show cable modem** commands are expanded to indicate to which paths the CMTS is making power adjustments and which modems have reached maximum transmit power settings. These conditions indicate unstable paths that should be serviced.

The following example shows the output of the **show cable flap-list** command:

```
Router# show cable flap-list
```

MAC Address	Upstream	Ins	Hit	Miss	CRC	P-Adj	Flap	Time
0010.7bb3.fdl9	Cable1/0/U1	0	2792	281	0	*45	58	Jul 27 16:54:50
0010.7bb3.fcfc	Cable1/0/U1	0	19	4	0	!43	43	Jul 27 16:55:01
0010.7bb3.fcdd	Cable1/0/U1	0	19	4	0	*3	3	Jul 27 16:55:01

The asterisk (*) indicates that the CMTS is using the power-adjustment method on this modem. An exclamation point (!) indicates that the modem has reached maximum transmit power.

Output of the **show cable modem** command appears below:

```
Router# show cable modem
```

Interface	Prim Sid	Online State	Timing Offset	Rec Power	QoS	CPE	IP address	MAC address
Cable1/0/U0	1	online	2257	0.00	3	0	10.30.128.142	0090.8330.0217
Cable1/0/U0	2	online	2262	*-0.50	3	0	10.30.128.145	0090.8330.020f
Cable1/0/U0	3	online	2260	0.25	3	0	10.30.128.146	0090.8330.0211
Cable1/0/U0	4	online	2256	*0.75	3	0	10.30.128.143	0090.8330.0216
Cable1/0/U0	5	online	2265	*0.50	3	0	10.30.128.140	0090.8330.0214
Cable1/0/U0	6	online	2256	0.00	3	0	10.30.128.141	0090.8330.0215
Cable1/0/U0	7	online	4138	!-1.00	3	1	10.30.128.182	0050.7366.124d
Cable1/0/U0	8	online	4142	!-3.25	3	1	10.30.128.164	0050.7366.1245
Cable1/0/U0	9	online	4141	!-3.00	3	1	10.30.128.185	0050.7366.17e3
Cable1/0/U0	10	online	4142	!-2.75	3	0	10.30.128.181	0050.7366.17ab
Cable1/0/U0	11	online	4142	!-3.25	3	1	10.30.128.169	0050.7366.17ef

Similar to the **show cable flap-list** command display, the * symbol in the **show cable modem** command output indicates that the CMTS is using the power-adjustment method on this CM. The ! symbol indicates that the CM has reached maximum transmit power.

Using Other Related Commands

The following related Cisco IOS commands can be used to do maintenance on or display information about a cable modem.

- The following clears the counters for a cable modem (or all cable modems) in the station maintenance list:
clear cable modem {mac-addr | ip-addr | all} counters
- The following displays the QoS, modem status, In and Out octets, IP and MAC addresses per SID:
show int cable slot/port sid
- The following drops the modem's RF link by removing a modem from the keepalive polling list. This forces the modem to reset. Note the warning below.
clear cable-modem {mac-addr | ip-addr | all} reset



Tip

The **clear cable-modem all reset** command causes all modems to go offline and disrupt service for your users. It is best used in a test or nonproduction environment.

- The following uses a MAC-layer ping to determine if the cable modem is online. It uses smaller data units on the wire than a standard IP ping, resulting in lower overhead. This command works even if the IP layer in the modem is down or has not completed registration:

```
ping DOCSIS cable-modem mac-addr / IP address
```

- The following displays the timing offset, receive power, and QoS values by cable interface, SID, and MAC address:

```
show cable modem [ip-address / MAC-address]
```

- The following displays the current allocation table and frequency assignments:

```
show cable spectrum-group [spectrum group number]
```

- The following displays maximum, average, and minimum percent of online time and offline time for a given SID on a given cable router interface:

```
show int slot/port sid connectivity
```

- The following command displays input and output rates, input errors, CRC, frames, overruns, underruns, collisions, interface resets. High input errors in the CMTS retrieved from this query suggest noisy upstream. In older versions of the chassis, loose midplane and line card screws caused a similar problem:

```
show interface slot/downstream-port
```

- The following command displays upstream packet discards, errors, error-free packets, correctable and uncorrectable errors, noise, and micro-reflection statistics.

```
show interface slot/downstream-port upstream
```

Configuration Examples for Flap List Troubleshooting

The following excerpt from a configuration file shows a typical flap-list configuration:

```
!  
cable flap-list insertion-time 120  
cable flap-list power-adjust threshold 3  
cable flap-list miss-threshold 4  
cable flap-list aging 8  
cable flap-list size 8191
```

...

Additional References

For additional information related to the Flap List Troubleshooting feature, refer to the following references:

Related Documents

Related Topic	Document Title
CMTS Command Reference	<i>Cisco Broadband Cable Command Reference Guide</i>, at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/cable/bbcmref/index.htm
Cisco IOS Release 12.2 Command Reference	Cisco IOS Release 12.2 Configuration Guides and Command References, at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/index.htm
Cisco Broadband Troubleshooter	<i>Getting Started with Cisco Broadband Troubleshooter</i> and Release Notes, at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/cable/trblshtr/index.htm
Cisco Cable Manager	<i>Cisco Cable Manager Users' Guide</i>, Release 2.0, at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/cable/cbl_mgt/index.htm
Cisco uBR7100 Series Universal Broadband Router Documentation	<i>Cisco uBR7100 Series Universal Broadband Router Hardware Installation Guide</i>, at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/cable/ubr7100/hig7100/index.htm <i>Cisco uBR7100 Series Universal Broadband Router Software Configuration Guide</i>, at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/cable/ubr7100/scg7100/index.htm

Related Topic	Document Title
Cisco uBR7200 Series Universal Broadband Router Documentation	<i>Cisco uBR7200 Series Universal Broadband Router Hardware Installation Guide</i>, at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/cable/cab_rout/cr72hig/index.htm <i>Cisco uBR7200 Series Universal Broadband Router Software Configuration Guide</i>, at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/cable/cab_rout/cr72scg/index.htm
Cisco uBR10012 Universal Broadband Router Documentation	<i>Cisco uBR10012 Universal Broadband Router Hardware Installation Guide</i>, at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/cable/ubr10k/ubr10012/hig/index.htm <i>Cisco uBR10012 Universal Broadband Router Software Configuration Guide</i>, at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/cable/ubr10k/ubr10012/scg/index.htm

Standards

Standards ¹	Title
ANSI/SCTE 22-1 2002 (formerly SP-RFI-C01-011119)	Data-Over-Cable Service Interface Specification DOCSIS 1.0 Radio Frequency Interface (RFI) (http://www.cablemodem.com)
SP-RFIv1.1-I08-020301	Data-over-Cable Service Interface Specifications Radio Frequency Interface Specification (http://www.cablemodem.com)
SP-BPI+-I08-020301	DOCSIS Baseline Privacy Interface Plus Specification (http://www.cablemodem.com)

1. Not all supported standards are listed.

MIBs

MIBs ¹	MIBs Link
CISCO-CABLE-SPECTRUM-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

1. Not all supported MIBs are listed.

RFCs

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

Technical Assistance

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

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, TeleRouter, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0502R)

Copyright © 2003 Cisco Systems, Inc. All rights reserved.



Internal DOCSIS Configuration File Generator for the Cisco CMTS

Feature Specifications for the Internal DOCSIS Configuration File Generator

Feature History

Release	Modification
Release 12.1(2)EC	This feature was supported on the Cisco uBR7200 series routers.
Release 12.1(5)EC	This feature was supported on the Cisco uBR7100 series routers.
Release 12.2(4)BC1	This feature was supported on the Release 12.2 BC train for all Cisco CMTS platforms.

Supported Platforms

Cisco uBR7100 series, Cisco uBR7200 series, Cisco uBR10012 universal broadband routers.

Finding Support Information for Platforms and Cisco IOS Software Images

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

Contents

This document contains the following major sections that describe the Internal DOCSIS Configuration File Generator for the Cisco CMTS routers:

- [Prerequisites for the Internal DOCSIS Configuration File Generator, page 176](#)
- [Restrictions for the Internal DOCSIS Configuration File Generator, page 176](#)
- [Information About the Internal DOCSIS Configuration File Generator, page 177](#)
- [How to Use the Internal DOCSIS Configuration File Generator, page 179](#)
- [Configuration Examples for the Internal DOCSIS Configuration File Generator, page 196](#)
- [Additional References, page 198](#)



Corporate Headquarters:

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

Copyright © 2003 Cisco Systems, Inc. All rights reserved.

Prerequisites for the Internal DOCSIS Configuration File Generator

- The Internal DOCSIS Configuration File Generator feature supports the Baseline Privacy Interface (BPI) options only in Cisco IOS software images that support BPI or BPI+ encryption.
- To allow CMs to download the configuration files, you must also enable the router's onboard TFTP server, using the **tftp-server** command. Unless you are running on a small lab network, you should also remove the default limit of 10 TFTP sessions by using the service udp-small-serves max-servers no limit command.
- The following commands are also recommended when using the Internal DOCSIS Configuration File Generator feature:
 - **cable time-server**—Enables the Cisco CMTS to function as a time-of-day (ToD) server.
 - **ip dhcp pool**—Configures the Cisco CMTS as a DHCP server. Otherwise, you need an external DHCP server.
 - **ip dhcp ping packets 0**—Improves the scalability of the Cisco CMTS DHCP server.

Restrictions for the Internal DOCSIS Configuration File Generator

- The Internal DOCSIS Configuration File Generator feature supports a shared secret (using the **cable shared-secret** command) but does not support secondary shared secrets (using the **cable shared-secondary-secret** command).
- The DOCSIS specifications limit the size of MAC-layer management messages to 1522 bytes, which in turn limits the amount of Vendor-Specific Information Fields (VSIF) you can include in the DOCSIS configuration file. This is because DOCSIS requires that when the cable modem sends its Registration Request (REG-REQ) message to the CMTS, it must include the configuration information, including the VSIF fields, found in the DOCSIS configuration file.

In particular, this maximum packet size imposes a limit on the number of Cisco IOS CLI commands you can include as VSIF fields in the DOCSIS configuration file. The exact number of commands that will fit depends on the other information included in the file, as well as the length of each command.

If the REG-REQ message is larger than 1522 bytes, the cable modem will likely report errors similar to the following errors that appear on Cisco uBR900 series cable access routers:

```
%LINK-4-TOOBIG: Interface cable-modem0, Output packet size of 1545 bytes too big
%LINEPROTO-5-UPDOWN: Line protocol on Interface cable-modem0, changed state to down
```

In addition, the CMTS also reports that the cable modem timed out during the registration process. If this occurs, you can try the following steps:

- Reduce the length of the commands by using the abbreviated form of the command. For example, you can specify the **int c0** instead of the full command **interface cable-modem0**.
- SNMP MIB objects are not included in the Registration Request message, so wherever possible, replace the CLI commands with the corresponding SNMP MIB object statements in the DOCSIS configuration file.

- If a large number of CLI commands must be given, use VSIF option 128 to download a Cisco IOS configuration file to the cable modem.

**Tip**

For complete details on what is included in the REG-REQ message, see Chapter 6 of the DOCSIS 1.1 specification.

Information About the Internal DOCSIS Configuration File Generator

This section provides the following information about the Internal DOCSIS Configuration File Generator feature:

- [Feature Overview, page 177](#)
- [DOCSIS Configuration File Commands, page 178](#)
- [Benefits, page 179](#)

Feature Overview

The Data-over-Cable Service Interface Specifications (DOCSIS) standard requires that cable modems download a DOCSIS configuration file before being allowed to register on the cable network. This configuration file contains parameters that control the modem's access to the network, such as the maximum upstream and downstream rates, the maximum number of customer premises equipment (CPE) devices supported by the cable modem, and whether the connected CPE is allowed access to the service provider's network.

DOCSIS configuration files are saved in a binary format, as required by the DOCSIS specifications. Typically service providers use a separate DOCSIS configuration file editor on an external server to create the DOCSIS configuration files that are used on their network. Then the providers must save the files to the appropriate Trivial File Transfer Protocol (TFTP) server so that they can be delivered to cable modems as they register on the cable network.

To simplify this process, Cisco CMTS routers offer the option of creating DOCSIS configuration files on the router. These files are stored as text commands that are part of the router's Cisco IOS configuration. When a cable modem requests a DOCSIS configuration file, the Cisco CMTS router dynamically creates the binary version of the file and uses the router's onboard TFTP server to deliver it to the appropriate cable modem.

Service providers thus have the following options as to how DOCSIS configuration files can be created and delivered to cable modems:

- The Cisco Internal DOCSIS Configurator File Generator creates DOCSIS configuration files as part of the router's Cisco IOS configuration. When the file is to be transmitted by the TFTP server, the router creates the binary file that is required by the DOCSIS specifications, and the TFTP server transmits that binary file to the cable modem. This allows rapid changes to be made to a DOCSIS configuration file simply by giving the appropriate Cisco IOS command-line interface (CLI) commands.
- A standalone DOCSIS configuration file editor can be used to create the binary DOCSIS configuration file, which is then transferred to the router's Flash memory or PCMCIA memory device. The TFTP server can then be instructed to send that file to cable modems as requested. To

make a change in this file, the standalone DOCSIS configuration file editor must make those changes and the new file must be transferred back to the router's Flash memory or PCMCIA memory device.

- A standalone DOCSIS configuration file editor can be used to create the binary DOCSIS configuration file, which is then stored on a separate TFTP server in the cable headend network. This TFTP server is responsible for transmitting that file to cable modems as requested. To make a change in this file, the standalone DOCSIS configuration file editor must make those changes and the new file transferred back to the standalone TFTP server.

DOCSIS Configuration File Commands

To create a DOCSIS configuration file, use the **cable config-file** command in global configuration mode. This command creates the configuration file in the router's running configuration and then enters cable configuration file mode, at which point you can enter any or all of the subcommands listed in [Table 12](#).

Table 12 DOCSIS Configuration File Editor Subcommands

Command	Description
access-denied	Specifies whether CPE devices attached to the cable modem are allowed access to the cable network. Note This subcommand does NOT disconnect the cable modem from the cable network. It instead prevents the CPE devices connected to the cable modem from accessing the cable network.
channel-id	Specifies the upstream channel ID to be used by the cable modem.
cpe max	Specifies the maximum number of CPE devices that can use the cable modem to connect to the network.
download	Specifies that the cable modem should download a new software image, if necessary, from a TFTP server before beginning operations on the cable network.
frequency	Specifies the center frequency for a downstream channel for the cable modem.
option	Specifies configuration file options that are not supported by the other cable config-file commands. In particular, this command allows unspecified vendor-specific options that can vary from vendor to vendor and from model to model.
privacy	Enables or disables Baseline Privacy Interface (BPI) encryption on the cable modem. Note To enable BPI operations on a cable modem, you must use both the privacy and service-class privacy commands.
service-class	Specifies additional class of service (CoS) profiles to support different types of traffic flows, such as real-time traffic and traffic that has a guaranteed minimum bandwidth.

Table 12 DOCSIS Configuration File Editor Subcommands (continued)

Command	Description
snmp manager	Specifies the IP address for a Simple Network Management Protocol (SNMP) manager that is allowed access to the cable modem.
timestamp	Enables the time-stamping of a DOCSIS configuration file when it is sent to a cable modem so that it cannot be captured and replayed at a later time for a cable modem that is not authorized to use that file. Also, the time-stamp feature automatically ensures time synchronization between the DOCSIS configuration file and the CMTS. To ensure time synchronization between an external TFTP server and the CMTS, the TFTP server should use a time synchronization protocol, such as Network Time Protocol (NTP).

Benefits

- Allows multiple service operator provisioners, service providers, and other users to create, edit, and internally store a DOCSIS configuration file on the CMTS to provide operational instructions for DOCSIS cable modems and set-top boxes.
- Because this is a built-in tool on the Cisco CMTS, this feature removes the requirement for standalone TFTP servers to create and deliver DOCSIS configuration files.
- Changes can be made to DOCSIS configuration files by giving one or more CLI commands. You do not have to use a standalone DOCSIS configuration file editor to make the changes, create a new binary file, and then transfer it to the Cisco CMTS router.

Related Features

The Internal DOCSIS Configuration File Generator feature creates DOCSIS configuration files and saves them as part of the Cisco CMTS router's startup or running configuration file. To create standalone DOCSIS configuration files, you can use the standalone DOCSIS configuration file editor that is available at the following URL:

<http://www.cisco.com/cgi-bin/tablebuild.pl/cpe-conf>



Note

You must have an account on Cisco.com to access this location.

How to Use the Internal DOCSIS Configuration File Generator

To create and use the router's onboard DOCSIS configuration file editor, see the following sections. Each task in the list is identified as either required or optional.

- [Creating and Configuring a DOCSIS Configuration File](#) (required)
- [Specifying SNMP MIB Objects \(Option 11\)](#) (optional)

- [Specifying Vendor-Specific Information Fields \(Option 43\)](#) (optional)
- [Configuring the Router's Onboard TFTP Server](#) (required)

For syntax and usage information on the cable-specific commands shown in this section, see the [Cisco Broadband Cable Command Reference Guide](#) on Cisco.com and on the Documentation CD-ROM.

For information about any other commands, see the [Cisco IOS Release 12.2 documentation set](#) on Cisco.com.

Creating and Configuring a DOCSIS Configuration File

The following shows how to use the **cable config-file** and its subcommands to create a DOCSIS configuration file that is stored as part of the router's running configuration memory.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cable config-file** *filename*
4. **access-denied**
5. **channel-id** *upstreamchan-id*
6. **cpe** *maxcpe-num*
7. **download image** *filename* [*oui oui-list*]
8. **download server** *ip-address*
9. **frequency** *freq*
10. **option** *n* [**instance** *inst-num*] {**ascii** *string* | **hex** *hexstring* | **ip** *ip-address*}
11. **privacy grace-time** {**authorization** *value* | **tek** *value*}
12. **privacy timeout** {**authorize** *value* | **operational** *value* | **re-authorize** *value* | **reject** *value* | **rekey** *value*}
13. **service-class** *class* {**guaranteed-upstream** *us-bandwidth* **max-burst** *burst-size* **max-downstream** *max-dsbandwidth* **max-upstream** *max-usbandwidth* **priority** *priority-num* **privacy**}
14. **snmp manager** *ip-address*
15. **timestamp**
16. **exit**
17. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	cable config-file filename Example: Router(config)# cable config-file new.cm Router(config-file)#	Creates a DOCSIS configuration file and enters cable config-file configuration mode. The <i>filename</i> can be any arbitrary string that uniquely identifies this configuration file. This is also the filename to be used when sending the configuration file to a cable modem with a TFTP server.
Step 4	access-denied Example: Router(config-file)# access-denied Router(config-file)#	(Optional) Instructs the cable modem to prevent CPE devices from accessing the cable network. The default is the no form of this command, which allows CPE devices to access the cable network.
Step 5	channel-id upstreamchan-id Example: Router(config-file)# channel-id 4 Router(config-file)#	(Optional) Instructs the cable modem to use a specific upstream channel ID. The valid range for <i>upstreamchan-id</i> is 0 to 255, depending on the number of upstream ports on the cable interface card. For telco-return cable modems, this value must either be 0 or left unspecified.
Step 6	cpe maxcpe-num Example: Router(config-file)# cpe 8 Router(config-file)#	(Optional) Specifies the maximum number of CPE devices that can use the cable modem to connect to the network. The valid range for <i>maxcpe-num</i> is 1 to 254, with a default of 1.
Step 7	download image filename [oui oui-list] Example: Router(config-file)# download image ubr925-v9y-mz oui 00.00.0C Router(config-file)#	(Optional) Specifies that the cable modem should download and execute a new software image before coming online. <i>filename</i> = Fully qualified path name for the software image as it exists on the TFTP server. <i>oui-list</i> = (Optional) Specifies up to eight Organizational Unique Identifiers (OUIs). The cable modem must match one of these OUI values before it can download the software image. This ensures that a cable modem downloads software images made only by the proper vendor.
Step 8	download server ip-address Example: Router(config-file)# download server 10.10.10.13 Router(config-file)#	(Optional) Specifies the IP address for the TFTP server from which the cable modem should download new software images. If not specified, the cable modem uses the same TFTP server that provided its DOCSIS configuration file.

	Command or Action	Purpose
Step 9	frequency <i>freq</i> Example: Router(config-file)# frequency 453000000 Router(config-file)#	(Optional) Specifies the center frequency for the downstream channel to be used by the cable modem. The valid range for <i>freq</i> is 88 to 860 MHz. The default is for the modem to scan the downstream for available frequencies.
Step 10	option <i>n</i> [instance <i>inst-num</i>] { ascii <i>string</i> hex <i>hexstring</i> ip <i>ip-address</i> } Example: Router(config-file)# option 43 hex 08:03:00:00:0C:80:07:69:6F:73:2E:63:66:67 Router(config-file)#	(Optional) Specifies a TLV option that is not otherwise available, such as VSIF fields. <i>n</i> = TLV option code. The valid range range is 5 to 254. instance <i>inst-num</i> = (Optional) Specifies an instance of this option so that you can give the same option multiple times. The valid range is 0 to 255. ascii <i>string</i> = Specifies the data as a network verification tool (NVT) ASCII string. If the string contains white space, you must surround it with quotes. hex <i>hexstring</i> = Specifies the data as a raw hexadecimal string. Each byte is two hexadecimal digits, and each byte can be separated by a period, colon, or white space. A maximum of 254 bytes can be specified. ip <i>ip-address</i> = Specifies the data in the form of an IP address.
Step 11	privacy grace-time { authorization <i>value</i> tek <i>value</i> } Example: Router(config-file)# privacy grace-time authorization 1000 Router(config-file)# privacy grace-time tek 800 Router(config-file)#	(Optional) Enables Baseline Privacy Interface (BPI) encryption and configures the grace-time timer values: authorization <i>value</i> = Specifies the authorization grace time in seconds. The valid range is 1 to 1800 seconds, with a default of 600 seconds. tek <i>value</i> = Specifies the Traffic Exchange Key (TEK) grace time in seconds. The valid range is 1 to 1800 seconds, with a default of 600 seconds.
Step 12	privacy timeout { authorize <i>value</i> operational <i>value</i> re-authorize <i>value</i> reject <i>value</i> rekey <i>value</i> } Example: Router(config-file)# privacy timeout authorize 15 Router(config-file)#	(Optional) Enables Baseline Privacy Interface (BPI) encryption and configures the following timeout values: authorize <i>value</i> = Specifies the authorize wait timeout in seconds. The valid range is 2 to 30 seconds, with a default of 10 seconds. operational <i>value</i> = Specifies the operational wait timeout in seconds. The valid range is 1 to 10 seconds, with a default of 1 second. re-authorize <i>value</i> = Specifies the re-authorize wait timeout in seconds. The valid range is 1 to 20 seconds, with a default of 10 seconds. reject <i>value</i> = Specifies the authorize reject wait timeout in seconds. The valid range is 1 to 600 seconds, with a default of 60 seconds. rekey <i>value</i> = Specifies the rekey wait timeout in seconds. The valid range is 1 to 10 seconds, with a default of 1 second.

Command or Action	Purpose
Note To enable BPI operations on the cable modem, you must use the privacy command to enable BPI operations in general, and then use the service-class privacy command to enable BPI on that specific CoS profile.	
Step 13 <pre>service-class class {guaranteed-upstream us-bandwidth max-burst burst-size max-downstream max-dsbandwidth max-upstream max-usbandwidth priority priority-num privacy}</pre> Example: <pre>Router(config-file)# service-class 8 max-downstream 100000 priority 4 privacy Router(config-file)#</pre>	(Optional) Creates a class of service (CoS) profile that specifies the quality of service (QoS) parameters the cable modem can use for traffic. class = Specifies service class number. The valid range is 1 to 16, with a default of 1. guaranteed-upstream us-bandwidth = Specifies the guaranteed upstream bandwidth in kbps. The valid range is 0 to 100000 kbps, with a default of 0, which indicates no guaranteed bandwidth. max-burst burst-size = Specifies the maximum upstream burst size in bytes. The valid range is 0 to 65535, with a default value of 0, which signifies unlimited burst length. Cisco recommends a value in the range of 1600 to 1800 bytes. max-downstream max-dsbandwidth = Specifies the maximum downstream data rate in kilobits/sec allowed for traffic associated with this class of service. The valid range is 0 to 100000 kbps, with a default of 0. max-upstream max-usbandwidth = Specifies the maximum upstream bandwidth in kilobits/sec for traffic associated with this class of service. The valid range is 0 to 100000 kbps, with a default of 0, which is no maximum upstream data rate. priority priority-num = Specifies the service class priority. The valid range is 0 to 7, where 7 is the highest-priority service-class setting. privacy = Enables Baseline Privacy Interface (BPI) on this service flow.
Step 14 <pre>snmp manager ip-address</pre> Example: <pre>Router(config-file)# snmp manager 10.10.10.143 Router(config-file)#</pre>	(Optional) Specifies the IP address of an SNMP manager allowed to manage the cable modem. The default is that no SNMP manager is defined.
Step 15 <pre>timestamp</pre> Example: <pre>Router(config-file)# timestamp Router(config-file)#</pre>	(Optional) Enables time-stamp generation of DOCSIS configuration files. When the router's TFTP server sends the DOCSIS configuration file to the cable modem, it adds a field containing the current date and time, to avoid unauthorized parties from capturing the file and replaying it at a later time.

	Command or Action	Purpose
Step 16	Router(config-file)# exit Example: Router(config-file)# exit Router(config)#	Exits cable configuration file mode.
Step 17	Router(config)# exit Example: Router(config)# exit Router#	Exits global configuration mode.

**Note**

When you have enabled a DOCSIS shared secret, using the **cable shared-secret** command, it is automatically applied to the DOCSIS configuration files that are created by the Internal DOCSIS Configuration File Generator feature when the file is sent to a cable modem requesting it.

Specifying SNMP MIB Objects (Option 11)

The DOCSIS specification allows SNMP objects to be set using option 11 in the DOCSIS configuration file. Most writable SNMP attributes can be set using this option. The cable modem treats the SET requests in the DOCSIS configuration file as fully authorized, so SNMP attributes can be set in the DOCSIS configuration file without specifying an SNMP manager or community string.

This section demonstrates the following common uses of this technique to set attributes in DOCS-CABLE-DEVICE-MIB (defined in RFC 2669 or the SNMP management of DOCSIS cable devices):

- [Specifying Multiple SNMP Managers and Community Strings, page 184](#)
- [Specifying an LLC Filter, page 186](#)
- [Specifying a Filter to Block Microsoft NetBIOS Networking and File-Sharing Traffic, page 187](#)

Specifying Multiple SNMP Managers and Community Strings

The DOCS-CABLE-DEVICE-MIB contains a set of attributes that specify the SNMP managers that are allowed access to the cable modem. This section illustrates how to use SNMP to define the following sets of SNMP managers:

- SNMP Manager 1—Allows read-only access to all IP addresses on all interfaces, with a community string of **Public**.
- SNMP Manager 2—Allows read-write access to SNMP managers only on the network 10.0.0.0 on the cable interface, with the community string of **Private**.

These entries are created as instances of the docsDevNmAccessEntry table in DOCS-CABLE-DEVICE-MIB. [Table 13](#) shows the SNMP attributes that must be set to enable these SNMP managers. Following this table are the **cable config-file** commands that create a DOCSIS configuration file that sets these attributes.

**Note**

To specify only an IP address for an SNMP manager in the DOCSIS configuration file, use the **cable config-file snmp manager** command.

Table 13 *docsDevNmAccessEntry*

Object ID Number / Name	Type	Value	Description
SNMP Manager Entry 1—Allows read-only access to all IP addresses on all interfaces, with a community string of Public			
1.3.6.1.2.1.69.1.2.1.7.1 docsDevNmAccessStatus.1	Integer	5	Creates table entry number 1 but does not activate it yet.
1.3.6.1.2.1.69.1.2.1.2.1 docsDevNmAccessIp.1	IP Address	255.255.255.255*	Allows SNMP requests from any source IP address.
1.3.6.1.2.1.69.1.2.1.3.1 docsDevNmAccessIpMask.1	IP Address	0.0.0.0	Specifies that any subnet mask is allowed for the source IP address.
1.3.6.1.2.1.69.1.2.1.4.1 docsDevNmAccessCommunity.1	Octet String	Public	Sets the community string for this group of SNMP managers to Public .
1.3.6.1.2.1.69.1.2.1.5.1 docsDevNmAccessControl.1	Integer	2	Specifies that this group of SNMP Managers has read-only access.
1.3.6.1.2.1.69.1.2.1.6.1 docsDevNmAccessInterfaces.1	Octet String	0	Allows SNMP access from all interfaces on the cable modem.
1.3.6.1.2.1.69.1.2.1.7.1 docsDevNmAccessStatus.1	Integer	1	Enables this entry to allow access by the specified SNMP managers.
SNMP Manager Entry 2—Allows read-write access to SNMP managers only on the network 10.0.0.0 on the cable interface, with the community string of Private			
1.3.6.1.2.1.69.1.2.1.7.2 docsDevNmAccessStatus.2	Integer	5	Creates table entry number 2 but does not activate it yet.
1.3.6.1.2.1.69.1.2.1.2.2 docsDevNmAccessIp.2	IP Address	10.0.0.0	Allows SNMP requests from hosts only on the network 10.0.0.0.
1.3.6.1.2.1.69.1.2.1.3.2 docsDevNmAccessIpMask.2	IP Address	255.0.0.0	Specifies the subnet mask for the allowable hosts.
1.3.6.1.2.1.69.1.2.1.4.2 docsDevNmAccessCommunity.2	Octet String	Private	Sets the community string for this group of SNMP managers to Private .
1.3.6.1.2.1.69.1.2.1.5.2 docsDevNmAccessControl.2	Integer	3	Specifies that this group of SNMP Managers has read-write access.
1.3.6.1.2.1.69.1.2.1.6.2 docsDevNmAccessInterfaces.2	Octet String	0x40	Allows SNMP access only from the cable interface.
1.3.6.1.2.1.69.1.2.1.7.2 docsDevNmAccessStatus.1	Integer	1	Enables this entry to allow access by the specified SNMP managers.

The following commands are the lines in the CMTS Cisco IOS configuration file that would create the DOCSIS configuration file that sets up these filters on the cable modem:

```
!SNMP Manager Entry 1—Allows read-only access to all IP addresses on all interfaces,
! with a community string of Public
option 11 instance 1 hex 30 82 00 10 06 0B 2B 06 01 02 01 45 01 02 01 07 01 02 01 05
option 11 instance 2 hex 30 82 00 13 06 0B 2B 06 01 02 01 45 01 02 01 02 01 40 04 FF FF FF FF
option 11 instance 3 hex 30 82 00 13 06 0B 2B 06 01 02 01 45 01 02 01 03 01 40 04 00 00 00 00
```

```

option 11 instance 4 hex 30 82 00 15 06 0B 2B 06 01 02 01 45 01 02 01 04 01 04 06 70 75 62 6C 69 63
option 11 instance 5 hex 30 82 00 10 06 0B 2B 06 01 02 01 45 01 02 01 05 01 02 01 02
option 11 instance 6 hex 30 82 00 10 06 0B 2B 06 01 02 01 45 01 02 01 06 01 04 01 C0
option 11 instance 7 hex 30 82 00 10 06 0B 2B 06 01 02 01 45 01 02 01 07 01 02 01 01
! SNMP Manager Entry 2—Allows read-write access to SNMP managers only on the
! network 10.0.0.0 on the cable interface, with the community string of Private
option 11 instance 8 hex 30 82 00 10 06 0B 2B 06 01 02 01 45 01 02 01 07 02 02 01 05
option 11 instance 9 hex 30 82 00 13 06 0B 2B 06 01 02 01 45 01 02 01 02 02 40 04 0A 00 00 00
option 11 instance 10 hex 30 82 00 13 06 0B 2B 06 01 02 01 45 01 02 01 03 02 40 04 FF 00 00 00
option 11 instance 11 hex 30 82 00 16 06 0B 2B 06 01 02 01 45 01 02 01 04 02 04 07 70 72 69 76 61 74 65
option 11 instance 12 hex 30 82 00 10 06 0B 2B 06 01 02 01 45 01 02 01 05 02 02 01 03
option 11 instance 13 hex 30 82 00 10 06 0B 2B 06 01 02 01 45 01 02 01 06 02 04 01 40
option 11 instance 14 hex 30 82 00 10 06 0B 2B 06 01 02 01 45 01 02 01 07 02 02 01 01

```

Specifying an LLC Filter

The DOCS-CABLE-DEVICE-MIB contains a set of attributes that can implement Layer 3 Logical Link Control (LLC) filters. This section illustrates the following LLC filters:

- Filter 1 allows IP packets on all interfaces.
- Filter 2 allows IP ARP packets on all interfaces.
- All other Layer 3 traffic is blocked.

These filters are created by creating instances of the docsDevFilterLLCEntry table in DOCS-CABLE-DEVICE-MIB. [Table 14](#) shows the SNMP attributes that must be set to activate these filters. Following this table are the **cable config-file** commands that create a DOCSIS configuration file that sets these attributes.

Table 14 Setting Attributes in docsDevFilterLLCEntry to Allow only IP and IP ARP Traffic

Object ID Number / Name	Type	Value	Description
1.3.6.1.2.1.69.1.6.1.0 docsDevFilterLLCUnmatchedAction.0	Integer	1	Specifies that the default action is to discard all traffic that does not match one of the active LLC filters.
Filter 1—Allows IP traffic on all interfaces			
1.3.6.1.2.1.69.1.6.2.1.2.1 docsDevFilterLLCStatus.1	Integer	5	Creates LLC filter 1 but doesn't activate it yet.
1.3.6.1.2.1.69.1.6.2.1.3.1 docsDevFilterLLCIfIndex.1	Integer	0	Applies this filter to all interfaces on the cable modem.
1.3.6.1.2.1.69.1.6.2.1.4.1 docsDevFilterLLCProtocolType.1	Integer	1	Specifies that Ethertype frames are being filtered.
1.3.6.1.2.1.69.1.6.2.1.5.1 docsDevFilterLLCProtocol.1	Integer	2048	Allows frames carrying IP traffic to pass.
1.3.6.1.2.1.69.1.6.2.1.2.1 docsDevFilterLLCStatus.1	Integer	1	Activates this filter.
Filter 2—Allows IP ARP traffic on all interfaces			
1.3.6.1.2.1.69.1.6.2.1.2.2 docsDevFilterLLCStatus.2	Integer	5	Creates LLC filter 2 but doesn't activate it yet.
1.3.6.1.2.1.69.1.6.2.1.3.2 docsDevFilterLLCIfIndex.2	Integer	0	Applies this filter to all interfaces on the cable modem.
1.3.6.1.2.1.69.1.6.2.1.4.2 docsDevFilterLLCProtocolType.2	Integer	1	Specifies that Ethertype frames are being filtered.

Table 14 Setting Attributes in docsDevFilterLLCEntry to Allow only IP and IP ARP Traffic (continued)

Object ID Number / Name	Type	Value	Description
1.3.6.1.2.1.69.1.6.2.1.5.2 docsDevFilterLLCProtocol.2	Integer	2054	Allows frames carrying IP ARP traffic to pass.
1.3.6.1.2.1.69.1.6.2.1.2.2 docsDevFilterLLCStatus.2	Integer	1	Activates this filter.

The following commands are the lines in the CMTS Cisco IOS configuration file that would create the DOCSIS configuration file that sets up these filters on the cable modem:

```
! Discards all traffic that does not match one of the LLC filters
option 11 instance 101 hex 30 82 00 0F 06 0A 2B 06 01 02 01 45 01 06 01 00 02 01 01
! Defines filter 1 to allow IP traffic to pass on all interfaces
option 11 instance 102 hex 0B 15 30 82 00 11 06 0C 2B 06 01 02 01 45 01 06 02 01 02 01 02 01 05
option 11 instance 103 hex 0B 15 30 82 00 11 06 0C 2B 06 01 02 01 45 01 06 02 01 03 01 02 01 00
option 11 instance 104 hex 0B 15 30 82 00 11 06 0C 2B 06 01 02 01 45 01 06 02 01 04 01 02 01 01
option 11 instance 105 hex 0B 16 30 82 00 12 06 0C 2B 06 01 02 01 45 01 06 02 01 05 01 02 02 08 00
option 11 instance 106 hex 0B 15 30 82 00 11 06 0C 2B 06 01 02 01 45 01 06 02 01 02 01 02 01 01
! Defines filter 2 to allow IP ARP traffic to pass on all interfaces
option 11 instance 107 hex 0B 15 30 82 00 11 06 0C 2B 06 01 02 01 45 01 06 02 01 02 02 02 01 05
option 11 instance 108 hex 0B 15 30 82 00 11 06 0C 2B 06 01 02 01 45 01 06 02 01 03 02 02 01 00
option 11 instance 109 hex 0B 15 30 82 00 11 06 0C 2B 06 01 02 01 45 01 06 02 01 04 02 02 01 01
option 11 instance 110 hex 0B 16 30 82 00 12 06 0C 2B 06 01 02 01 45 01 06 02 01 05 02 02 02 08 06
option 11 instance 111 hex 0B 15 30 82 00 11 06 0C 2B 06 01 02 01 45 01 06 02 01 02 02 02 01 01
```

Specifying a Filter to Block Microsoft NetBIOS Networking and File-Sharing Traffic

This section illustrates the following filters for IP traffic:

- Filter 1 blocks all TCP traffic on all interfaces to destination ports 137–139 (Microsoft NetBIOS networking and file-sharing traffic)
- Filter 2 blocks all UDP traffic on all interfaces to destination ports 137–139 (Microsoft NetBIOS networking and file-sharing traffic)
- Filter 3 blocks all inbound UDP traffic on the Ethernet interface from source ports 67 and 68 (DHCP and bootp servers)
- All other IP traffic that does not match one of these filters is allowed to pass.

These filters are created by creating instances of the docsDevFilterIpEntry table in DOCS-CABLE-DEVICE-MIB. Table 15 shows the SNMP attributes that must be set to activate these filters. Following this table are the **cable config-file** commands that create a DOCSIS configuration file that sets these attributes.



Note

The values in Table 15 that are marked with an asterisk are the default values and do not need to be specified to create the filter.

Table 15 Setting Attributes in docsDevFilterIpEntry to Block Microsoft Networking and File Sharing

Object ID Number / Name	Type	Value	Description
1.3.6.1.2.1.69.1.6.3.0 docsDevFilterIpDefault.0	Integer	2	Sets the default behavior for IP packets, which is to allow any IP packet to pass if it does not match an activated filter.

Filter 1—Blocks TCP traffic to destination ports 137–139 on all interfaces

Table 15 *Setting Attributes in docsDevFilterIpEntry to Block Microsoft Networking and File Sharing (continued)*

Object ID Number / Name	Type	Value	Description
1.3.6.1.2.1.69.1.6.4.1.2.1 docsDevFilterIpStatus.1	Integer	5	Creates IP filter number 1 but does not activate it yet.
1.3.6.1.2.1.69.1.6.4.1.3.1 docsDevFilterIpControl.1	Integer	1*	Discards all IP packets matching filter number 1.
1.3.6.1.2.1.69.1.6.4.1.4.1 docsDevFilterIpIfIndex.1	Integer	0	Applies this filter to all interfaces on the cable modem.
1.3.6.1.2.1.69.1.6.4.1.5.1 docsDevFilterIpDirection.1	Integer	3	Applies this filter to both inbound and outbound traffic.
1.3.6.1.2.1.69.1.6.4.1.6.1 docsDevFilterIpBroadcast.1	Integer	2*	Applies this filter to all traffic (including broadcast and multicast traffic).
1.3.6.1.2.1.69.1.6.4.1.7.1 docsDevFilterIpSaddr.1	IP Address	0.0.0.0*	Matches any source IP address.
1.3.6.1.2.1.69.1.6.4.1.8.1 docsDevFilterIpSmask.1	IP Address	0.0.0.0*	
1.3.6.1.2.1.69.1.6.4.1.9.1 docsDevFilterIpDaddr.1	IP Address	0.0.0.0*	Matches any destination IP address.
1.3.6.1.2.1.69.1.6.4.1.10.1 docsDevFilterIpDmask.1	IP Address	0.0.0.0*	
1.3.6.1.2.1.69.1.6.4.1.11.1 docsDevFilterIpProtocol.1	Integer	6	Matches TCP packets.
1.3.6.1.2.1.69.1.6.4.1.12.1 docsDevFilterIpSourcePortLow.1	Integer	0*	Applies this filter to traffic for all source ports (0–65535).
1.3.6.1.2.1.69.1.6.4.1.13.1 docsDevFilterIpSourcePortHigh.1	Integer	65535*	
1.3.6.1.2.1.69.1.6.4.1.14.1 docsDevFilterIpDestPortLow.1	Integer	137	Applies this filter to traffic for destination ports 137–139.
1.3.6.1.2.1.69.1.6.4.1.15.1 docsDevFilterIpDestPortHigh.1	Integer	139	
1.3.6.1.2.1.69.1.6.4.1.2.1 docsDevFilterIpStatus.1	Integer	1	Activates this filter.
Filter 2—Blocks UDP traffic to destination ports 137–139 on all interfaces			
1.3.6.1.2.1.69.1.6.4.1.2.2 docsDevFilterIpStatus.2	Integer	5	Creates IP filter number 2 but does not activate it yet.
1.3.6.1.2.1.69.1.6.4.1.3.2 docsDevFilterIpControl.2	Integer	1*	Discards all IP packets matching filter number 2.
1.3.6.1.2.1.69.1.6.4.1.4.2 docsDevFilterIpIfIndex.2	Integer	0	Applies this filter to all interfaces on the cable modem.
1.3.6.1.2.1.69.1.6.4.1.5.2 docsDevFilterIpDirection.2	Integer	3	Applies this filter to both inbound and outbound traffic.
1.3.6.1.2.1.69.1.6.4.1.6.2 docsDevFilterIpBroadcast.2	Integer	2*	Applies this filter to all traffic (including broadcast and multicast traffic).

Table 15 Setting Attributes in docsDevFilterIpEntry to Block Microsoft Networking and File Sharing (continued)

Object ID Number / Name	Type	Value	Description
1.3.6.1.2.1.69.1.6.4.1.7.2 docsDevFilterIpSaddr.2	IP Address	0.0.0.0*	Matches any source IP address.
1.3.6.1.2.1.69.1.6.4.1.8.2 docsDevFilterIpSmask.2	IP Address	0.0.0.0*	
1.3.6.1.2.1.69.1.6.4.1.9.2 docsDevFilterIpDaddr.2	IP Address	0.0.0.0*	Matches any destination IP address.
1.3.6.1.2.1.69.1.6.4.1.10.2 docsDevFilterIpDmask.2	IP Address	0.0.0.0*	
1.3.6.1.2.1.69.1.6.4.1.11.2 docsDevFilterIpProtocol.2	Integer	17	Matches UDP packets.
1.3.6.1.2.1.69.1.6.4.1.12.2 docsDevFilterIpSourcePortLow.2	Integer	0*	Applies this filter to traffic for all source ports (0–65535).
1.3.6.1.2.1.69.1.6.4.1.13.2 docsDevFilterIpSourcePortHigh.2	Integer	65535*	
1.3.6.1.2.1.69.1.6.4.1.14.2 docsDevFilterIpDestPortLow.2	Integer	137	Applies this filter to traffic for destination ports 137–139.
1.3.6.1.2.1.69.1.6.4.1.15.2 docsDevFilterIpDestPortHigh.2	Integer	139	
1.3.6.1.2.1.69.1.6.4.1.2.2 docsDevFilterIpStatus.2	Integer	1	Activates this filter.
Filter 3—Blocks DHCP servers on the Ethernet network (all inbound UDP traffic on the Ethernet interface from source port 67)			
1.3.6.1.2.1.69.1.6.4.1.2.3 docsDevFilterIpStatus.3	Integer	5	Creates IP filter number 3 but does not activate it yet.
1.3.6.1.2.1.69.1.6.4.1.3.3 docsDevFilterIpControl.3	Integer	1	Discards all IP packets matching filter number 3.
1.3.6.1.2.1.69.1.6.4.1.4.3 docsDevFilterIpIfIndex.3	Integer	1	Applies this filter to all interfaces on the cable modem.
1.3.6.1.2.1.69.1.6.4.1.5.3 docsDevFilterIpDirection.3	Integer	1	Applies this filter to inbound traffic only.
1.3.6.1.2.1.69.1.6.4.1.6.3 docsDevFilterIpBroadcast.3	Integer	2*	Applies this filter to all traffic (including broadcast and multicast traffic).
1.3.6.1.2.1.69.1.6.4.1.7.3 docsDevFilterIpSaddr.3	IP Address	0.0.0.0*	Matches any source IP address.
1.3.6.1.2.1.69.1.6.4.1.8.3 docsDevFilterIpSmask.3	IP Address	0.0.0.0*	
1.3.6.1.2.1.69.1.6.4.1.9.3 docsDevFilterIpDaddr.3	IP Address	0.0.0.0*	Matches any destination IP address.
1.3.6.1.2.1.69.1.6.4.1.10.3 docsDevFilterIpDmask.3	IP Address	0.0.0.0*	
1.3.6.1.2.1.69.1.6.4.1.11.3 docsDevFilterIpProtocol.3	Integer	17	Matches UDP packets.

Table 15 Setting Attributes in docsDevFilterIpEntry to Block Microsoft Networking and File Sharing (continued)

Object ID Number / Name	Type	Value	Description
1.3.6.1.2.1.69.1.6.4.1.12.3 docsDevFilterIpSourcePortLow.3	Integer	67	Applies this filter to traffic from source ports 67 and 68.
1.3.6.1.2.1.69.1.6.4.1.13.3 docsDevFilterIpSourcePortHigh.3	Integer	68	
1.3.6.1.2.1.69.1.6.4.1.14.3 docsDevFilterIpDestPortLow.3	Integer32	0*	Applies this filter to traffic for all destination ports.
1.3.6.1.2.1.69.1.6.4.1.15.3 docsDevFilterIpDestPortHigh.3	Integer32	65535*	
1.3.6.1.2.1.69.1.6.4.1.2.3 docsDevFilterIpStatus.3	Integer	1	Activates this filter.

The following commands appear in the CMTS Cisco IOS configuration file that creates the DOCSIS configuration file that sets up these filters on the cable modem. The command lines that start with an exclamation point (!) are the default values and do not need to be specified to create the filters.

```
cable config-file setsnmp.cm
! Sets the default behavior for IP traffic, to allow traffic that does not match any filters to pass
option 11 instance 200 hex 30 82 00 0F 06 0A 2B 06 01 02 01 45 01 06 03 00 02 01 02
!
! These lines define filter 1 to block TCP traffic to ports 137–139 on all interface
option 11 instance 201 hex 30 82 00 11 06 0C 2B 06 01 02 01 45 01 06 04 01 02 01 02 01 05
option 11 instance 202 hex 30 82 00 11 06 0C 2B 06 01 02 01 45 01 06 04 01 03 01 02 01 01
option 11 instance 203 hex 30 82 00 11 06 0C 2B 06 01 02 01 45 01 06 04 01 04 01 02 01 00
option 11 instance 204 hex 30 82 00 11 06 0C 2B 06 01 02 01 45 01 06 04 01 05 01 02 01 03
!option 11 instance 205 hex 30 82 00 11 06 0C 2B 06 01 02 01 45 01 06 04 01 06 01 02 01 02
!option 11 instance 206 hex 30 82 00 14 06 0C 2B 06 01 02 01 45 01 06 04 01 07 01 40 04 00 00 00 00
!option 11 instance 207 hex 30 82 00 14 06 0C 2B 06 01 02 01 45 01 06 04 01 08 01 40 04 00 00 00 00
!option 11 instance 208 hex 30 82 00 14 06 0C 2B 06 01 02 01 45 01 06 04 01 09 01 40 04 00 00 00 00
!option 11 instance 209 hex 30 82 00 14 06 0C 2B 06 01 02 01 45 01 06 04 01 0A 01 40 04 00 00 00 00
option 11 instance 210 hex 30 82 00 11 06 0C 2B 06 01 02 01 45 01 06 04 01 0B 01 02 01 06
!option 11 instance 211 hex 30 82 00 11 06 0C 2B 06 01 02 01 45 01 06 04 01 0C 01 02 01 00
!option 11 instance 212 hex 30 82 00 13 06 0C 2B 06 01 02 01 45 01 06 04 01 0D 01 02 03 00 FF FF
option 11 instance 213 hex 30 82 00 12 06 0C 2B 06 01 02 01 45 01 06 04 01 0E 01 02 02 00 89
option 11 instance 214 hex 30 82 00 12 06 0C 2B 06 01 02 01 45 01 06 04 01 0F 01 02 02 00 8B
option 11 instance 215 hex 30 82 00 11 06 0C 2B 06 01 02 01 45 01 06 04 01 02 01 02 01 01
!
!These lines define filter 2 to block UDP traffic to ports 137–139 on all interfaces
option 11 instance 216 hex 30 82 00 11 06 0C 2B 06 01 02 01 45 01 06 04 01 02 02 02 01 05
option 11 instance 217 hex 30 82 00 11 06 0C 2B 06 01 02 01 45 01 06 04 01 03 02 02 01 01
option 11 instance 218 hex 30 82 00 11 06 0C 2B 06 01 02 01 45 01 06 04 01 04 02 02 01 00
option 11 instance 219 hex 30 82 00 11 06 0C 2B 06 01 02 01 45 01 06 04 01 05 02 02 01 03
!option 11 instance 220 hex 30 82 00 11 06 0C 2B 06 01 02 01 45 01 06 04 01 06 02 02 01 02
!option 11 instance 221 hex 30 82 00 14 06 0C 2B 06 01 02 01 45 01 06 04 01 07 02 40 04 00 00 00 00
!option 11 instance 222 hex 30 82 00 14 06 0C 2B 06 01 02 01 45 01 06 04 01 08 02 40 04 00 00 00 00
!option 11 instance 223 hex 30 82 00 14 06 0C 2B 06 01 02 01 45 01 06 04 01 09 02 40 04 00 00 00 00
!option 11 instance 224 hex 30 82 00 14 06 0C 2B 06 01 02 01 45 01 06 04 01 0A 02 40 04 00 00 00 00
option 11 instance 225 hex 30 82 00 11 06 0C 2B 06 01 02 01 45 01 06 04 01 0B 02 02 01 11
!option 11 instance 226 hex 30 82 00 11 06 0C 2B 06 01 02 01 45 01 06 04 01 0C 02 02 01 00
!option 11 instance 227 hex 30 82 00 13 06 0C 2B 06 01 02 01 45 01 06 04 01 0D 02 02 03 00 FF FF
option 11 instance 228 hex 30 82 00 12 06 0C 2B 06 01 02 01 45 01 06 04 01 0E 02 02 02 00 89
option 11 instance 229 hex 30 82 00 12 06 0C 2B 06 01 02 01 45 01 06 04 01 0F 02 02 02 00 8B
option 11 instance 230 hex 30 82 00 11 06 0C 2B 06 01 02 01 45 01 06 04 01 02 02 02 01 01
!These lines define filter 3 to block DHCP and BOOTP traffic on the Ethernet interface
option 11 instance 231 hex 30 82 00 11 06 0C 2B 06 01 02 01 45 01 06 04 01 02 03 02 01 05
option 11 instance 232 hex 30 82 00 11 06 0C 2B 06 01 02 01 45 01 06 04 01 03 03 02 01 01
```

```

option 11 instance 233 hex 30 82 00 11 06 0C 2B 06 01 02 01 45 01 06 04 01 04 03 02 01 01
option 11 instance 234 hex 30 82 00 11 06 0C 2B 06 01 02 01 45 01 06 04 01 05 03 02 01 01
!option 11 instance 235 hex 30 82 00 11 06 0C 2B 06 01 02 01 45 01 06 04 01 06 03 02 01 02
!option 11 instance 236 hex 30 82 00 14 06 0C 2B 06 01 02 01 45 01 06 04 01 07 03 40 04 00 00 00 00
!option 11 instance 237 hex 30 82 00 14 06 0C 2B 06 01 02 01 45 01 06 04 01 08 03 40 04 00 00 00 00
!option 11 instance 238 hex 30 82 00 14 06 0C 2B 06 01 02 01 45 01 06 04 01 09 03 40 04 00 00 00 00
!option 11 instance 239 hex 30 82 00 14 06 0C 2B 06 01 02 01 45 01 06 04 01 0A 03 40 04 00 00 00 00
option 11 instance 240 hex 30 82 00 11 06 0C 2B 06 01 02 01 45 01 06 04 01 0B 03 02 01 11
option 11 instance 241 hex 30 82 00 11 06 0C 2B 06 01 02 01 45 01 06 04 01 0C 03 02 01 43
option 11 instance 242 hex 30 82 00 11 06 0C 2B 06 01 02 01 45 01 06 04 01 0D 03 02 01 44
!option 11 instance 243 hex 30 82 00 11 06 0C 2B 06 01 02 01 45 01 06 04 01 0E 03 02 01 00
!option 11 instance 244 hex 30 82 00 13 06 0C 2B 06 01 02 01 45 01 06 04 01 0F 03 02 03 00 FF FF
option 11 instance 245 hex 30 82 00 11 06 0C 2B 06 01 02 01 45 01 06 04 01 02 03 02 01 01

```

Specifying Vendor-Specific Information Fields (Option 43)

The **cable config-file option** command allows you to specify DOCSIS configuration file parameters that are not supported by other **cable config-file** commands. The most common use of the **cable config-file option** command is to specify vendor-specific information field (**option 43**), which vendors use to implement features that are unique to their products.

When you use the vendor-specific option, you must specify the data using the **hex** option. The hexadecimal data must be presented in the DOCSIS Type/Length/Value (TLV) format, where the first byte specifies the suboption type, the second byte specifies the length of the data, and the remaining bytes specify the data itself. The exact meaning of the suboption type and data values is defined by each vendor.

For example, Cisco cable modems support a vendor-specific suboption (128) that instructs the cable modem to download and execute a Cisco IOS configuration file. The data for this suboption is the fully qualified path name of the Cisco IOS configuration file on the TFTP server. Other vendors, however, could define vendor-specific suboption 128 to have a totally different function.

To ensure that a vendor-specific option is executed only by equipment that supports that option, the vendor ID must always be the first part of the data in an **option 43** command. The suboption number for the vendor ID function is **08**, and the data is the 3-byte organization unique identifier (OUI) for that vendor, as issued by the Institute of Electrical and Electronics Engineers (IEEE).

The vendor could have defined a global OUI for all of their equipment, or they could have requested a separate OUI ID for different products or family of products. For example, the global OUI for Cisco equipment is **00 00 0C**.



Note

Each **option 43** command must specify one and only one vendor ID, and the vendor ID must be the first TLV in the **hex** data string.

This section demonstrates how to use the **option 43** command to configure the following Cisco vendor-specific options:

- [Specifying the Download of a Cisco IOS Configuration File, page 192](#)
- [Typical H.323 VoIP Configuration, page 192](#)

Specifying the Download of a Cisco IOS Configuration File

The following example shows how to configure a Cisco uBR924, Cisco uBR925, or Cisco CVA122 so that it downloads a Cisco IOS configuration file named **ios.cfg**. Two vendor-specific options are included: suboption 8, which specifies the vendor ID, and suboption 128, which specifies the configuration file name.

```
router(config)# cable config-file iosfile.cm
router(config-file)# option 43 hex 08:03:00:00:0C:80:07:69:6F:73:2E:63:66:67
router(config-file)# exit
router(config)#
```

The hexadecimal data shown in this command consists of the three TLVs shown in [Table 16](#):

Table 16 TLV Values for Sample Option 43 Command

Type	Length	Value
TLV 1—Vendor ID, Suboption 8		
08	03	00:00:0C (the ID for Cisco cable equipment)
TLV2—Cisco IOS Configuration File, Suboption 128		
80	07	69:6F:73:2E:63:66:67 (ASCII hexadecimal bytes for ios.cfg)

Typical H.323 VoIP Configuration

The following demonstrates how to configure a Cisco uBR924, Cisco uBR925, or Cisco CVA122 router for VoIP operations using the H.323 protocol. The configuration begins by defining a service class for voice operations and then uses **option 43** commands to specify the Cisco IOS commands that are needed to configure the router for VoIP operations.

```
router(config)# cable config-file voiph323.cm
router(config-file)# service-class 1 max-downstream 2000000
router(config-file)# service-class 1 max-upstream 1000000
router(config-file)# service-class 1 priority 5
router(config-file)# service-class 1 guaranteed-upstream 128000
router(config-file)# service-class 1 max-burst 1800
router(config-file)# service-class 1 privacy
router(config-file)# option 43 instance 1 hex 08:03:00:00:0C:0A:01:02:0B:09:01:01:
05:02:04:00:02:71:00
router(config-file)# option 43 instance 2 hex 2B:1C:08:03:00:00:0C:83:15:65:6E:61:62:
6C:65:20:70:61:73:73:77:6F:72:64:20:63:61:62:6C:65
router(config-file)# option 43 instance 3 hex 2B:0E:08:03:00:00:0C:83:07:67:61:74:65:
77:61:79
router(config-file)# option 43 instance 4 hex 2B:1D:08:03:00:00:0C:83:16:69:6E:74:65:
72:66:61:63:65:20:63:61:62:6C:65:2D:6D:6F:64:65:6D:30
router(config-file)# option 43 instance 5 hex 2B:22:08:03:00:00:0C:83:1B:68:33:32:33:
2D:67:61:74:65:77:61:79:20:76:6F:69:70:20:69:6E:74:65:72:66:61:63:65
router(config-file)# option 43 instance 6 hex 2B:3B:08:03:00:00:0C:83:34:68:33:32:33:
2D:67:61:74:65:77:61:79:20:76:6F:69:70:20:69:64:20:67:6B:2D:72:65:73:20:69:70:61:64:64:
72:20:31:39:32:2E:31:36:38:2E:32:2E:36:33:20:31:37:31:39
router(config-file)# option 43 instance 7 hex 2B:27:08:03:00:00:0C:83:20:68:33:32:33:
2D:67:61:74:65:77:61:79:20:76:6F:69:70:20:74:65:63:68:2D:70:72:65:66:69:78:20:31:23
router(config-file)# option 43 instance 8 hex 2B:13:08:03:00:00:0C:83:0C:6C:69:6E:
65:20:76:74:79:20:30:20:34
router(config-file)# option 43 instance 9 hex 2B:0C:08:03:00:00:0C:83:05:6C:6F:67:69:6E
router(config-file)# option 43 instance 10 hex 2B:15:08:03:00:00:0C:83:0E:70:61:73:73:
77:6F:72:64:20:63:61:62:6C:65
router(config-file)# option 43 instance 11 hex 2B:17:08:03:00:00:0C:83:10:65:78:65:63:
2D:74:69:6D:65:6F:75:74:20:30:20:30
```



```
router(config-file)# option 43 instance 12 hex 2B:0A:08:03:00:00:0C:83:03:65:6E:64
router(config-file)# exit
router(config)#
```

Table 17 shows the TLVs for each instance of the option 43 command, showing the commands and other functions that each performs.

Table 17 TLV Values to Enable the Cisco Cable Monitor

Type	Length	Value
Instance 1—Enables the two voice ports and sets the IP precedence value		
08	03	00:00:0C (the ID for Cisco cable equipment)
0A	01	02 (enables two voice ports)
0B	09	01:01:05 (specifies IP precedence level 5) 02:04:00:02:71:0 (sets the IP precedence for a downstream rate-limit of 160 kbps)
Instance 2—enable password cable command		
08	03	00:00:0C (the ID for Cisco cable equipment)
83	15	83:15:65:6E:61:62:6C:65:20:70:61:73:73:77:6F:72:64:20:63:61:62:6C:65 (enable password cable command)
Instance 3—gateway command		
08	03	00:00:0C (the ID for Cisco cable equipment)
83	07	83:07:67:61:74:65:77:61:79 (gateway command)
Instance 4—interface cable-modem0 command		
08	03	00:00:0C (the ID for Cisco cable equipment)
83	16	83:16:69:6E:74:65:72:66:61:63:65:20:63:61:62:6C:65:2D:6D:6F:64:65:6D:30 (interface cable-modem0 command)
Instance 5—h323-gateway voip interface command		
08	03	00:00:0C (the ID for Cisco cable equipment)
83	1B	83:1B:68:33:32:33:2D:67:61:74:65:77:61:79:20:76:6F:69:70:20:69:6E:74:65:72:66:61:63:65 (h323-gateway voip interface command)
Instance 6—h323-gateway h323-gavoip id gk-res ipaddr 192.168.2.63 1719 command		
08	03	00:00:0C (the ID for Cisco cable equipment)
83	34	83:34:68:33:32:33:2D:67:61:74:65:77:61:79:20:76:6F:69:70:20:69:64:20:67:6B:2D:72:65:73:20:69:70:61-64:64:72:20:31:39:32:2E:31:36:38:2E:32:2E:36:33:20:31:37:31:39 (h323-gateway h323-gavoip id gk-res ipaddr 192.168.2.63 1719 command)
Instance 7—h323-gateway voip tech-prefix 1# command		
08	03	00:00:0C (the ID for Cisco cable equipment)
83	20	83:20:68:33:32:33:2D:67:61:74:65:77:61:79:20:76:6F:69:70:20-74:65:63:68:2D:70:72:65:66:69:78:20: 31:23 (h323-gateway voip tech-prefix 1# command)

Table 17 TLV Values to Enable the Cisco Cable Monitor

Type	Length	Value
Instance 8—line vty 0 4 command		
08	03	00:00:0C (the ID for Cisco cable equipment)
83	0C	83:0C:6C:69:6E:65:20:76:74:79:20:30:20:34 (line vty 0 4 command)
Instance 9—login command		
08	03	00:00:0C (the ID for Cisco cable equipment)
83	05	83:05:6C:6F:67:69:6E (login command)
Instance 10—password cable command		
08	03	00:00:0C (the ID for Cisco cable equipment)
83	0E	83:0E:70:61:73:73:77:6F:72:64:20:63:61:62:6C:65 (password cable command)
Instance 11—exec-timeout 0 0 command		
08	03	00:00:0C (the ID for Cisco cable equipment)
83	10	83:10:65:78:65:63:2D:74:69:6D:65:6F:75:74:20:30: 20:30 (exec-timeout 0 0 command)
Instance 12—end command		
08	03	00:00:0C (the ID for Cisco cable equipment)
83	03	83:03:65:6E:64 (end command)

Configuring the Router's Onboard TFTP Server

To enable the router's onboard TFTP server, so that it can transfer the DOCSIS configuration files to the cable modems, use the following procedure.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **service udp-small servers max-servers no limit**
4. **tftp-server server**
5. **tftp-server device:filename alias tftp-filename**
6. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	service udp-small servers max-servers no limit Example: Router(config)# service udp-small servers max-servers no limit Router(config)#	Enables the router's onboard User Datagram Protocol (UDP) servers, such as the TFTP server, and allows an unlimited number of sessions.
Step 4	tftp-server server Example: Router(config)# tftp-server server Router(config)#	Enables the TFTP server.
Step 5	tftp-server device:filename alias tftp-filename Example: Router(config)# tftp-server disk0:gold.cm alias gold.cm Router(config)#	(Optional) Specifies that when a request is made for a file named <i>tftp-filename</i> , the TFTP server should transfer the file named <i>filename</i> from the specified <i>device</i> file system. Typically, device is flash , disk0 , or disk1 . Note This command is needed only for configuration and other files that are created elsewhere and are copied on to the router's Flash memory and PCMCIA memory cards. This command is not needed for the DOCSIS configuration files that are created with the cable config-file command.
Step 6	r exit Example: Router(config)# exit Router#	Exits global configuration mode.

Configuration Examples for the Internal DOCSIS Configuration File Generator

This section provides DOCSIS configuration file examples as well as a typical DHCP server configuration example.

- [Platinum.cm, page 196](#)
- [Disable.cm, page 196](#)
- [Configuration Files and DHCP Server Configuration, page 197](#)

Platinum.cm

The following example creates a DOCSIS configuration file named platinum.cm with the following parameters:

- Service class 1 that specifies a maximum upstream data rate of 10 kbps, a guaranteed upstream data rate of 1 kbps, a maximum downstream rate of 100 kbps, and a maximum burst size of 1600 bytes.
- A maximum of 30 CPE devices can access the cable network through this cable modem.
- Timestamps are generated to prevent cable modems from caching and replaying the DOCSIS configuration files.

```
!
cable config-file platinum.cm
service-class 1 max-upstream 10
service-class 1 guaranteed-upstream 1
service-class 1 max-downstream 100
service-class 1 max-burst 1600
cpe max 30
timestamp
```

Platinum.cm with BPI Enabled

The following example uses the same platinum.cm file that is shown above, but with the **privacy** and **service-class privacy** commands that are needed to enable BPI operations on the cable modem.

```
!
cable config-file platinum.cm
privacy
service-class 1 max-upstream 10
service-class 1 guaranteed-upstream 1
service-class 1 max-downstream 100
service-class 1 max-burst 1600
service-class 1 privacy
cpe max 30
timestamp
```

Disable.cm

The following configuration example creates a DOCSIS configuration file named disable.cm that allows the cable modem to come online but prevents any of its CPE devices from accessing the cable network. The maximum upstream rate is limited to 1 kbps.

```
cable config-file disable.cm
access-denied
service-class 1 max-upstream 1
service-class 1 max-burst 1600
timestamp
```

Configuration Files and DHCP Server Configuration

The following example shows the following DOCSIS configuration files being configured:

- test.cm = Allows each cable modem to have up to four CPE devices and creates service class 1. Timestamps are also used to ensure cable modems cannot cache the configuration file and replay it later.
- denied.cm = Instructs the cable modem to deny access to the cable network to any of the CPE devices that are connected to the cable modem.

This example also shows a typical DHCP server configuration.

```
service udp-small-servers max-servers no-limit
cable time-server
!
cable config-file test.cm
cpe max 4
service-class 1 priority 2
service-class 1 max-upstream 128
service-class 1 max-downstream 1000
timestamp
cable config-file denied.cm
access-denied
!
!
ip dhcp pool modems-c3
network 10.30.128.0 255.255.240.0
bootfile test.cm
next-server 10.30.128.1
default-router 10.30.128.1
option 7 ip 10.30.128.1
option 4 ip 10.30.128.1
option 2 hex 0000.0000
```

Additional References

For additional information related to the Internal DOCSIS Configuration File Generator, refer to the following references:

Related Documents

Related Topic	Document Title
Configuring Baseline Privacy Interface (BPI) Encryption	To use BPI encryption, the Cisco CMTS must also be configured for BPI or BPI+ encryption, using the cable privacy command. For information on the command, refer to the Cisco Broadband Cable Command Reference Guide on Cisco.com and on the Documentation CD-ROM.
Configuring the Trivial File Transfer Protocol (TFTP) Server	For information on configuring the router's onboard TFTP server, refer to the "Configuring Basic File Transfer Services" chapter in the Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2 on Cisco.com.
Creating an All-in-One Configuration	For information on how to configure a Cisco CMTS that acts as a Dynamic Host Configuration Protocol (DHCP), Time-of-Day (ToD), and TFTP server in an "all-in-one configuration," refer to the Configuring DHCP, ToD, TFTP services on Cisco's CMTS: All-In-One Configuration guide on Cisco.com.
Using MAX CPE Parameters	For information on the MAX CPE and related parameters, see the chapter <i>Maximum CPE or Host Parameters for the Cisco CMTS</i> in the Cisco CMTS Feature Guide, at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/cable/cab_rout/cmtsfg/index.htm
Using a Shared Secret	For information on using a shared secret to protect DOCSIS configuration files from interception or alteration, see the description of the cable shared-secret command in the <i>Cisco CMTS Commands</i> chapter in the Cisco Broadband Cable Command Reference Guide, at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/cable/bbcmref/index.htm

Standards

Standards ¹	Title
ANSI/SCTE 22-1 2002 (formerly SP-RFI-C01-011119)	Data-Over-Cable Service Interface Specification DOCSIS 1.0 Radio Frequency Interface (RFI) (http://www.cablemodem.com)
ANSI/SCTE 22-2 2002 (formerly SP-BPI-I01-970922)	Data-Over-Cable Service Interface Specification DOCSIS 1.0 Baseline Privacy Interface (BPI)

Standards ¹	Title
SP-RFIV1.1-I09-020830	Data-Over-Cable Service Interface Specifications Radio Frequency Interface Specification, version 1.1
SP-BPI+-I09-020830	Data-Over-Cable Service Interface Specifications Baseline Privacy Plus Interface Specification (http://www.cablemodem.com)

1. Not all supported standards are listed.

MIBs

MIBs ¹	MIBs Link
- DOCS-CABLE-DEVICE-MIB (RFC 2669) - DOCS-IF-MIB (RFC 2670)	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

1. Not all supported MIBs are listed.

RFCs

RFCs ¹	Title
RFC 1918	<i>Address Allocation for Private Internets</i>
RFC 2669	<i>DOCSIS Cable Device MIB Cable Device Management Information Base for DOCSIS compliant Cable Modems and Cable Modem Termination Systems (DOCS-CABLE-DEVICE-MIB)</i>
RFC 2670	<i>Radio Frequency (RF) Interface Management Information Base for MCNS/DOCSIS Compliant RF Interfaces (DOCS-IF-MIB)</i>

1. Not all supported RFCs are listed.

Technical Assistance

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

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, TeleRouter, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0502R)

Copyright © 2003 Cisco Systems, Inc. All rights reserved.



Maximum CPE and Host Parameters for the Cisco CMTS

This document describes how to use the different methods to control subscriber access that are allowed by the Data-over-Cable Service Interface Specifications (DOCSIS) for use on cable networks.

Feature Specifications for the MAX CPE and Host Parameters

Feature History

Release	Modification
Release 12.0(6)SC	The cable max-hosts and cable modem max-hosts commands were introduced for the Cisco uBR7200 series routers.
Release 12.0(10)SC	The cable modem max-cpe command was introduced for the Cisco uBR7200 series routers.
Release 12.1(2)EC1	Support for these features was added to the Cisco IOS Release 12.1 EC train for the Cisco uBR7200 series routers.
Release 12.1(5)EC	Support for these features was added for the Cisco uBR7100 series routers.
Release 12.2(4)BC1	Support for these features was added to the Cisco IOS Release 12.2 BC train for the Cisco uBR7100 series, Cisco uBR7200 series, and Cisco uBR10012 routers.

Supported Platforms

Cisco uBR7100 series, Cisco uBR7200 series, and Cisco uBR10012 universal broadband routers.

Finding Support Information for Platforms and Cisco IOS Software Images

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

Contents

- [Information About the MAX CPE and Host Parameters, page 202](#)
- [How to Configure the MAX CPE and Host Parameters, page 209](#)
- [Configuration Examples for the MAX CPE and Host Parameters, page 213](#)
- [Additional References, page 215](#)

Information About the MAX CPE and Host Parameters

The DOCSIS specification includes a number of provisions to allow service providers to control the exact number of subscribers who can access the network through any particular cable modem:

- **MAX CPE**—This required parameter is configured in DOCSIS 1.0 configuration files (TLV 18) and controls how many different CPE devices can access the network during the current session. (This parameter is always enforced, and if it is not specified in the configuration file, it defaults to 1.)
- **MAX CPE IP**—This optional parameter is configured in DOCSIS 1.1 configuration files (TLV 35), or by adding a row to the docsSubMgtCpeControlTable table in the DOCSIS Subscriber Management MIB (DOCS-SUBMGT-MIB). It specifies the maximum number of simultaneous IP addresses that are permitted behind a cable modem at any one time. Both
- **MAX Host**—This optional parameter is configured on the Cisco CMTS, and specifies the maximum number of CPE devices (MAC addresses) that the CMTS will allow to have network access behind a particular cable modem. You can use one of three CLI commands to set the value of this parameter for a particular cable modem (**cable modem max-hosts**), for all cable modems on a particular cable interface (**cable max-hosts**), or for all cable modems on the Cisco CMTS (**cable modem max-cpe**).

**Note**

In addition, the DOCSIS configuration file contains a Network Access parameter that specifies whether the CPE devices behind the cable modem can access the cable network. If this parameter is set to Disabled, no CPE devices behind a cable modem are able to access the network, regardless of the settings of the MAX CPE, MAX CPE IP, and MAX Host parameters.

**Tip**

Also, the Cisco CMTS lists offline cable modems in its internal database for 24 hours. The CMTS does not reset the CPE counts for these offline cable modems until the 24 hour period expires and the cable modems come back online. If the cable modems come back online before the 24 hour period expires, the CMTS continues to use the existing CPE counts.

All of these methods are similar in purpose, but they are configured differently and have a different impact on cable modems and their CPE devices.

The cable modem enforces the MAX CPE and MAX CPE IP values, and the CMTS enforces the MAX Host value. Because CPE devices can come online and offline at any time, it is important to understand how these different parameters interact, and how the cable modem and CMTS enforce them.

**Note**

The MAX CPE parameter provides Layer 2 control of CPE devices. The MAX CPE IP parameter provides Layer 3 control of CPE devices. The two methods are complimentary but not otherwise related.

MAX CPE

In DOCSIS 1.0 cable networks, the MAX CPE parameter is the primary means of controlling the number of CPE devices that can connect to the cable network using any particular cable modem. This parameter is configured in the DOCSIS configuration file (TLV 18) and controls how many different CPE devices can access the network during the current session. If not specified in the DOCSIS configuration file, it defaults to a value of 1.

**Note**

In DOCSIS 1.1 cable networks, the CMTS ignores the MAX CPE parameter that is specified in the DOCSIS configuration file, and uses the [MAX CPE IP](#) parameter instead.

Each time a new CPE device attempts to connect to the cable network, the cable modem logs its hardware (MAC) address. If the cable modem has not reached its MAX CPE number of MAC addresses yet, the new CPE device is allowed to access the network. If the cable modem has reached its MAX CPE limit, it drops the traffic from any additional CPE devices.

By default, the cable modem learns new MAC addresses on a first-come, first-served basis. You can also preconfigure the allowable MAC addresses for CPE devices by entering those MAC addresses in the DOCSIS configuration file (TLV 14). These cable modem gives these preconfigured MAC addresses preference in connecting to the network.

The DOCSIS specification does not allow cable modems to age out MAC addresses, so a MAC address stays in the cable modem's log table until the cable modem is reset. You should therefore think of this parameter as specifying the maximum number of CPE devices that can connect during any particular session, instead of the maximum number of CPE devices that can simultaneously connect to the cable network.

For example, if you set MAX CPE to 2, a customer could use their cable modem to connect a maximum of two CPE devices (two MAC addresses) to the cable network. A customer could choose to connect two PCs simultaneously to their cable modem and use both to access the network.

However, if the customer then disconnected these PCs and connected two new PCs, the cable modem would not allow the new PCs to come online, because they would be the third and fourth MAC addresses that are connected to the cable modem. The customer would have to reset the cable modem before being able to use the new PCs.

**Note**

The MAX CPE value, if present, must be a positive integer in DOCSIS 1.0 configuration files. This parameter can be zero in DOCSIS 1.1 configuration files, but if so, the cable modem uses a MAX CPE value of 1. If the MAX CPE parameter is not present in either type of DOCSIS configuration file, it defaults to 1.

MAX CPE IP

The MAX CPE IP parameter is applicable only in DOCSIS 1.1 cable networks. This parameter specifies whether the cable modem should perform IP address filtering on the CPE devices. If so, this attribute also specifies the maximum number of simultaneous IP addresses that are permitted behind the modem at any one time.

The MAX CPE IP parameter is configured in the DOCSIS configuration file (TLV 35), or by using SNMP commands to set the docsDevCpeIpMax attribute (in DOCS-CABLE-DEVICE-MIB) for the cable modem. By default, this parameter is not enabled and the Cisco CMTS does not actively manage CPE devices, unless you enable the use of the MAX CPE IP parameter by using the **cable submgt default active** command.

**Note**

In DOCSIS 1.1 networks, the CMTS ignores the MAX-CPE value (TLV 18) from the DOCSIS configuration file and uses the MAX CPE IP value instead.

If this feature is enabled, the cable modem learns the allowable IP addresses the first time that the CPE device sends an IP packet out into the network. IP addresses are added to the docsDevFilterCpeTable table. This address table is cleared automatically when the cable modem is reset or powered off, or you can manually clear the IP address table by setting the docsSubMgtCpeControlReset attribute in the appropriate table entry for this cable modem.

In DOCSIS 1.1 networks, the MAX CPE IP parameter can be configured as follows:

- If MAX CPE IP is set to -1, the cable modem does not filter any IP packets on the basis of their IP addresses, and CPE IP addresses are not added to the modem's CPE address table
- If MAX CPE IP is set to 0, the cable modem does not filter any IP packets on the basis of the IP addresses. However, the source IP addresses are still entered into the modem's CPE address table.
- If MAX CPE IP is set to a positive integer, it specifies the maximum number of IP addresses that can be entered into the modem's CPE address table. The modem compares the source IP address for packets it receives from CPE devices to the addresses in this table. If a match is found, the packet is processed; otherwise, the packet is dropped.

**Tip**

In Cisco IOS Release 12.2(8)BC1, a similar address filtering mechanism exists on the CMTS. See the description of the docsSubMgtCpeControlMaxCpeIp attribute in the DOCS-SUBMGT-MIB MIB for details. The CMTS uses the MAX CPE IP value as part of its own filtering process, but the two filters operate independently on the cable modem and CMTS.

MAX Host

The MAX Host parameter is configured on the Cisco CMTS and specifies the maximum number of CPE devices (MAC addresses) that the CMTS will allow to have network access. You can control this parameter for individual cable modems, for all cable modems on a particular cable interface, or for all cable modems on the Cisco CMTS, depending on the CLI command being used:

- **cable modem max-hosts**—Configures MAX Host for a particular cable modem.
- **cable max-hosts**—Configures MAX Host for all cable modems on a particular cable interface.
- **cable modem max-cpe**—Configures MAX Host for all cable modems on the Cisco CMTS. You can use the **unlimited** keyword to specify that the Cisco CMTS should not enforce a MAX Host limit for cable modems.

When this is enabled, the Cisco CMTS learns a MAC address the first time that the CPE device accesses the cable network. After the Cisco CMTS has logged the maximum number of MAC addresses specified by a MAX Host parameter, it will drop all traffic from CPE devices that have any other MAC address.

**Tip**

In DOCSIS 1.1 cable networks, when both the MAX CPE IP and MAX Host parameters are configured, the Cisco CMTS uses the lesser value to determine the maximum number of CPE devices that are allowed behind each cable modem.

**Note**

The entire MAX Host address table is cleared whenever the Cisco CMTS is reset. You can also clear an entry for a particular CPE device using the **clear cable host** command.

Specifying MAX Host and MAX CPE Values

Typically, you would set the MAX Host parameter to a number that is greater than the value for the cable modem's MAX CPE or MAX CPE IP parameter. This would allow customers to switch between multiple computers, without requiring them to reboot their cable modem, and without requiring any action on the part of the service provider's network administrators.

For example, if you set MAX CPE or MAX CPE IP to a value of 2 for a cable modem, then you could set the MAX Host parameter to a value of 4. This would enable the cable modem to connect four different CPE devices to the cable network, but only two of them could be online simultaneously.

However, if you set the MAX Host parameter to a number smaller than the value of MAX CPE or MAX CPE IP in the DOCSIS configuration file, then the MAX CPE or MAX CPE IP value always takes precedence. For example, if the MAX CPE value is 2 and the MAX Host value is 1, both the cable modem and CMTS allow up to two CPE devices to pass traffic for that cable modem.

Specifying an Unlimited Value for Max Host

The **cable modem max-cpe** command, which affects all cable modems on the CMTS, supports the **unlimited** keyword, which specifies that the CMTS should not enforce any limit on CPE devices. When you configure the CMTS with the unlimited **keyword**, this setting, you are allowing cable modems to support any number of CPE devices.

Do not use the **unlimited** option without also specifying the proper value for MAX CPE in the DOCSIS configuration file, so that each cable modem can control the maximum number of CPE devices it supports. In addition, to prevent users from requesting an unlimited number of IP address, be sure to configure the DHCP servers so that they control how many IP addresses are assigned to the CPE devices behind each cable modem.

Interoperation of the Maximum CPE Parameters

The different methods of CPE control can all be active simultaneously. They can interact with one another but do not conflict with one another. [Table 18](#) lists each method and compares their characteristics.

Table 18 Comparison of the Different Max CPE and Max Host Control Mechanisms

Method	Configuration Method	Function	Can Be Changed By...
Methods that are configured on the cable modem:			
Network Access Control	DOCSIS Configuration File	Prevents all network access for CPE devices	Reset of cable modem
MAX CPE	DOCSIS Configuration File	Limits MAC addresses (Layer 2 control)	Reset of cable modem
MAX CPE IP	DOCSIS Configuration File SNMP Set Command	Limits IP addresses (Layer 3 control)	SNMP Set Command
Methods that are configured on the CMTS:¹			
MAX CPE IP (the CMTS uses this value if MAX CPE IP is not specified in the DOCSIS configuration file)	DOCSIS Configuration File CLI Command SNMP Set Command	Limits IP addresses (Layer 3 control)	CLI Command SNMP Set Command
MAX Host Parameters			
MAX Host for one cable modem (cable modem max-hosts)	CLI Commands	Limits CPE devices for one particular cable modem	New CLI Command
MAX Host for a cable interface (cable max-hosts)		Limits CPE devices for all cable modems on a particular cable interface	
MAX Host for a CMTS (cable modem max-cpe)		Limits CPE devices for all cable modems on a Cisco CMTS	

1. In Cisco IOS Release 12.2(4)BC1 and later releases, the Cisco CMTS does not actively manage CPE devices unless this has been enabled using the **cable submgmt default active** command.

Table 18 lists the MAX CPE parameters in order of priority. For example, the Network Access Control and MAX CPE parameters interact as follows:

- If the Network Access Control field for a cable modem is set to Disabled, none of that modem's CPE devices will be able to access the network, regardless of how the other parameters are set.
- If Network Access Control is Enabled and MAX CPE is set to 1 for a cable modem, then a maximum of one CPE device will be able to access the network, no matter how the remaining parameters are configured.

Table 18 also lists the MAX Host parameters in order of more specific to less specific, where the more specific override the settings of the less specific. For example, if you use the **cable modem max-cpe** command to set the MAX Host value for all CMs to 2, you can still use the **cable modem max-hosts** command to give a particular CM a MAX Host value of 8.

In addition, the MAX CPE IP and MAX Host parameters interact as follows:

- When both the MAX CPE IP parameter and the MAX Host parameter for a specific cable modem are specified, the CMTS uses the value specified for MAX Host for that particular modem.
- When both the MAX CPE IP parameter and the MAX Host parameter for a cable interface are specified, the CMTS uses the larger value of the two.
- When both the MAX CPE IP parameter and the MAX Host parameter for the CMTS are specified, the CMTS uses the smaller value of the two.

**Tip**

The Cisco CMTS keeps inactive cable modems listed in its internal database for 24 hours. The CMTS does not reset the CPE counts for these offline cable modems until the 24 hour period expires and the cable modems come back online. If the cable modems come back online before the 24 hours expires, the CMTS continues to use the existing CPE counts.

Possible Conflicts Between Parameters

The recommended procedure for disconnecting one PC from a cable modem and reconnecting a new one is the following:

1. The user first releases the IP address assigned to the PC. The user can do this either by using a utility such as winipcfg, or by shutting down the PC.
2. The user disconnects the old PC and reconnects the new PC to the cable modem.
3. The user reboots the cable modem so as to clear out its MAX CPE values.
4. After the cable modem has come online, the user boots the new PC so that it can obtain the correct IP address and come online.

This procedure will allow the MAX CPE value on the cable modem to stay synchronized with the MAX Host value on the CMTS. Problems can occur in the following situations:

- If the user does not release the IP address from the old PC before connecting a new one, the CMTS is not informed that the new PC is replacing the old one, and therefore counts both PCs when calculating the Host value. If the new value exceeds the MAX Host value, the CMTS does not allow the new PC to come online. The service provider will have to issue the **clear cable host** command to remove the old PC from the MAX Host table, so as to allow the new PC to come online.
- If the user does not reboot the cable modem after disconnecting the old PC, the cable modem retains the old PC's MAC address and continues to count it when calculating the CPE value. If the new value exceeds the MAX CPE value, the cable modem does not allow the new PC to come online. The user will have to reboot the cable modem before the new PC can come online.
- If the user booted their PC before turning on the cable modem or before connecting the Ethernet cable to the cable modem. In this case, the operating system typically assigns a static private IP address (such as 169.254.232.199, which is the default Windows IP address). When the cable modem then boots or is connected to the PC, it logs the PC's private IP address as one of the allowable IP addresses. So, if MAX CPE IP is set to 1, the PC will not be allowed access to the Internet. You must reboot the cable modem to clear its IP address tables, and allow the PC to acquire an IP address from the DHCP server. (To avoid this problem, set the docsDevCpeIpMax attribute for the cable modem to -1 in the DOCSIS configuration file. CableLabs has proposed -1 as the new default, but this change has not yet been given final approval or been implemented in current software releases.)

To reduce service-impacting problems when users replace PCs without following the above guidelines, service providers can configure the MAX Host parameter for a value greater than the MAX CPE value. This allows users to replace a limited number PCs without releasing the IP address and still be able to come online. (Users should continue to reboot the cable modem, however, because that is the only way to clear their internal CPE counter.)

For example, if you configure MAX CPE for a cable modem at 2, and MAX Host at 4, the user can connect any two PCs to the cable modem at any one time. The user can then replace both PCs with new PCs, reboot the cable modem, and have both PCs come online.

The CMTS CPE table for this cable modem lists all four PCs, and the user can switch between them at will, as long as the user reboots the cable modem after each switch. The user, however, is not allowed to bring a fifth PC online until one of the previous PCs has been cleared from the CMTS, using the **clear cable host** command.

**Note**

The cable modem always enforces the MAX CPE parameter, regardless of the setting of the other parameters.

Summary of CPE Address Control

In DOCSIS 1.1 cable networks, CPE address control is done as part of the following process, which also includes Layer 2 and Layer 3 filtering:

1. MAC address filtering—Packets are filtered on the basis of the MAC address for the CPE device. The filter is controlled by the MAX CPE parameter, as set in the DOCSIS configuration file.
2. Logical Link Control (LLC) filtering—Packets are filtered on the basis of the protocol for the packets. The filter is controlled by the docsDevFilterLLCTable table on the cable modem.
3. CPE IP address filtering—Packets are filtered on the basis of the IP address for the CPE device, as controlled by the MAX CPE IP value, as well as the docsDevCpeIpMax attribute and the docsDevFilterCpeTable table on the CMTS.
4. Access list filtering—Packets are filtered on the basis of access lists. IP filtering is controlled by the docsDevFilterIpTable table, and SNMP access filters are controlled by the docsDevNmAccessTable table.
5. MAX Host control—The CMTS allows access for CPE devices on the basis of the MAX Host parameters.

**Tip**

This document does not describe the LLC and access list filtering. For more information about these filters, see the [DOCS-CABLE-DEVICE-MIB](#) MIB for more information on the SNMP attributes and tables that are listed above.

Benefits

- CMTS flexibility allows multiple service operator provisioners, service providers, and other users to synchronize between the CMTS and the cable modem the maximum number of permitted CPE devices that can be connected behind a cable modem.
- Changes can be made by using CLI commands or by using SNMP commands.

How to Configure the MAX CPE and Host Parameters

To reset the maximum number of permitted CPE devices recognized by the CMTS, use one of the following configuration commands. All procedures are optional, depending on the service provider's requirements.

- [Configuring the MAX CPE Parameter on the Cisco CMTS, page 209](#)
- [Configuring the MAX Hosts Parameter for a Cable Interface, page 211](#)
- [Configuring the MAX Hosts Parameter for a Particular Cable Modem, page 212](#)

**Note**

The CMTS assigns the MAX Host value to a cable modem at the time that the cable modem registers with the CMTS. Changing any of the MAX Host commands affects only cable modems that register after the change.

Configuring the MAX CPE Parameter on the Cisco CMTS

To configure MAX CPE parameter, use the following procedure, beginning in user EXEC mode.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cable modem max-cpe** [*number* | **unlimited**]
4. **cable submgmt default active**
5. **cable submgmt default max-cpe** *cpe-num*
6. **exit**

DETAILED STEPS

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

Command or Action	Purpose
Step 3 <pre>cable modem max-cpe [<i>number</i> unlimited]</pre> Example: Router(config)# cable modem max-cpe 8 Router(config)#	Sets the value of the MAX CPE parameter on the Cisco CMTS for all cable interfaces. number = Maximum number of CPE devices supported by cable modems. The valid range for <i>number</i> is 1 to 255, with a default of 0 (which indicates that the Cisco CMTS uses the MAX CPE value specified by each cable modem's DOCSIS configuration file). If <i>number</i> is larger than the MAX CPE value in the cable modem's DOCSIS configuration file or is set to unlimited, this command overrides the configuration file value. If <i>number</i> is smaller than the cpe-max value in the cable modem's DOCSIS configuration file, the value set in the configuration file takes precedence. unlimited = Specifies that the CMTS does not enforce a limit on the number of CPE devices connected to a single cable modem. The cable modem is responsible for controlling the maximum number of CPEs, and the DHCP server is responsible for controlling the number of IP addresses assigned to the CPEs behind a single cable modem. Note If the value in the configuration file is zero and no cable modem max-cpe is configured, then no CPE device is able to obtain an IP address.
Step 4 <pre>cable submgmt default active</pre> Example: Router(config)# cable submgmt default active Router(config)#	Specifies that the CMTS should actively manage CPE devices. The default is the no version of this command, so that the CMTS does not actively manage CPE devices. Note This command is required before the Cisco CMTS will manage CPE devices when running a Cisco IOS Release 12.2 BC software image.
Step 5 <pre>cable submgmt default max-cpe <i>cpe-num</i></pre> Example: Router(config)# cable submgmt default max-cpe 4 Router(config)#	(Optional) Specifies the default value for the MAX-CPE parameter that the CMTS should use when the cable modem does not specify a MAX-CPE value in its DOCSIS configuration file. The range is 1 to 255, with a default of 16.
Step 6 <pre>exit</pre> Example: Router(config)# exit Router#	Exits global configuration mode.

**Note**

Use of the **cable modem max-cpe unlimited** command can open a security hole in the system by enabling denial of service attacks. It could allow a single user to obtain a large number of IP addresses, and thereby cause the entire network to go down after this single user has reserved all available IP addresses.

Configuring the MAX Hosts Parameter for a Cable Interface

To configure MAX Hosts parameter for all cable modems on a particular cable interface, use the following procedure, beginning in user EXEC mode.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface cable** *x/y*
4. **cable max-hosts** *number*
5. **exit**
6. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable Router#	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal Router(config)#	Enters global configuration mode.
Step 3	interface cable <i>x/y</i> Example: Router(config)# interface cable 4/0 Router(config-if)#	Enters cable interface configuration mode for the specified cable interface:
Step 4	cable max-hosts <i>number</i> Example: Router(config-if)# cable max-hosts 10 Router(config-if)#	Specifies the maximum number of hosts that each cable modem on this cable interface can support. The valid range is 0 to 255, with a default of 0 (which indicates that the Cisco CMTS uses the value specified in the cable modem's DOCSIS configuration file).

	Command or Action	Purpose
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.

Configuring the MAX Hosts Parameter for a Particular Cable Modem

To configure MAX Hosts parameter for a particular cable modem, use the following procedure, beginning in user EXEC mode.

SUMMARY STEPS

1. **enable**
2. **cable modem** {*mac-addr* | *ip-addr*} **max-hosts** {*number* | **default**}

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable Router#	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	cable modem { <i>mac-addr</i> <i>ip-addr</i> } max-hosts { <i>number</i> default } Example: Router# cable modem 000C.0102.0304 max-hosts 8 Router#	Specifies the maximum number of hosts allowed behind this particular cable modem: • <i>mac-addr</i> = Specifies the hardware (MAC) address for the particular cable modem. • <i>ip-addr</i> = Specifies the IP address for the particular cable modem. • <i>number</i> = Maximum number of CPE devices that this particular cable modem can support. The valid range is 0 to 255, with a default of 0 (which indicates that the Cisco CMTS uses the value specified in the cable modem's DOCSIS configuration file). • default = Sets the MAX Hosts parameter to 0.

Configuration Examples for the MAX CPE and Host Parameters

The following example shows how to allow the CMTS to recognize a maximum of four CPE devices attached to online cable modems for a CMTS:

```
cable modem max-cpe 4
```

The following example shows how to set the maximum CPE devices recognized by the CMTS for a cable interface to 15:

```
cable max-hosts 15
```

The following example shows how to allow the CMTS to recognize a maximum of 30 attached CPE devices for a specific cable modem of IP address 172.172.172.12:

```
cable modem 172.172.172.12 max-hosts 30
```

Sample Outputs

To display the current configuration and status of a cable interface, use the **show running-config** command in privileged EXEC mode. The following is sample output that shows that the CMTS permits up to five CPE devices to use the specified cable interface to pass traffic.

```
interface Cable3/0
 ip address 192.168.1.1 255.255.255.0 secondary
 ip address 10.1.1.1 255.255.255.0
 load-interval 30
 no keepalive
 cable max-hosts 5
 cable downstream annex B
 cable downstream modulation 256qam
 cable downstream interleave-depth 32
 cable downstream frequency 507000000
 cable upstream 0 frequency 27008000
 cable upstream 0 power-level 0
 cable upstream 0 minislots-size 32
 cable upstream 0 modulation-profile 2
 no cable upstream 0 shutdown
 cable upstream 1 frequency 29008000
 cable upstream 1 power-level 0
 cable upstream 1 channel-width 3200000
 cable upstream 1 minislots-size 4
 no cable upstream 1 shutdown
 cable dhcp-giaddr policy
 cable helper-address 172.17.110.131
end
```

You can also use the **more system:running-config** command to verify the maximum number of permitted CPE devices for a cable interface. Look for a notation, such as “cable max-host 4,” in the cable interface configuration information, as shown in the following sample output:

```
CMTS01# more system:running-config

Building configuration...
Current configuration:
!
interface Cable6/0
 ip address 1.1.1.1 255.255.255.0
 no keepalive
```

```

cable max-hosts 4
cable insertion-interval 2000
cable downstream annex B
cable downstream modulation 64qam
cable downstream interleave-depth 32
cable downstream symbol-rate 5056941
cable upstream 0 frequency 15008000
cable upstream 0 fec
cable upstream 0 scrambler
no cable upstream 0 shutdown

```

You can use the **show cable modem detail** command to list information on each CPE device permitted for a cable modem. The command displays the max cpe value as configured in the DOCSIS configuration file for the cable modem, and in parentheses the value of *n* configured in the **cable modem max-cpe** command, if different. See the following sample output where the CMTS is configured for max-cpe equal to four and then max-cpe equal to unlimited:

```
test-cmts# show cable modem detail
```

Interface	SID MAC address	Max CPE	Concatenation	Rx SNR
Cable4/0/U0 1	0001.9659.47bb	1	yes	37.37
Cable4/0/U0 2	0001.9659.47ab	1	yes	33.70
Cable4/0/U0 3	0001.9659.47bf	1	yes	30.67
Cable4/0/U0 4	0001.9659.3ef7	1	yes	28.84
Cable4/0/U0 5	0001.9659.47eb	1	yes	30.89

```
test-cmts# conf t
```

Enter configuration commands, one per line. End with CNTL/Z.

```
test-cmts(config)# cable modem max-cpe ?
```

```
<1-255> Number
```

```
unlimited Max CPE not enforced
```

```
test-cmts(config)# cable modem max-cpe 4
```

```
test-cmts(config)# end
```

```
test-cmts#
```

```
00:05:11: %SYS-5-CONFIG_I: Configured from console by console
```

```
test-cmts# show cable modem detail
```

Interface	SID MAC address	Max CPE	Concatenation	Rx SNR
Cable4/0/U0 1	0001.9659.47bb	.1 (4)	yes	37.00
Cable4/0/U0 2	0001.9659.47ab	.1 (4)	yes	33.54
Cable4/0/U0 3	0001.9659.47bf	.1 (4)	yes	30.70
Cable4/0/U0 4	0001.9659.3ef7	.1 (4)	yes	29.00
Cable4/0/U0 5	0001.9659.47eb	.1 (4)	yes	30.92

```
test-cmts# conf t
```

Enter configuration commands, one per line. End with CNTL/Z.

```
test-cmts(config)# cable modem max
```

```
test-cmts(config)# cable modem max-cpe ?
```

```
<1-255> Number
```

```
unlimited Max CPE not enforced
```

```
test-cmts(config)# cable modem max-cpe unli
```

```
test-cmts(config)# cable modem max-cpe unlimited
```

```
test-cmts(config)# ^Z
```

```
test-cmts#
```

```

00:06:06: %SYS-5-CONFIG_I: Configured from console by console
test-cmts# show cable modem detail
Interface      SID MAC address      Max CPE Concatenation Rx SNR
Cable4/0/U0 1      0001.9659.47bb      1 (ul)      yes      36.64
Cable4/0/U0 2      0001.9659.47ab      1 (ul)      yes      33.26
Cable4/0/U0 3      0001.9659.47bf      1 (ul)      yes      30.73
Cable4/0/U0 4      0001.9659.3ef7      1 (ul)      yes      29.15
Cable4/0/U0 5      0001.9659.47eb      1 (ul)      yes      30.95

```

Additional References

For additional information related to configuring the MAX CPE and Host parameters on the Cisco CMTS, refer to the following references:

Related Documents

Related Topic	Document Title
CMTS Command Reference	<i>Cisco Broadband Cable Command Reference Guide</i>, at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/cable/bbccmref/index.htm
Cisco IOS Release 12.2 Command Reference	Cisco IOS Release 12.2 Configuration Guides and Command References, at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/index.htm
Interaction of MAX CPE Parameters	<i>How MAX-CPE in DOCSIS File and CMTS Works</i>, at the following URL: http://www.cisco.com/warp/customer/109/max_cpe_in_docsis.html

Standards

Standards ¹	Title
SP-RF1v1.1-I08-020301	Data-Over-Cable Service Interface Specifications Radio Frequency Interface Specification, version 1.1 (http://www.cablemodem.com)

1. Not all supported standards are listed.

MIBs

MIBs ¹	MIBs Link
DOCS-CABLE-DEVICE-MIB DOCS-SUBMGT-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

1. Not all supported MIBs are listed.

Technical Assistance

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

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, TeleRouter, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0502R)

Copyright © 2003 Cisco Systems, Inc. All rights reserved.



N+1 Redundancy for the Cisco Cable Modem Termination System

This chapter provides procedures and commands by which to configure N+1 Redundancy on the Cisco Cable Modem Termination System (CMTS), using Cisco uBR10012 or Cisco uBR7246VXR universal broadband routers with the Cisco 3x10 RF Switch.

N+1 Redundancy is made possible with the addition of the Cisco RF Switch to your cable headend network. Together with the Cisco uBR10012 and/or the Cisco uBR7246VXR routers, the Cisco RF Switch provides a fully redundant system that enables cable operators to achieve PacketCable system availability, minimize service disruptions, and simplify operations.

N+1 Redundancy is an important step toward high availability on CMTS and telecommunications networks that use broadband media. N+1 Redundancy can help limit Customer Premises Equipment (CPE) downtime by enabling robust automatic switchover and recovery in the event that there is a localized system failure.

Beginning with Cisco IOS Release 12.2(15)BC2a, N+1 Redundancy adds synchronization between HCCP Working interface configurations and those inherited upon switchover to HCCP Protect interfaces. This makes the configuration of both easier and switchover times faster.

Cisco IOS and Cisco RF Switch Firmware for N+1 Redundancy

Two operating systems govern the configuration and operation of N+1 Redundancy on the Cisco CMTS:

- Cisco Internetwork Operating System (IOS)—governs the configuration and operation of Cisco universal broadband routers, and works closely with Cisco RF Switch Firmware when configured in N+1 Redundancy.



Note The Cisco IOS CLI now synchronizes configurations between HCCP Working and Protect interfaces. Preconfiguration of the Protect interfaces is no longer required in most circumstances.

- Cisco RF Switch Firmware—governs the configuration and operation of Cisco RF Switches, including the MAC addresses on RF Switch interfaces.

Both command-line interfaces above are required for configuration and testing of N+1 Redundancy.

Cisco IOS Feature Specifications for N+1 Redundancy on the Cisco Cable Modem Termination System

Release	Modification
12.1(10)EC	HCCP support introduced on the Cisco uBR7200 series routers.
12.2(4)XF1, 12.2(4)BC1	HCCP N+1 Redundancy support was added for the Cisco uBR10012 router and uBR10-LCP2-MC28C cable interface line card.
12.2(8)BC2	HCCP N+1 Redundancy support was added for the Cisco uBR10012 router and Cisco uBR10-LCP2-MC16x cable interface line cards.
12.2(11)BC1	HCCP N+1 Redundancy support was added for the Cisco uBR7246VXR router and Cisco uBR-LCP-MC16x cable interface line cards.
12.2(15)BC1	HCCP N+1 Redundancy support introduced for the Cisco uBR10012 router and Cisco UBR10-MC 5X20U or -S/D broadband processing engine (BPE).
12.2(15)BC2a	- HCCP N+1 Redundancy support introduced for the Cisco uBR7246VXR router and the Cisco uBR 3x10 RF Switch. - CLI Usability—Synchronizes HCCP interface configuration between Working and Protect interfaces. - Support for N+1 Redundancy for the Cisco UBR10-MC 5X20U or -S/D BPE on the Cisco uBR10012 router. IF Muting on the Cisco CMTS for non-SNMP-capable Upconverters — enables N+1 Redundancy on CMTS headends that do not use SNMP-enabled upconverters.

Feature History for Cisco RF Switch Firmware

Several performance and configuration enhancements have been added to Cisco RF Switch Firmware, released in the following most recent Versions:

- Version 2.50—SNMPv1 Upconverters and Traps, Default Gateway for Remote TFTP Transfer
- Version 3.30—Improved switchover times, DHCP Server, several new commands or command enhancements for slot configuration and system information
- Version 3.50—Further improved switchover times, optimized ARP cache feature, ARP timeout configuration, and additional **show** command enhancements for ARP and configuration status

Refer to the [Cisco RF Switch Firmware Command Reference Guide](#) on Cisco.com for complete feature descriptions and command histories for the Firmware Versions listed above.

Additional Cisco Broadband Cable High Availability Features

Cisco High Availability (HA) for Broadband Cable products includes these and additional features:

- N+1 HCCP Redundancy
- DOCSIS Stateful Switchover (DSSO)
- Gigabit Ethernet
- PacketCable Support
- Route Processor Redundancy Plus (RPR+)

These and additional HA features are described further in the Cisco White Paper, [Cisco Cable IP Solutions for High-Availability Networks](#), available on Cisco.com.

Finding Support Information for Platforms and Cisco IOS Software Images

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

Contents

This chapter provides the following procedures and commands to configure, test and debug the N+1 Redundancy scheme on your Cisco universal broadband router CMTS:

- [Prerequisites, page 221](#)
- [Restrictions and Limitations, page 222](#)
- [Information About N+1 Redundancy and the Cisco Universal Broadband CMTS, page 225](#)
- [Cisco RF Switch Configuration Tasks for N+1 Redundancy, page 235](#)
- [Cisco CMTS Configuration Tasks for N+1 Redundancy, page 241](#)
- [Switchover Testing Tasks for N+1 Redundancy, page 251](#)
- [Configuration Examples for Cisco N+1 Redundancy, page 259](#)
- [Additional References, page 293](#)
- [Glossary, page 295](#)

Prerequisites

To use N+1 HCCP Redundancy, ensure the following conditions are met:

- To implement N+1 Redundancy, you must use an image from a supported Cisco IOS software release. Refer to the release notes for your platform on Cisco.com to verify the availability of the N+1 Redundancy feature.
- Your downstream plant must meet Data-over-Cable Service Interface Specifications (DOCSIS) 1.0 or DOCSIS 1.1 requirements.
- Customer cable modems must meet requirements for your network and service offerings. All third-party cable modems must be DOCSIS 1.0- or DOCSIS 1.1-compliant and configured for two-way data communication.

Restrictions and Limitations

General N+1 Redundancy Restrictions and Limitations

These restrictions apply to N+1 Redundancy on both the Cisco uBR10012 and Cisco uBR7246VXR routers.

- When using the **show hccp channel switch** Cisco IOS command, the system communicates with each module in the RF Switch that comprises the bitmap. This requires a much longer period for timeout—contrasted with the lesser timeout required for the system to verify connectivity. Use the **show hccp g m channel** command to view each individual member of an HCCP group.

Cable upstream configuration commands are described in the *Cisco Broadband Cable Command Reference Guide* on Cisco.com:

<http://www.cisco.com/univercd/cc/td/doc/product/cable/bbcmref/index.htm>

- **HCCP interface configuration can be removed** from either Working or Protect Interfaces. However, the following HCCP restrictions apply to HCCP N+1 Redundancy on either the Cisco uBR10012 or Cisco uBR7246VXR router:
 - Before removing HCCP configurations from an active Working interface, either shut down the Protect or lockout switchover functions using the **hccp group lock member-id** command in global configuration mode. Otherwise the Protect interface may declare the Working interface to have failed and may attempt to switch over.
 - Do not remove HCCP configurations from an active Protect interface. The active HCCP group member should be restored to its corresponding Working interface (revertback) before removing HCCP configuration from the Protect interface.



Note

This restriction does not apply when removing HCCP configuration from a Protect interface while it is in standby mode and N+1 Redundancy is in normal Working mode.

For information about modifying HCCP configuration, refer to the section titled “[Maintaining Online Cable Modem Service When Removing HCCP Configuration from Working HCCP Interfaces](#)” section on page 248.

- **Downstream (DS) modulation, interleave depth** and **DOCSIS Annex mode** must be the same for all members in the same HCCP group. For configuration information, refer to the “[Preconfiguring HCCP Protect Interfaces for N+1 Redundancy](#)” section on page 242.
- **When using external, non-SNMP upconverters**, DS frequencies must be set to be the same across all cable interface line cards that are protected by the same Protect line card.

N+1 Redundancy Restrictions and Requirements for the Cisco uBR7246VXR Router

- Cisco recommends that the lowest slot interface be the master when configuring cable interface bundling on the Cisco uBR7246VXR router.
- Cisco uBR7246VXR CMTS interfaces that are bundled in IP switch over together.

N+1 Redundancy Restrictions and Requirements for the Cisco uBR10012 Router

Restrictions for Cisco IOS Release 12.2(15)BC2a

If you use DOCSIS 1.1 provisioned cable modems in your network and you are considering deploying Cisco IOS Release 12.2(15)BC2a, Cisco recommends that you disable HCCP N+1 Redundancy until further notification, or that you reduce instances of manual switchover from HCCP Working to Protect via the command line interface (CLI).

Cable interface line cards in HCCP Working or Protect status may reload or experience intermittent failure during HCCP N+1 switchover in Cisco IOS Release 12.2(15)BC2a:

- Cable interface line cards that are in HCCP Working status may reload during N+1 switchover from HCCP Working to Protect status.
- You may experience HCCP memory overrun when cable interface line cards in HCCP Working status switch over to HCCP Protect status.

General Requirements for the Cisco uBR10012 Router with All Cable Interface Line Cards

- A **TCC+ card** must be installed in your Cisco uBR10012 router in order to employ the Cisco RF Switch in your cable headend system. For more detailed information on the TCC+ card, refer to the *Cisco uBR10012 Universal Broadband Router TCC+ Card* document available on Cisco.com:

<http://www.cisco.com/univercd/cc/td/doc/product/cable/ubr10k/ubr10012/frus/tcc5094.htm>

- Use the **IP address from the local loopback interface** as the Working interface IP address when configuring Hot-Standby Connection-to-Connection Protocol (HCCP) on the Cisco uBR10012 router. Cisco strongly recommends that you create a loopback interface on the Cisco uBR10012 router, and then assign the loopback interface's IP address to the HCCP protect configuration.
- Using slot 5/1 as the Protect interface is easiest for physical wiring to the Cisco RF Switch when used with the Cisco uBR10012 router.
- **Cisco IOS downgrade** can be performed while retaining N+1 functionality, as supported by earlier Cisco IOS releases. However, when downgrading your Cisco IOS software from release 12.2(15)BC2a to an earlier release, N+1 Redundancy requires that you preconfigure the Protect interface(s) with the **cable upstream connector** command. Without this HCCP preconfiguration, the upstream channel does not come up again after a switchover.

Restrictions with the Cisco UBR10-MC 5X20U or -S/D BPE

- **MAC domains and corresponding DS interface pairs switch over together.** Each ASIC processor on the Cisco UBR10-MC 5X20U or -S/D BPE supports two MAC domains. MAC domains that share a common ASIC processor (JIB) must be configured so that they share the same state, Active or Standby. As a result, each interface in the pair switches over with the other.

Downstream MAC domain pairings would be downstream (DS) ports 0 and 1, ports 2 and 3, and a solitary port 4, which has its own JIB. For example, these interface pairings share the same JIB and switch over together as follows:

- cable interface 5/0/0 and 5/0/1
- cable interface 5/0/2 and 5/0/3
- Cable interface 5/0/4 is on the third ASIC processor, which is not shared with another interface.



Note

If HCCP is not configured on an interface that shares a MAC processor with another configured interface, it does not switch over and could cause issues. The same holds true if an ASIC companion is "locked out" during a failover.

Disabling HCCP Revertive on Protect Cable Interfaces

The cable interface line cards pair up interfaces that share the same JIB (ASIC processor) as explained in the restriction immediately above.

As a result, when HCCP keepalive is enabled on paired DS channels, both DS channels in the pair switch over together if either DS channel has a keepalive failure. For example, if HCCP is configured on DS channels 0 and 1, and DS channel 0 has a keepalive failure, then DS channel 1 also fails because it shares the same JIB with DS channel 0.

When HCCP *revertive* is enabled on both downstream channels in the pair, the interface that experiences the keepalive failure does not revert back automatically to active state. This is desirable behavior because it prevents revertback to active state prematurely—before the cause of an external failure is confirmed and remedied.



Note

The default HCCP revertive time for HCCP interfaces is 30 minutes.

However, the JIB companion interface may act upon the default revertive time of 30 minutes. The companion interface attempts to revert back to active state after 30 minutes (when HCCP revertive is enabled). This creates conflict with the failed companion interface on the same JIB.



Note

Therefore, Cisco recommends that you disable automatic HCCP revertive functions on both Protect downstream channels of a JIB that use keepalive or tracking. If you have keepalive and tracking enabled, or you are using the UBR10-MC 5X20U or -S/D in N+1 configuration, disable the revertive function on both Protect interfaces.

To disable the HCCP revertive function on Protect interfaces, use the **no hccp group revertive** command in cable interface configuration mode. Disable revertive on each HCCP Protect interface:

no hccp group revertive

Syntax Description

group	The group number for the specified interface. Valid values are any number from 1 to 255, inclusive.

For additional information about configuring or removing HCCP, refer to the “Cisco CMTS Configuration Tasks for N+1 Redundancy” section on page 241, and to the **hccp revertive** command in the *Cisco Broadband Cable Command Reference Guide* on Cisco.com:

<http://www.cisco.com/univercd/cc/td/doc/product/cable/bbccmref/index.htm>

Information About N+1 Redundancy and the Cisco Universal Broadband CMTS

This section describes the following concepts that relate to N+1 Redundancy:

- [The Components and Terminology of N+1 Redundancy](#)
- [IF Muting on the Cisco CMTS for non-SNMP-capable Upconverters](#)

The Components and Terminology of N+1 Redundancy

N+1 Redundancy is made possible with the addition of the Cisco RF Switch to your cable headend network. The N+1 Redundancy protection scheme you select for your system depends on your CMTS platform and upon the number of cable interface line cards or Broadband Processing Engines (BPEs) that you have installed in the Cisco router chassis.

N+1 Redundancy is available for these Cisco Cable Modem Termination System (CMTS) platforms:

Table 1 Cisco CMTS Platforms Supporting N+1 Redundancy

CMTS Platform/N+1	Line Cards or BPEs	Supported Upconverters	Cisco RF Switch
Cisco uBR10012	• UBR10-LCP2-MC16C • UBR10-LCP2-MC16C= • UBR10-LCP2-MC16E • UBR10-LCP2-MC16E= • UBR10-LCP2-MC16S • UBR10-LCP2-MC16S= • uBR10-LCP2-MC28C • UBR10-LCP2-MC28C • UBR10-MC 5X20U or -S/D	• SNMP with RF Muting • non-SNMP¹ with IF Muting	Cisco 3x10 RF Switch (one or multiple)
Cisco uBR7246VXR	• UBR-MC28C • UBR-MC16S • UBR-MC16C	• SNMP with RF Muting • non-SNMP¹ with IF Muting	Cisco 3x10 RF Switch (two)

1. non-SNMP upconverters are supported beginning with Cisco IOS Release 12.2(15)BC2a.

N+1 Redundancy refers to Working cable interface line cards (N) being protected by one additional line card (+1). The two types of Cisco N+1 configuration are as follows:

- 8+1 (7+1)—Refers to an eight-card redundancy scheme in which seven Working cable interface line cards are protected by one additional Protect line card. This is the default N+1 configuration for the Cisco uBR10012 router. This redundancy scheme is also referred to as 7+1 redundancy, which is the more physically accurate term.
- 4+1—Refers to a four-card redundancy scheme in which four Working cable interface line cards are protected by one additional Protect line card.

Upconverters may reside between the Cisco RF Switch and the downstream (DS) interface on the Cisco CMTS. Cisco IOS supports both SNMP and non-SNMP-capable upconverters.

N+1 Redundancy on the Cisco uBR10012 Universal Broadband Router

The eight-card 7+1 Redundancy scheme for the Cisco uBR10012 router supports redundancy for the cable interface line cards installed in a fully populated Cisco uBR10012 chassis. Other redundancy schemes are designed to support partial cable interface line card populations in a Cisco uBR10012 chassis.

A single Cisco uBR10012 CMTS can support up to eight Cisco cable interface line cards, each featuring one to five downstream and six to 20 upstream cable interfaces for a total of up to 40 downstream and 160 upstream interfaces in the chassis.

A single Cisco RF Switch can then be connected to this Cisco uBR10012 CMTS, allowing you to deploy an N+1 Redundancy scheme where one protecting cable interface line card supports from one to seven Working cable interface line cards in the same chassis.

The Cisco uBR10012 router supports N+1 Redundancy on the following Cisco uBR10012 cable interface line cards (broadband processing engines—BPEs):

Cable Interface Line Card	N+1 Redundancy Introduced
Cisco UBR10-MC 5X20U or -S/D	Cisco IOS Release 12.2(15)BC2a
Cisco UBR10-MC 5X20U or -S/D	Cisco IOS Release 12.2(15)BC1 Note Commencing with Cisco IOS Release 12.2(15)BC2a, this cable interface line card is end-of life (EOL). Cisco now supports the newly available Cisco UBR10-MC 5X20U or -S/D BPE.
Cisco uBR10-LPC2-MC16C, Cisco uBR10-LCP2-MC16E, Cisco uBR10-LCP2-MC16S	Cisco IOS Release 12.2(8)BC2
uBR10-LCP2-MC28C	Cisco IOS Release 12.2(4)XF1, 12.2(4)BC1

The Cisco uBR10012 router contains eight slots, numerated as shown in [Figure 1](#), using the slot/port CLI convention (for example, slot 8/0).

A Cisco uBR10012 router identifies a subinterface addresses by slot number, subslot number, and downstream (DS) port number, in the format slot/subslot/DS port. For example, the address of a subinterface could be 5/1/0 (slot 5, subslot 1 and DS port 0).

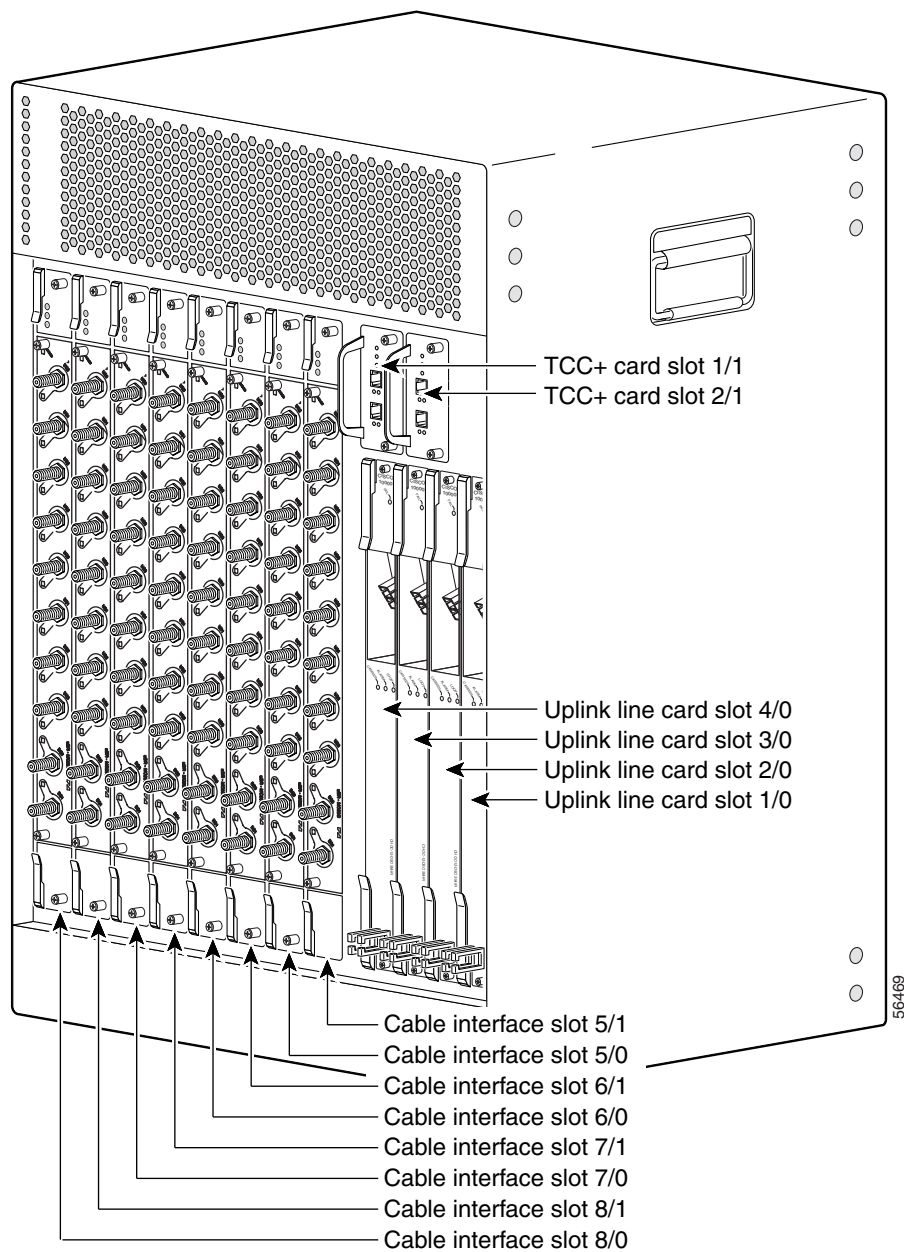
Cisco IOS command line syntax is unique when selecting or defining slots, subslots and ports for the Cisco uBR10012 router. For example, the syntax of the Cisco IOS command **interface cable slot/subslot/port** identifies a cable interface on the Cisco uBR10012 router. The following are the valid values for this and similar such commands:

- *slot* = 5 to 8
- *subslot* = 0 or 1
- *port* = 0 to 4 (depending on the cable interface)

[Figure 1](#) illustrates the numeration of these cable interfaces on the Cisco uBR10012 router chassis.

Chassis Slot Numeration and Selection on the Cisco uBR10012 Router

Figure 1 Cisco uBR10012 Chassis Slot Numeration —Rear View



N+1 Redundancy on the Cisco uBR7246VXR Universal Broadband Router

The 4+1 redundancy scheme for the Cisco uBR7246VXR router supports redundancy for the cable interface line cards installed in four fully populated router chassis.



Note

Cisco recommends using the chassis with the most memory, network processing engine (NPE) power and additional resources as the Protect chassis.

Each Cisco uBR7246VXR can support up to four Cisco cable interface line cards, each featuring one or two downstream and six or eight upstream cable interfaces, for a total of up to eight downstream and 32 upstream interfaces in the chassis.

Two Cisco RF Switches can be connected to four Working and one Protect Cisco uBR7246VXR routers, allowing you to deploy an N+1 Redundancy scheme in which one protecting cable interface line card in the Working uBR7246VXR supports one Working cable interface line card in each of the four Working chassis.

The Cisco uBR7246VXR router supports N+1 Redundancy on the following cable interface line cards:

Cable Interface Line Card	N+1 Redundancy Introduced
Cisco uBR-MC16U/X	Cisco IOS Release 12.2(15)BC2a
Cisco uBR-MC28C	Cisco IOS Release 12.2(15)BC2a

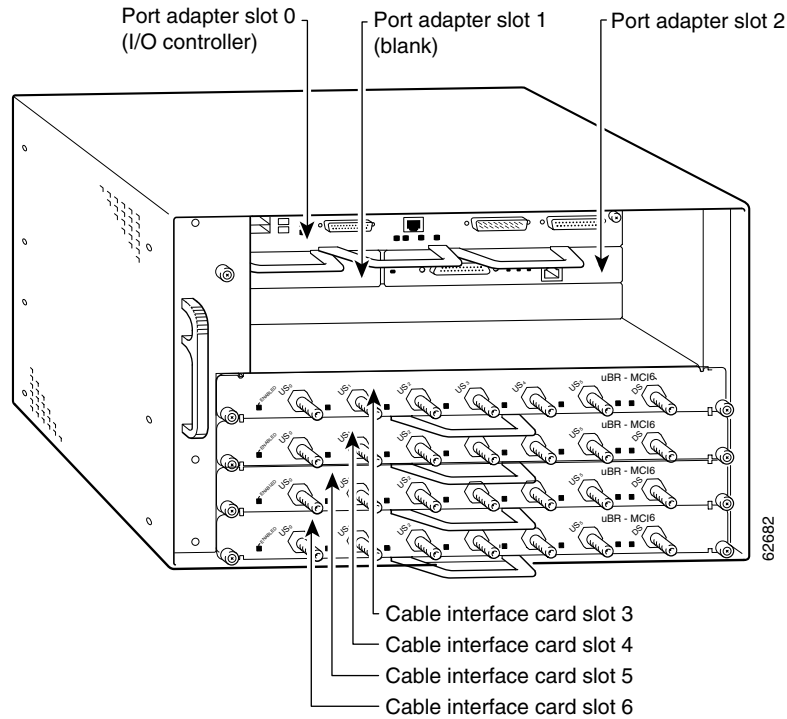
Chassis Slot Numeration on the Cisco uBR7246VXR Router

For Cisco uBR7200 series components, the slot number is the chassis slot in which a port adapter or a cable interface card is installed. The logical interface number is the physical location of the interface port on a port adapter. Numbers on a Cisco uBR7200 series router begin with 0.

Using a Cisco uBR7246VXR router chassis to illustrate, slot/port positioning is as follows:

- Slot 0—I/O controller
- Slot 1-2—Cisco port adapters
- Slot 3-6—Cisco cable interface line cards; the upstream ports on the card start with port 0.

For the Cisco uBR7246VXR reference design discussed in this guide, line card (LC) 1 in Cisco uBR7246VXR 5 protects the Working LC 1 in router chassis 1, 2, 3, and 4. LC 2 in chassis 5 protects the Working line card 2 in chassis 1, 2, 3, and 4, and so forth.

Figure 2 Cisco uBR7246VXR Router Chassis Slot Numbering—Rear View

N+1 Redundancy and the Cisco RF Switches

The Cisco RF Switch can be operated in two separate modes, either in 8+1 configuration, or in 4+1 configuration as two RF Switches.



Note

The default N+1 Redundancy mode for the Cisco RF Switch is 8+1. This does not require change when configuring N+1 Redundancy on the Cisco uBR10012 router with the Cisco UBR10-MC 5X20U or -S/D BPE.

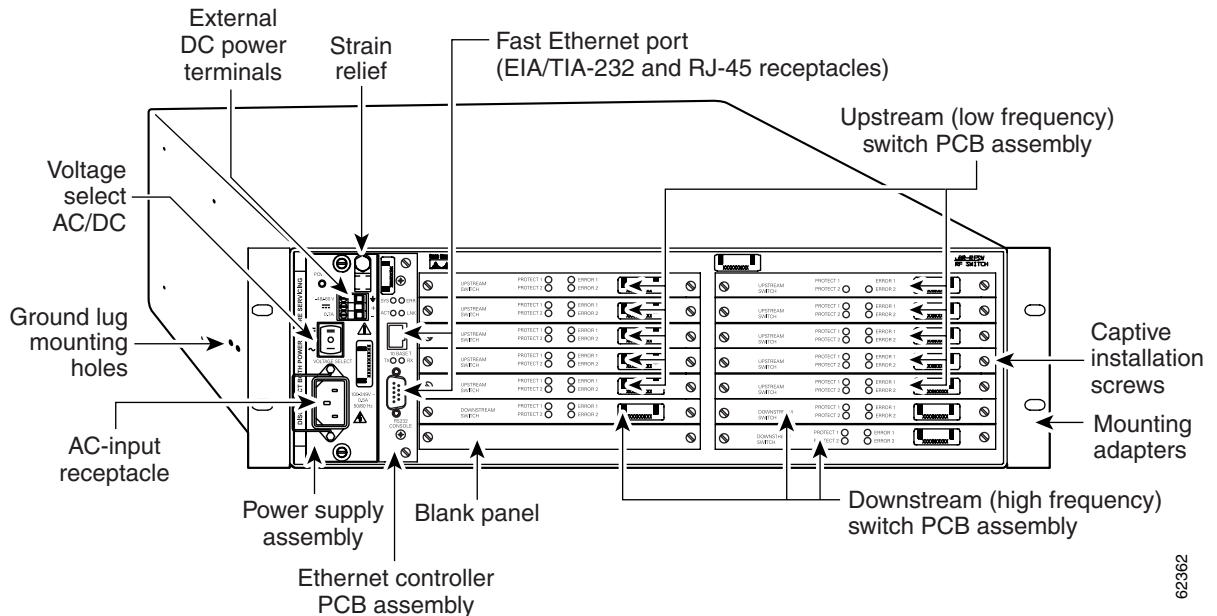


Note

The **show configuration** command and other Cisco RF Switch commands contain the `Card Protect Mode` field. When this field displays 8+1, this indicates that the Cisco RF Switch is configured for N+1 Redundancy, where eight or less Working line cards are possible.

Cisco 3x10 RF Switch Chassis Overview

Figure 3 Cisco RF Switch Chassis—Front View



62362

In both of the Cisco RF Switches, the slot number is the chassis slot in which an Ethernet controller or an upstream or downstream card is installed, and the logical interface number is the physical location of the interface port on an Ethernet controller.

The MAC-layer or hardware address is a standardized data link layer address that is required for certain network interface types. The Cisco RF Switch uses a specific method to assign and control the MAC-layer addresses of its Ethernet controller.

The Ethernet controller and upstream and downstream assembly slots maintain the same slot number regardless of whether other Ethernet controllers or upstream or downstream cards have been installed or removed. However, when you move an upstream or downstream card to a different slot, the logical interface number changes to reflect the new slot number. The Ethernet card is always installed in the same slot.

All LAN interfaces (ports) require unique MAC-layer addresses, also known as hardware addresses. Typically, the MAC address of an interface is stored on a memory component that resides directly on the interface circuitry; however, the OIR feature requires a different method.

The OIR feature allows you to remove an Ethernet controller or an upstream or downstream assembly and replace it with another identically configured one. If the new controller or assembly matches the controller or assembly you removed, the system immediately brings it online. In order to allow OIR, an address allocator with a unique MAC address is stored in an EEPROM on the Cisco RF Switch midplane. Each address is reserved for a specific port and slot in the switch, regardless of whether an Ethernet controller or an upstream or downstream assembly resides in that slot.

The MAC addresses are assigned to the slots in sequence. The first address is assigned to Ethernet controller slot 0, and the next addresses are assigned to upstream and downstream assembly slots 1 through 14. This address scheme allows you to remove the Ethernet controllers or assemblies and insert them into other switches without causing the MAC addresses to move around the network or be assigned to multiple devices.

Example:

Modules 1-10 below are upstream (US) modules in the Cisco uBR 3x10 RF Switch.

The remainder of the modules are either assigned to downstream functions or are not used.

- Module 1 uses Port a for slots 1-8 on the Working, and it uses Port a of Protect slot 1 and/or Protect slot 2.
- Module 2 uses CMTS Ports 1h through 8h, and Protect Port 1h and Protect Port 2h.
- Module 3 uses port b.
- Module 4 uses port i.
- Module 5 uses port c.
- Module 6 uses port j.
- Module 7 uses port d.
- Module 8 uses port k.
- Module 9 uses port e.
- Module 10 uses port l.
- Module 11 uses port f.
- Module 12 uses port m.
- Module 13 uses port g.
- Module 14 uses port n, which is not used on the Cisco uBR 3x10 RF Switch.

The Cisco uBR 3x10 RF Switch works with the Cisco uBR10012 router and supports three downstream modules and 10 upstream modules. Each RF switch module supports the full frequency range specified by DOCSIS and EuroDOCSIS standards.

IF Muting on the Cisco CMTS for non-SNMP-capable Upconverters

Beginning with Cisco IOS Release 12.2(15)BC2a, Cisco supports IF Muting with both SNMP and non-SNMP-capable upconverters in N+1 Redundancy. IF Muting offers the following benefits:

- IF Muting for either type of upconverter significantly increases the N+1 protection schemes that are available for Cisco CMTS headends.
- IF Muting offers the additional benefit of being faster than RF Muting.
- IF Muting is enabled by default. The Cisco CMTS automatically enjoys the benefits and availability of IF Muting.

IF Muting functions in the following manner:

- IF output from the Working cable interface line card is enabled.
- IF output from the Protect cable interface line card is disabled.
- When a switchover occurs from Working to Protect, the IF output of the Working card is disabled and that of the Protect is enabled. If an interface is in Active mode, RF output is enabled.
- When the cable interface line card first comes up after a system failure, IF output is muted until the Cisco CMTS determines if each interface is in active or standby mode (in either Working or Protect state). When an interface is active (Working or Protect), IF output is enabled. When an interface is in standby mode, IF output is muted.

The relevance and support for IF Muting is dependent on the type of Cisco CMTS being used. This is a summary of IF Muting in relation to three sample scenarios:

- Case1—External upconverters are not controlled nor controllable. In this type of scenario, the external upconverter either cannot be controlled remotely or the Cisco CMTS is not configured to control the external upconverter.

- This type of Cisco CMTS is newly supported with Cisco IOS Release 12.2(15)BC2a. Previously, such customers could not enable N+1 Redundancy in the Cisco CMTS headend because they use upconverters that previously could not be controlled from the Cisco CMTS.
- Case 2—The Cisco CMTS is configured to control an external upconverter. Cisco continues to support N+1 Redundancy in this scenario (in which IF Muting is not required). The Cisco CMTS uses RF Muting of the upconverter in this scenario—automatically enabled when an HCCP upconverter statement is configured.
- Case 3—The Cisco CMTS uses internal upconverter(s), as with the Cisco UBR10-MC 5X20U or -S/D BPE. Cisco continues to support N+1 Redundancy in this scenario (in which IF muting is not required). The Cisco CMTS uses RF muting in this scenario (automatically enabled) because the upconverter is configured by the CMTS to do RF Muting.

IF Muting and HCCP Configuration

HCCP interface configuration typically entails three tasks:

- Working or Protect mode
- Upconverter statement
- RF switch statement

When you configure HCCP on an interface, but you do not specify an upconverter statement, this dictates whether IF Muting is active. With no upconverter statement in the interface configuration, IF Muting becomes active by default.

For additional details, refer to the procedures in these sections:

- [Cisco RF Switch Configuration Tasks for N+1 Redundancy, page 235](#)
- [Cisco CMTS Configuration Tasks for N+1 Redundancy, page 241](#)

Restrictions for IF Muting

Shared Downstream Frequency

All the interfaces in the same HCCP group must use the same downstream frequency. To define the downstream center frequency for the cable interface line card, use the cable downstream frequency command in cable interface configuration mode. On cable interfaces with an integrated upconverter, use the **no** form of this command to remove the downstream frequency and to disable the RF output.

cable downstream frequency *down-freq-hz*

no cable downstream frequency

The **no** form of this command is supported only on the Cisco uBR-MC28U/X cable interface line card and the UBR10-MC 5X20U or -S/D.

- *down-freq-hz*—The known center frequency of the downstream carrier in Hz (the valid range is 55 MHz to 858 MHz). The usable center frequency range depends on whether the downstream is configured for DOCSIS or EuroDOCSIS operations:
 - DOCSIS — 91 to 857 MHz
 - EuroDOCIS — 112 to 858 MHz

The Cisco IOS supports a superset of these standards, and setting a center frequency to a value outside these limits violates the DOCSIS or EuroDOCSIS standards. Cisco does not guarantee the conformance of the downstream and upconverter outputs when using frequencies outside the DOCSIS or EuroDOCSIS standards.

For additional information about this command, refer to the [Cisco Broadband Cable Command Reference Guide](#) on Cisco.com.

Requirements for IF Muting

For non-SNMP-capable upconverters to be used with IF Muting, RF output must be less than -3 dBmV when:

- IF input is absent.
- The switchover time from Working to Protect is less than one second. That is, when IF is applied to the upconverter, the RF output must be present within one second.

If either of these requirements is not met, the integrity of the N+1 switchover operations could be compromised.

Cisco RF Switch Configuration Tasks for N+1 Redundancy

You must configure and activate both the Cisco RF Switch and the Cisco CMTS to ensure that N+1 Redundancy operates correctly. You must also configure HCCP Working interfaces and groups.

Perform these procedures in sequence when configuring N+1 Redundancy on the Cisco RF Switch.

	Procedure	Purpose
Step 1	“Configuring the Cisco RF Switch for N+1 Redundancy” procedure on page 1-235	(Required) Provides required and optional configurations on the Cisco RF Switch, including MAC and IP addressing, SNMP configurations, and switchover interface groups.
Step 2	“Creating Cisco RF Switch Module Bitmaps” procedure on page 1-238	(Required) Provides required configuration of hexadecimal-format module bitmaps that indicate which upstream (US) and downstream (DS) modules belong to a switchover group.

Configuring the Cisco RF Switch for N+1 Redundancy

SUMMARY STEPS

1. **set mac address** *mac-address* (optional)
2. **set ip address** *ip-address netmask* (optional)
3. **set slot config** { *upstreamslots* | *downstreamslots* } (optional)
4. **set snmp community read-write private** (optional)
5. **set snmp host** *ip-address* (optional)
6. **set snmp traps** (optional)
7. **set protection** {4|8} (required)
8. **set password** *text* (optional)
9. **set tftp-host** *ip-address* (optional)
10. **set switchover-group** *group-name module-bitmap* | **all** (required)

DETAILED STEPS

	Command	Purpose
Step 1	set mac address <i>mac-address</i> Example: <pre>rfswitch> set mac address 0000.8c01.1111</pre>	(Optional) To specify the MAC address of the Ethernet port on the Cisco RF Switch (used to connect to the LAN), use the set mac address command at the Cisco RF Switch command line interface. The MAC address must be specified using a trio of hexadecimal values. For example, set mac address <i>hex.hex.hex</i> . To negate the existing MAC address assignment and specify a new one, use the no form of this command. If no MAC address is specified, the Cisco RF Switch assumes the default OUI MAC address value.

Step 2	<pre>set ip address ip-address netmask [dhcp]</pre> Example: <pre>rfswitch> set ip address 172.16.10.3 255.255.255.0</pre>	(Optional) To specify a static IP address and relative netmask of the Ethernet interface on the Cisco RF Switch, use the set ip address command in User mode. To restore the default setting, use the no form of this command. Default setting differs according to your Firmware Version: • The default IP configuration for Version 3.30 and 3.50 is DHCP enabled. • The dhcp keyword enables the specified IP address as the address for DHCP services on the network. This keyword also produces the same result as the no form of this command for Version 3.30 and 3.50—it enables DHCP. • The default IP configuration for Version 2.50 is the static IP address of 10.0.0.1 255.255.255.0.
Step 3	<pre>set slot config {upstreamslots downstreamslots }</pre> Example: Cisco 3x10 RF Switch (default) <pre>rfswitch> set slot config 0x03ff 0x1c00</pre>	(Optional) Sets the chassis slot-to-line card configuration. The command no set slot config restores the default, which is a 3x10 configuration. Setting a bit position tells the Cisco RF Switch to expect that type of card installed in the slot. A zero in both parameters indicates that the slot should be empty. Both <i>upstreamslots</i> and <i>dstreamslots</i> are 16-bit hex integer bit-masks that represent whether the slot is enabled/configured for that type of card. The right-most bit represents slot 1. For additional bitmap conversion information, refer to the <i>Bitmap Calculator for N+1 Configuration with the Cisco RF Switch</i> (Microsoft Excel format) http://www.cisco.com/warp/public/109/BitMap.xls As there are only 14 slots in the Cisco RF Switch chassis, the upper two Most Significant Bits (MSBs) of the 16-bit integer are ignored. Note Changes made to the slot configuration on the Cisco RF Switch do not take effect until the system is rebooted (reload command), or an event occurs which causes the enumeration of the chassis line cards to reset.
Step 4	<pre>set snmp community read-write private</pre> Example: <pre>rfswitch> set snmp community read-write private</pre>	(Optional) To specify the Simple Network Management Protocol (SNMP) community string on the Cisco RF Switch, use the set snmp community command at the Cisco RF Switch command line interface. This command enables you to gain read and write access to the Cisco RF Switch. The <i>community</i> string must be entered as a string of text. To negate the existing <i>community</i> string and make way for a new one, use the no form of this command. If no SNMP string is entered, the SNMP string assumes the default value private. Note Currently, the private keyword is the only SNMP community string supported on the Cisco RF Switch. The default value of private is the proper setting under normal circumstances.
Step 5	<pre>set snmp host ip-address</pre> Example: <pre>rfswitch> set snmp host 172.16.10.3</pre>	(Optional) To specify the IP address that receives SNMP notification messages, use the set snmp host command at the Cisco RF Switch command line interface. You can specify more than one SNMP IP address simply by entering this command once for each IP address you want to specify. To negate an existing SNMP IP address assignment, use the no form of this command. If no SNMP IP address is specified, the Cisco RF Switch does not transmit any SNMP notification messages.
Step 6	<pre>set snmp traps</pre> Example: <pre>rfswitch> set snmp traps</pre>	(Optional) To enable SNMP reporting for all modules on the Cisco RF Switch, use the set snmp traps command in the Cisco RF Switch User mode. To deactivate SNMP reporting, use the no form of this command. SNMP reporting is enabled by default on the Cisco RF Switch.

Step 7	set protection {4 8} Example: <pre>rfswitch> set protection 8</pre>	(Required) To set the line card protection scheme, specifying the N+1 protection scheme under which the Cisco RF Switch operates, use the set protection command in Cisco RF Switch User mode. • set protection 4—Specifies that the Cisco RF Switch operate using a 4+1 protection scheme. • set protection 8—Specifies that the Cisco RF Switch operate using an 8+1 protection scheme. To negate the existing protection scheme specification, use the no form of this command. The default protection scheme for the Cisco RF Switch is 8+1.
Step 8	set password text Example: <pre>rfswitch> set password cisco</pre>	(Optional) To specify an access password for the Cisco RF Switch command line interface, use the set password command at the Cisco RF Switch command line interface. To negate the existing access password, use the no form of this command.
Step 9	set tftp-host ip-address Example: <pre>rfswitch> set tftp host 172.16.10.17</pre>	(Optional) To specify the host IP address of the TFTP server through which the Cisco RF Switch enables file transfer, use the set tftp-host command at the Cisco RF Switch command line interface. To negate an existing host IP address specification for the remote TFTP server, use the no form of this command. (No default TFTP server IP address is supported on the Cisco RF Switch.)
Step 10	set switchover-group group-name module-bitmap all Example: <pre>rfswitch> set switchover-group a12345 0xAA200000</pre>	(Required) To specify a new or existing switchover group name (to which a Cisco RF Switch module is assigned), use the set switchover group command at the Cisco RF Switch command line interface. A switchover group is a collection of Cisco RF Switch interfaces that are all configured to switch over at the same time. • <i>group-name</i> — Can be an alpha-numeric string beginning with a non-numeric character. • <i>module-bitmap</i> — Defines a Cisco RF Switch module, and must be specified as an eight-character hexadecimal identifier or assigned the all keyword. Note Refer to the “Creating Cisco RF Switch Module Bitmaps” section on page 238 for instructions on creating an appropriate hexadecimal module bitmap. • all — Keyword instructs the Cisco RF Switch to automatically switch over all upstream and downstream interfaces connected to the switch module in question. Note When setting bit maps on the RF Switch, type 0x in front of the bitmap identifier so that the RF Switch recognizes hexadecimal code. Otherwise, the RF Switch assumes the bitmap is in decimal code. To negate an existing switchover group, use the no set switchover-group command at the Cisco RF Switch command line interface. Note You do not need to specify <i>module-bitmap</i> when negating an existing switchover group. For example, the command no set switchover-group a12345 will eliminate the switchover group named “a12345.” Once a switchover group containing one or more Cisco RF Switch modules has been defined, you can use the switch command to enable N+1 Redundancy behavior on the Cisco RF Switch, as described in the following section, “Switchover Testing Tasks for N+1 Redundancy.”

Step 11	save config Example: rfswitch> save config	This command saves the latest configuration or image upgrade changes in both Flash and Bootflash, and synchronizes Backup and Working copies in each.
Step 12	reboot or reload Example: rfswitch> reload	This command restarts the Cisco RF Switch so that all changes above take effect.

Creating Cisco RF Switch Module Bitmaps

Perform the following steps to produce a hexadecimal-format module bitmap that you can then assign to Working or Protect Cisco RF Switch modules. Module bitmaps for the Cisco RF Switch are comprised of 32-bit map assignments that you translate to an eight-character hexadecimal module bitmap identifier.

This procedure cites an example of a typical Working cable interface module map with 8+1 redundancy configuration. This scenario connects cable interfaces to the Cisco RF Switch following the example described in the “[Cabling](#)” chapter of the *Cisco RF Switch Hardware Installation and Configuration Guide*:

- Interfaces A, B, C, D, and F comprise the four upstream and one downstream connections to the first MAC domain of a uBR10-LCP2-MC28C cable interface line card installed in a Cisco uBR10012 Series chassis.
- Interfaces H, I, J, K, and M comprise the four upstream and one downstream connections to the second MAC domain on the same cable interface line card.



Note

Also refer to the *Bitmap Calculator for N+1 Configuration with the Cisco RF Switch* in Microsoft Excel format—available for download and use from Cisco.com.

SUMMARY STEPS

1. Logically break the two MAC domains up into separate groups and deal with them individually. Begin by determining the 32 binary values for the *first* MAC domain.
2. Convert the resulting binary quartets into decimal values.
3. Convert the eight resulting decimal values into hexadecimal values.
4. Repeat the steps above for the second MAC domain.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Logically break the two MAC domains up into separate groups and deal with them on their own.	Begin by determining the 32 binary values for the <i>first</i> MAC domain that will eventually define the eight decimal characters leading to the eight hexadecimal characters comprising your module bitmap by laying out the individual bits as follows. Note In order to optimize N+1 Redundancy behavior among the switch modules in the Cisco RF Switch, the internal mapping of the switch circuitry calls for the interfaces to be addressed as they are displayed in the example, below—A H B I C J D K L F M G N.

Command or Action	Purpose
Convert the eight resulting binary quartets into decimal values as follows:	Interim step.

Command or Action	Purpose
Convert the eight resulting decimal values into hexadecimal values as follows.	The eight resulting hexadecimal characters (in sequence) comprise the eight-character hexadecimal module bitmap for the first MAC domain featuring cable connections to interfaces A, B, C, D, and F on the Cisco RF Switch. Therefore, the resulting module bitmap is AA200000.

Command or Action	Purpose
Repeat the steps above for the second MAC domain.	Your resulting hexadecimal values should be as follows:

Therefore, the resulting module bitmap is 55100000.

**Note**

It is also permissible (and in some cases, recommended) to map the entire collection of cables from a cable interface line card into a single bitmap so that the entire cable interface line card switches over in the event of a local or remote failure. In such an instance, the combined layout of the two groups exemplified above would be as follows:

Interface	A	H	B	I	C	J	D	K	E	L	F	M	G	N	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	
Binary	1	1	1	1	1	1	1	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Decimal	15				15				5				0				0				0				0				0				
Hexadecimal	F				F				5				0				0				0				0				0				

After this combination, the resulting module bitmap is FF500000.

**Tip**

Cisco has provided for switchover of an entire cable interface line card by implementing a default module bitmap (referred to by the keyword **all**) that features an actual hexadecimal module bitmap value of FFFFFFFF.

It is also permissible (and in some cases, recommended) to map the entire collection of cables from a cable interface line card into a single bitmap so that the entire cable interface line card switches over in the event of a local or remote failure.

In such an instance, the combined layout of the two groups illustrated above would be as follows:

If you have a fault on one MAC domain, the other MAC domains will not switch over gracefully merely by toggling the Cisco RF Switch relays. If you have keepalive configured on the other MAC domains, they will eventually switch over, but not efficiently.

Another method is to have each interface track the other. Therefore, if one interface from a uBR10-LCP2-MC28C cable interface line card goes down, the other interfaces will follow if they have the tracking statement. With this approach, the interface cable 5/0/0 would show the following configuration, for example:

```
hccp 1 track c5/0/1
```

Interface 5/0/1 would show the following configuration:

```
hccp 2 track c5/0/0
```

**Tip**

Cisco recommends that you disable automatic HCCP revertive functions on both Protect downstream channels of a JIB that use keepalive or tracking. Refer to the [“Disabling HCCP Revertive on Protect Cable Interfaces”](#) section on page 224.

Cisco CMTS Configuration Tasks for N+1 Redundancy

You must configure and activate both the Cisco RF Switch and the Cisco CMTS to ensure that N+1 Redundancy operates correctly.



Note

Before a switchover can occur, the HCCP Protect interface automatically loads multiple configurations from the HCCP Working interface. All configurations are loaded to Protect automatically except DS modulation, DS interleave depth, and the DOCSIS Annex mode.

If Protect interface configuration occurs at the time of switchover, the PHY parameters are reset and cable modems go offline. To prevent this scenario, the Protect interface is synchronized with the latest 'sync' status received from any Working interface. Therefore, it is required that all HCCP Working interfaces within an HCCP group have identical configurations for the command-line interfaces described in this section. Any one of these Working interfaces provides the configuration of HCCP Protect interfaces.

Perform these procedures in sequence when configuring N+1 Redundancy on the Cisco CMTS.

	Procedure	Purpose
Step 1	Preconfiguring HCCP Protect Interfaces for N+1 Redundancy	(Required) Defines three functions on the HCCP Protect interfaces: DS modulation, DS interleave depth, and DOCSIS Annex mode.
Step 2	Operating DHCP with the Cisco RF Switch	(Optional) Provides instructions for using the DHCP client. DHCP operation is enabled by default, unless the user has set a static IP address from the RF Switch command-line interface (CLI). Commands have been added/enhanced to support DHCP operation.
Step 3	Configuring HCCP Groups for N+1 Redundancy	(Required) Defines HCCP Working and Protect interfaces, Cisco RF Switch commands, and upconverter statements (optional) on the Cisco CMTS as the first step in N+1 configuration.
Step 4	Enabling HCCP Protect Interfaces for N+1 Redundancy	(Required) Enables HCCP Protect interfaces, making ready for N+1 switchover from HCCP Working interfaces in the case of their failure.
Step 5	Maintaining Online Cable Modem Service When Removing HCCP Configuration from Working HCCP Interfaces	(Optional) Prevents cable modems from going offline during removal of HCCP configuration from Working interfaces.

Preconfiguring HCCP Protect Interfaces for N+1 Redundancy

There are three specific HCCP functions that do not synchronize between Working and Protect interfaces. Therefore, each HCCP interface should be configured in identical fashion for the following functions. These functions require manual configurations on HCCP Protect interfaces, as follows:

- downstream modulation—the modulation scheme used for downstream traffic to the subscriber’s cable modem
- downstream interleave depth—the interleaving amount of downstream symbols for impulse noise issues
- the DOCSIS Annex mode—the Motion Picture Experts Group (MPEG) framing format for a downstream port on a cable interface line card:
 - Annex A (Europe)
 - Annex B (North America)

These manual preconfigurations prevent HCCP Protect interfaces from inheriting unexpected or non-standard configurations from HCCP Working interfaces during switchover. Each of these three preconfigurations must be the same for all members of each HCCP group.

To define downstream modulation, interleave depth and downstream annex mode on your HCCP Protect interfaces, perform these steps at the Cisco IOS command-line interface (router console).

SUMMARY STEPS

1. **enable**
2. **config terminal**
3. **interface** *cableslot/subslot/port*
4. **cable downstream modulation { 64qam | 256qam }**
5. **cable downstream interleave-depth { 8 | 16 | 32 | 64 | 128 }**
6. **cable downstream annex { A | B }**
7. **Ctrl-Z**
8. **write memory**

DETAILED STEPS

	Command	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal Example: Router# config t	Moves to global configuration mode.

Step 3	interface <i>cableslot/subslot/port</i> Example: Router# interface cable8/1/0	Moves to interface configuration mode. Note Syntax for Interface Configuration mode differs between the Cisco uBR1012 and the Cisco uBR7246VXR routers. Refer to the Cisco Broadband Cable Command Reference Guide for complete command information.
Step 4	cable downstream modulation { 64qam 256qam } Example: Router(config-if)# cable downstream modulation 256qam	Sets the modulation format for a downstream port on a cable interface line card. The default setting is 64qam. • 64qam—Modulation rate is 6 bits per downstream symbol. • 256qam—Modulation rate is 8 bits per downstream symbol.
Step 5	cable downstream interleave-depth { 8 16 32 64 128 } Example: Router(config-if)# cable downstream interleave-depth 128	Sets the downstream interleave depth. A higher interleave depth provides more protection from bursts of noise on the HFC network by interleaving downstream symbols. The default setting is 32. • { 8 16 32 64 128 }—Indicates the downstream interleave depth in amount of symbols.
Step 6	cable downstream annex { A B } Example: Router(config-if)# cable downstream annex a	Sets the Motion Picture Experts Group (MPEG) framing format for a downstream port on a cable interface line card to either Annex A (Europe) or Annex B (North America). The default setting for Annex mode varies according to the cable interface line card or BPE in use. Refer to the corresponding configuration feature module for your specific modules. • A—Annex A. The downstream uses the EuroDOCSIS J.112 standard. • B—Annex B. The DOCSIS-compliant cable plants that support North American channel plans use ITU J.83 Annex B downstream radio frequency.
Step 7	Ctrl-Z Example: Router(config-if)# Ctrl^Z	When you have included all of the configuration commands to complete the configuration, enter ^Z (press the Control key while you press Z) to exit configuration mode.
Step 8	write memory Example: Router# write mem [OK] Router#	Writes the new configuration to nonvolatile random access memory (NVRAM). The system displays an OK message when the configuration has been stored.

For additional information about the commands in this section, refer to the [Cisco Broadband Cable Command Reference Guide](#) on Cisco.com.

Operating DHCP with the Cisco RF Switch

The latest Cisco IOS software release in support of the Cisco RF Switch includes full support for a DHCP client. DHCP operation is enabled by default, unless the user has set a static IP address defined at the command-line interface (CLI). Commands have been added/enhanced to support DHCP operation.

When the RF Switch boots, it checks to see if DHCP has been enabled. This is done via the RF Switch CLI in a variety of ways. You can use any of the following commands to enable DHCP:

- **set ip address dhcp**
- **set ip address** *ip-address subnet-mask*
- **no set ip address** (to set the default, with DHCP now the default)

**Note**

The RF Switch Firmware no longer assumes a static IP address of 10.0.0.1 as in versions prior to 3.00.

If enabled, the Cisco RF Switch installs the DHCP client and attempts to locate a DHCP server to request a lease. By default, the client requests a lease time of 0xffffffff (infinite lease), but this can be changed using the **set dhcp lease leasetime** command in User mode at the `rfswitch>` prompt, where *leasetime* is seconds. Because the actual lease time is granted from the server, this command is primarily used for debugging and testing purposes, and should not be required for normal operation.

When a server is located, the client requests settings for IP address and subnet mask, a gateway address, and the location of a TFTP server. The gateway address is taken from Option 3 (Router Option). The TFTP server address can be specified in a number of ways. The client checks the next-server option (*siaddr*), Option 66 (TFTP server name) and Option 150 (TFTP server address). If all three of the above are absent, the TFTP server address defaults to the DHCP server address. If the server grants a lease, the DHCP client records the offered lease time for renewal, and continues with the boot process, installing the other network applications (Tenet and SNMP), and the CLI.

When a server is not located within 20-30 seconds, the DHCP client is suspended and the CLI runs. The DHCP client will run in the background attempting to contact a server approximately every five seconds until a server is located, a static IP is assigned via the CLI, or the system is rebooted.

The CLI allows the user to override any of the network settings that may be received via the server, and assign static values for these settings. All of the “SET xxx” parameters are stored in `nvram`, and are used across reboots. Because the current network settings now may come from either DHCP or the CLI, a few changes/new commands have been implemented. First, the existing SHOW CONFIG command has been changed to show the settings of all the `nvram` parameters, which are not necessarily the ones in effect at the time.

To obtain the current network parameters in use, the new command SHOW IP has been added. In addition to the network settings, this command also shows the current IP mode (static versus DHCP), the status of the DHCP client, and the status of the Telnet and SNMP applications (which are only started if a valid IP exists).

An additional command, SHOW DHCP, has been added for informational purposes. This command shows the values received from the DHCP server, as well as the status of the lease time. The time values shown are in the format HH:MM:SS, and are relative to the current system time, which is also displayed.

Assignment of static values for any of the definable network parameters should go into effect immediately, and override the current setting without further action. This allows some of the parameters to remain dynamic, while fixing others. For example, DHCP could be used to obtain the IP address, while retaining the setting for the TFTP server set via the CLI. The one exception to this is when going from using a static IP to DHCP. Since the DHCP client is only installed at boot-up as required, transitioning from a static IP to DHCP requires the system to be rebooted for DHCP to take effect.

Configuring HCCP Groups for N+1 Redundancy

Once the Cisco RF Switch has been configured and enabled to support N+1 Redundancy, you must configure Cisco IOS and Cisco RF Switch Firmware to support the Cisco RF Switch. This procedure defines HCCP Working and Protect interfaces, Cisco RF Switch commands, and upconverter statements (optional) on the Cisco CMTS as the first step in N+1 configuration.


Note

When the Cisco CMTS CLI descriptions include the term *channel switch*, this term refers to the Cisco RF Switch.


Note

When configuring Hot-Standby Connection-to-Connection Protocol (HCCP) on the Cisco uBR10012 router, use the IP address from the local loopback interface as the Working interface IP address. Cisco strongly recommends that you create a loopback interface on the Cisco uBR10012 router, and then assign the loopback interface's IP address to the HCCP Protect configuration.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface cable** *slot/subslot/port*
4. **hccp group working member**
5. **hccp group protect member ip-address**
6. **hccp group channel-switch member-id upconverter name wavecom-xx**
protect-upconverter-ip-address module (upconverter) working-ip-address its-module
7. **hccp group channel-switch member-id channel-switch-name rfswitch-group ip-address**
module-bitmap position
8. **Ctrl-Z**
9. **write memory**

DETAILED STEPS

	Command	Purpose
Step 1	enable	Enables privileged EXEC mode.
	Example: Router> enable	Enter your password if prompted.
Step 2	configure terminal	Moves to global configuration mode.
	Example: Router# config t	
Step 3	interface cable <i>slot/subslot/port</i>	Moves to interface configuration mode.
	Example: Router# interface cable8/1/0	Note Syntax for Interface Configuration mode differs between the Cisco uBR1012 and the Cisco uBR7246VXR routers. Refer to the Cisco Broadband Cable Command Reference Guide for complete command information.

Step 4	hccp group working member-id Example: Router(config-if)# hccp 1 working 1	Designates a cable interface on a CMTS in the specified HCCP group to be a Working CMTS. Note The hccp group working member command is to be used for Working line card interfaces only. • <i>group</i>—The group number for the specified interface. Valid values are any number from 1 to 255, inclusive. • <i>member-id</i>—The member number for the specified interface. Valid values are any number from 1 to 255, inclusive.
Step 5	hccp group protect member-id ip-address Example: Router(config-if)# hccp 1 protect 2 10.10.10.1	Assigns the HCCP group number, defines the corresponding HCCP member, and defines the Working IP address of the interface used for HCCP communication. Note The hccp group protect member-id command is to be used for Protect line card interfaces only. Note The Working and Protect line cards are located on different chassis when using the Cisco uBR7246VXR router. Working and Protect line cards are located on the same Cisco uBR10012 router chassis. In the latter case, Cisco recommends that you use the Loopback IP address in this configuration.
Step 6	hccp group channel-switch member-id upconverter name wavcom-xx protect-upconverter-ip-address module (upconverter) working-ip-address its-module Example: Router(config-if)# hccp 1 channel-switch 2 uc wavcom-hd 10.97.1.21 2 10.97.1.21 14	Upconverter (optional). Configures the upconverter (UPx) topology so that the VCom upconverter becomes part of the specified HCCP member in a particular HCCP group. Note This procedure is not required when configuring N+1 Redundancy on the Cisco uBR10012 router with the Cisco UBR10-MC 5X20U or -S/D BPE. Note Steps 6 and 7 of this procedure are required for both the Working and the Protect interfaces.
Step 7	hccp group channel-switch member-id channel-switch-name rfswitch-group ip-address module-bitmap position Example: Router(config-if)# hccp 1 channel-switch 2 rfswitch-name rfswitch-group 10.97.1.20 AA200000 2	Configures the Cisco CMTS so that the specified Cisco RF Switch becomes part of the specified HCCP member in a particular HCCP group. • <i>ip address</i> — The IP address of the Cisco RF Switch. • <i>rf-switch-name</i> — Specifies the name of the Cisco RF Switch, and must also include the hexadecimal module-bitmap argument. Refer to the “Creating Cisco RF Switch Module Bitmaps” section on page 238 for instructions on creating an appropriate hexadecimal module bitmap. • <i>position</i> — This value specifies the slot/header of the Cisco RF Switch—there are eight on the Cisco uBR10012. Note Steps 6 and 7 of this procedure are required for both the Working and the Protect interfaces.
Step 8	Ctrl-Z Example: Router(config-if)# Ctrl+Z	Exits interface configuration mode, and returns you to global configuration mode.
Step 9	write memory Example: Router# copy running-config startup-config or Router# write memory	After configuring all domains, save your settings to the nonvolatile random access memory (NVRAM) to ensure that the system retains the settings after a power cycle.

For additional information about the commands in this section, refer to the [Cisco Broadband Cable Command Reference Guide](#) on Cisco.com.

Enabling HCCP Protect Interfaces for N+1 Redundancy

To enable HCCP Protect interfaces, making them available for N+1 switchover should the HCCP Working interfaces fail, use the **no shutdown** command in interface configuration mode on each HCCP Protect interface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface cableslot/subslot/port**
4. **no shutdown**
5. Repeat steps 3-4.
6. **Ctrl-Z**
7. **write memory**

DETAILED STEPS

	Command	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal Example: Router# config t	Moves to global configuration mode.
Step 3	interface cableslot/subslot/port Example: Router# interface cable8/1/0 Router(config-if)#	Moves to interface configuration mode for the desired interface. Select the HCCP Protect interface. Note Syntax for Interface Configuration mode differs between the Cisco uBR1012 and the Cisco uBR7246VXR routers. Refer to the Cisco Broadband Cable Command Reference Guide for complete command information.
Step 4	no shutdown Example: Router(config-if)# no shut	Enables the HCCP Protect interface.
Step 5	Repeat	Repeat steps 3-4 for every HCCP Protect interface.
Step 6	Ctrl-Z Example: Router(config-if)# Ctrl^Z	Exits interface configuration mode, and returns you to global configuration mode.
Step 7	write memory Example: Router# write mem	After enabling all HCCP Protect interfaces, save your settings to the nonvolatile random access memory (NVRAM) to ensure that the system retains the settings after a power cycle

Maintaining Online Cable Modem Service When Removing HCCP Configuration from Working HCCP Interfaces

- The following HCCP restriction applies to HCCP N+1 Redundancy on either the Cisco uBR10012 or Cisco uBR7246VXR router:
- Before removing HCCP configuration from an active Working interface, either shut down the protect or lockout switchover functions using the **hccp** group **lock** *member-id* command in interface configuration mode. Otherwise the Protect interface will declare the Working interface to have failed and will attempt to switch over.
 - Do not remove HCCP configuration from an active protect interface. The active member should be restored to its corresponding working interface (revertback) before removing HCCP configuration from the Protect interface.



Note

This restriction does not apply when removing HCCP configuration from a Protect interface while it is in standby mode and N+1 Redundancy is in normal Working mode.

- To prevent cable modems from going offline during removal of HCCP configuration (on Working interfaces), Cisco recommends using one of the following three procedures as a best practice:
- [Shutting Down HCCP Protect Interfaces](#)
 - or
 - [Locking out HCCP Interface Switchover](#)
 - [Removing HCCP Configuration from HCCP Working or HCCP Protect Interfaces](#)

Shutting Down HCCP Protect Interfaces

SUMMARY STEPS

1. **enable**
2. **config t**
3. **interface** *slot/subslot/port*
4. **shutdown**
5. Repeat the above steps as required to shutdown all Protect HCCP interfaces.

DETAILED STEPS

	Command	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal Example: Router# config t	Moves to global configuration mode.

Step 3	interface cable <i>slot/subslot/port</i> Example: Router# interface cable8/1/0	Moves to interface configuration mode.
Step 4	shutdown Example: Router(config-if)# shutdown	Shuts down the specified interface. This does not remove interface configuration—merely disables it.
Step 5	Repeat.	Repeat the above steps as required to shut down all Protect HCCP interfaces.

Locking out HCCP Interface Switchover

SUMMARY STEPS

1. **enable**
2. **hccp group lockout** *member-id*
3. Repeat above steps as required to lock out all Working HCCP interface switchovers.
4. **hccp group unlockout** *member*
5. **Ctrl-Z**
6. **write memory**

DETAILED STEPS

	Command	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	hccp group lockout <i>member-id</i> Example: Router# hccp 1 lockout 1	To prevent a Working HCCP interface from automatically switching to a Protect interface in the same group, use the hccp lockout command in privileged EXEC mode. This command disables HCCP for the specified member of the specified group. • <i>group</i> — The group number for the specified interface. Valid values are any number from 1 to 255, inclusive. • <i>member-id</i> — The member number for the specified interface. Valid values are any number from 1 to 255, inclusive. Note Even if an HCCP member is locked out, it switches over in circumstances in which it is tracking another HCCP interface. This condition applies when HCCP interfaces are configured manually to track each other, or when HCCP interfaces share the same JIB, such as with the Cisco UBR10-MC 5X20U or -S/D. Note With the Cisco uBR7246VXR CMTS, HCCP interface tracking occurs across all interfaces that share the same cable interface IP bundle. Therefore, if any one HCCP interface switches over, all interfaces in that bundle will switch over together, regardless of whether they are locked out or not.

Step 3	Repeat.	Repeat the above steps as required to prevent a Working interface from switching over. This manual override can be removed when desired, and retains HCCP configuration on the interface.
Step 4	hccp group unlockout member Example: Router# hccp 1 unlockout 1	Disables the HCCP lockout feature when desired (re-enabling N+1 Redundancy on the Working interface). <i>group</i> — The group number for the specified interface. Valid values are any number from 1 to 255, inclusive. <i>member-id</i> — The member number for the specified interface. Valid values are any number from 1 to 255, inclusive.

For additional information about the commands in this section, refer to the [Cisco Broadband Cable Command Reference Guide](#) on Cisco.com.

Removing HCCP Configuration from HCCP Working or HCCP Protect Interfaces

SUMMARY STEPS

1. **enable**
2. **config t**
3. **interface slot/subslot/port**
4. **no hccp group {working | protect} member**
5. Repeat the above steps as required to remove all Protect HCCP interface configurations.

DETAILED STEPS

	Command	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: Router# config t	Moves to global configuration mode.
Step 3	interface cable slot/subslot/port Example: Router# interface cable8/1/0	Moves to interface configuration mode.
Step 4	no hccp group {working protect} member-id Example: Router(config-if)# no hccp 1 protect 1	Turns off HCCP, and removes the specified HCCP configuration from the specified interface. <i>group</i> — The group number for the specified interface. Valid values are any number from 1 to 255, inclusive. <i>member-id</i> — The member number for the specified interface. Valid values are any number from 1 to 255, inclusive.
Step 5	Repeat.	Repeat the above steps as required to remove HCCP configuration from all desired HCCP Protect interfaces.

For additional information about the commands in this section, refer to the [Cisco Broadband Cable Command Reference Guide](#) on Cisco.com.

Switchover Testing Tasks for N+1 Redundancy

Each of these switchover test methods below provides an opportunity to test N+1 Redundancy on your Cisco uBR10012 or Cisco uBR7246VXR CMTS. Each test method results in the cable modems dropping connectivity temporarily, but staying online, with switchover to Protect line cards and interfaces.

Electromagnetic relays can develop a magnetic charge over time that could interfere with normal operations. Therefore, Cisco recommends periodic testing using these procedures to ensure smooth operation. The tests in this section help to improve overall system availability.

These switchover testing tasks apply to switchover from HCCP Working interfaces to HCCP Protect interfaces, or vice versa, when configured in N+1 Redundancy.

- [Pre-testing System Check Procedures, page 251](#)
- [Switchover Testing Procedures, page 255](#)

**Note**

To test route processor switchover functions on the Cisco uBR10012 router, refer to the document [Route Processor Redundancy Plus on the Cisco uBR10012 Universal Broadband Router](#) on Cisco.com.

Pre-testing System Check Procedures

As a best practice, Cisco strongly recommends analyzing the CMTS headend status prior to switchover testing.

**Caution**

Switchover testing with latent configuration or status problems can create disruptions in subscriber service.

Use these pre-test system checks prior to manual switchover testing:

- [Displaying HCCP Group Status on the Cisco CMTS, page 251](#)
- [Displaying HCCP Working and HCCP Protect Interface Status, page 253](#)
- [Displaying Cisco RF Switch Module Status on the Cisco RF Switch, page 254](#)

Displaying HCCP Group Status on the Cisco CMTS

As a best practice, Cisco recommends that you perform this test prior to performing any manual switchovers. This status check verifies stable redundancy operations. Should this procedure reveal any problems with online states, resolve these problems prior to performing a manual switchover. Otherwise, manual switchover for testing purposes might create additional problems.

SUMMARY STEPS

1. **enable**
2. **show hccp {group-member} channel-switch**
3. **show ip interface brief**

DETAILED STEPS

	Command	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	show hccp {group-member} channel-switch Example: Router# show hccp channel-switch Grp 1 Mbr 1 Working channel-switch: "uc" - enabled, frequency 555000000 Hz "rfswitch" - module 1, normal module 3, normal module 5, normal module 7, normal module 11, normal . . . Note For a complete example of command output, refer to the “Example: Channel Switch Information from the Cisco uBR10012 Router” section on page 273.	To display HCCP group status on the Cisco CMTS, including Cisco RF Switch information relevant to N+1 Redundancy behavior, use the show hccp channel-switch command in privileged EXEC mode. This command displays status for all channel switches belonging to the specified HCCP group and HCCP member. <i>group-member</i>—Optionally specifies a specific HCCP group member. If you do not specify an HCCP group member, the CMTS displays status for all channel switches known to the router. Potential causes for a fault or an unknown state while using the show hccp channel-switch command are: - SNMP misconfiguration on the Cisco RF Switch or CMTS - misconfigured access lists Note This command does not display HCCP interfaces that have been shut down (disabled).
Step 3	show ip interface brief Example: Router# show ip interface brief Interface IP-Address OK? Method Status Protocol Ethernet0/0/0 127.0.0.254 YES unset up up FastEthernet0/0/0 1.8.22.13 YES NVRAM up up SRP2/0/0 200.1.1.10 YES NVRAM up up SRP4/0/0 202.1.1.10 YES NVRAM up up Cable5/0/0 130.1.1.1 YES NVRAM up up Cable5/0/1 unassigned YES NVRAM up up Loopback0 203.1.1.10 YES NVRAM up up	Displays a summary of all interfaces, including the DPT WAN card.

For additional information about the commands in this section, refer to the [Cisco Broadband Cable Command Reference Guide](#) on Cisco.com.

Displaying HCCP Working and HCCP Protect Interface Status

As a best practice, Cisco recommends that you perform this test prior to performing any manual switchovers. This status check confirms the enabling of HCCP interfaces, and the direction of pending manual switchover tests.

To display a brief summary of the HCCP groups, configuration types, member numbers, and status for cable interfaces, use the **show hccp brief** command at the Cisco RF Switch prompt.

SUMMARY STEPS

1. **show hccp brief**

DETAILED STEPS

	Command	Purpose
Step 1	show hccp brief Example: Router# show hccp brief <pre> Interface Config Grp Mbr Status Ca5/0/0 Protect 1 3 standby Ca7/0/0 Working 1 3 active </pre>	To confirm that HCCP Working or Protect interfaces are configured and enabled, use the show hccp brief command in user EXEC or privileged EXEC mode. Note This command does not display HCCP interfaces that have been shut down (disabled). For complete information about the show hccp command, refer to the <i>Cisco Broadband Cable Command Reference Guide</i> on Cisco.com: http://www.cisco.com/univercd/cc/td/doc/product/cable/bccmref/index.htm

Examples

In Cisco IOS Release 12.2(8)BC2 and later 12.2 BC releases, the **brief** option also shows the amount of time left before the next re-synchronization and the time left before a restore:

Router# **show hccp brief**

```

Interface Config    Grp Mbr Status          WaitToResync    WaitToRestore
Ca5/0/0    Protect    1   3  standby          00:01:50.892
Ca7/0/0    Working    1   3   active          00:00:50.892    00:01:50.892

```

Router#

Displaying Cisco RF Switch Module Status on the Cisco RF Switch

As a best practice, Cisco recommends that you perform this pretest status check prior to performing any manual switchovers. This status check confirms the online and administrative states for all modules on the Cisco RF Switch itself.

To display current module status for one or more modules on the Cisco RF Switch, use the **show module all** command at Cisco RF Switch prompt.

SUMMARY STEPS

1. **show module {*module* | *group-name* | all}**

DETAILED STEPS

		Command	Purpose																																																							
Step 1	:	show module {<i>module</i> <i>group-name</i> all}	This command displays current status with these options: • a single, specified module • a group of modules • all modules on the Cisco RF Switch																																																							
		Example: <pre>rfswitch> show module all</pre> <table border="1"> <thead> <tr> <th>Module</th><th>Presence</th><th>Admin</th><th>Fault</th></tr> </thead> <tbody> <tr><td>1</td><td>online</td><td>0</td><td>ok</td></tr> <tr><td>2</td><td>online</td><td>0</td><td>ok</td></tr> <tr><td>3</td><td>online</td><td>0</td><td>ok</td></tr> <tr><td>4</td><td>online</td><td>0</td><td>ok</td></tr> <tr><td>5</td><td>online</td><td>0</td><td>ok</td></tr> <tr><td>6</td><td>online</td><td>0</td><td>ok</td></tr> <tr><td>7</td><td>online</td><td>0</td><td>ok</td></tr> <tr><td>8</td><td>online</td><td>0</td><td>ok</td></tr> <tr><td>9</td><td>online</td><td>0</td><td>ok</td></tr> <tr><td>10</td><td>online</td><td>0</td><td>ok</td></tr> <tr><td>11</td><td>online</td><td>0</td><td>ok</td></tr> <tr><td>12</td><td>online</td><td>0</td><td>ok</td></tr> <tr><td>13</td><td>online</td><td>0</td><td>ok</td></tr> </tbody> </table>	Module	Presence	Admin	Fault	1	online	0	ok	2	online	0	ok	3	online	0	ok	4	online	0	ok	5	online	0	ok	6	online	0	ok	7	online	0	ok	8	online	0	ok	9	online	0	ok	10	online	0	ok	11	online	0	ok	12	online	0	ok	13	online	0	ok
Module	Presence	Admin	Fault																																																							
1	online	0	ok																																																							
2	online	0	ok																																																							
3	online	0	ok																																																							
4	online	0	ok																																																							
5	online	0	ok																																																							
6	online	0	ok																																																							
7	online	0	ok																																																							
8	online	0	ok																																																							
9	online	0	ok																																																							
10	online	0	ok																																																							
11	online	0	ok																																																							
12	online	0	ok																																																							
13	online	0	ok																																																							

For additional information about the command in this section, refer to the [Cisco Broadband Cable Command Reference Guide](#) on Cisco.com.

Switchover Testing Procedures

The first two procedure below describe how to test the performance of N+1 Redundancy on your Cisco CMTS headend. The final procedure describes how to analyze Cisco CMTS headend status after switchover.

- [Testing Cisco RF Switch Relays with Manual Switchover, page 255](#)
- [Testing HCCP Groups with Manual Switchover, page 257](#)
- [Using the show cable modem Command After a Manual Switchover, page 258](#)

Testing Cisco RF Switch Relays with Manual Switchover

Cisco recommends testing the switch relays once a week (optimal) and at least once a month (minimal). Perform these steps to test the Working RF Switch relays with switchover to Protect.

**Tip**

You can toggle the relays on the switch without affecting the upconverter or any of the modems. This is important if testing the relays without actually switching any of the line cards or the corresponding upconverters. If a relay is enabled on the switch and a fail-over occurs, it will go to the proper state and not just toggle from one state to another.

SUMMARY STEPS

1. **telnet**
2. **test module or switch** *group-name 1*
3. **switch** *group-name 0*

DETAILED STEPS

	Command or Action	Purpose
Step 1	telnet <i>ip-address</i> / noecho Example: Router# telnet 172.16.10.3 /noecho	Initiate configuration by connecting to the Cisco RF Switch using the console or by using a Telnet session. Either provides CLI access for initiating a switchover. If a Telnet password is set on the Cisco RF Switch, type password <i>string</i>, where <i>string</i> is the previously-defined password set on the RF Switch. The Telnet password is set using the separate set password <i>string</i> command in Cisco RF Switch User mode. Note To prevent multiple users from changing the Firmware configuration at any one time, only a single Telnet client connection can be opened at a time, regardless of whether this connection is password-protected. Telnet access to the RF Switch from the router console makes double entries when typing. One workaround is to disable local echo. For example, from the Cisco uBR10012 router CLI, use the /noecho option (as shown at left). Common Telnet disconnect methods are as follows: • Press Ctrl+Break. • Press Ctrl+]. • Type quit or send break. Another Telnet disconnect method is as follows: a. Press Ctrl+Shift 6 6 x. b. Type disc 1 from the router CLI. For additional Telnet break sequences, refer to the document Standard Break Key Sequence Combinations During Password Recovery on Cisco.com.
Step 2	test module Example: rfswitch> test module or switch <i>group-name</i> <i>x</i> Example: rfswitch> switch 13 1	The test module command tests all the relays at once, and then returns to the normal Working mode.  Caution Do not use the test module command while in the Protect mode. Alternately, you can test an entire bitmap with switch <i>group-name</i> <i>x</i>, where <i>x</i> is the RF Switch header number. For example, the switch 13 1 tests port G on slot 1 of the Cisco RF Switch.
Step 3	switch <i>group-name</i> 0 Example: rfswitch> switch 13 0	Use the command switch <i>group name</i> 0 (or idle) to disable the relays, and to return to normal Working mode.

For additional information about the commands in this section, refer to the [Cisco Broadband Cable Command Reference Guide](#) on Cisco.com.

Testing HCCP Groups with Manual Switchover

Cisco recommends that you perform a periodic CLI switchover test of an HCCP group from the CMTS to test the Protect card and path. However, this type of switchover may take 4-6 seconds and could cause a small percentage of modems to go offline. Therefore, this test should be performed less often than previous tests, and only during off-peak hours.

SUMMARY STEPS

1. **enable**
2. **hccp group switch member**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	hccp group switch member Example: Router# hccp 1 switch 1	Manually switches a Working CMTS with its Protect CMTS peer (or vice versa).

For additional information about the commands in this section, refer to the [Cisco Broadband Cable Command Reference Guide](#) on Cisco.com.

Using the show cable modem Command After a Manual Switchover

If you are using HCCP 1+1 or N+1 Redundancy, the new primary processor after a switchover automatically creates a new database of the online cable modems. Use the following procedure to force IP traffic and to display cable modem status and information.

SUMMARY STEPS

1. **enable**
2. **show cable modem ip-address**
3. **ping ip-address**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	show cable modem ip-address Example: Router# show cable modem 172.16.10.3 MAC Address IP Address I/F MAC Prim RxPwr Timing Num BPI State Sid (db) Offset CPE Enb 0000.3948.ba56 8.60.0.8 C6/0/0/U0 online 1 0.50 2138 0 N	Identifies the IP address of a specific cable modem to be displayed. You can also specify the IP address for a CPE device behind a cable modem, and information for that cable modem is displayed.
Step 3	ping ip-address Example: Router# ping 172.16.10.3	Forces IP traffic by sending an ICMP ECHO packet.

For additional information about the commands in this section, refer to the [Cisco Broadband Cable Command Reference Guide](#) on Cisco.com.

Configuration Examples for Cisco N+1 Redundancy

This section provides the following configuration examples of N+1 Redundancy. Each chassis-level example below illustrates a distinct implementation of N+1 Redundancy on the Cisco CMTS.

Table 3 Summary Table of N+1 Configuration Examples—Cisco IOS 12.2(15)BC2a, Firmware 3.50

Example	Cisco RF Switch ¹	N+1 Mode	Cisco Router Chassis ²	Cisco Cable Interface Line Cards	Upconverters
Cisco RF Switch Module Examples					
Example: Cisco 3x10 RF Switch Modules in 8+1 Mode	3x10 RF	8+1 ³	uBR10012	Not described	Not described
Example: Cisco 3x10 RF Switch Modules in 4+1 Mode	3x10 RF	4+1	uBR7246VXR (five)	uBR10K-MC28C	VCom HD4040 (three)
Cisco uBR10012 Chassis Configuration Examples					
Examples: Cisco 3x10 RF Switch with Cisco uBR10012 Chassis	3x10 RF	8+1 ³	uBR10012	UBR10-MC 5X20U or -S/D (five)	Not described
Example: Channel Switch Information from the Cisco uBR10012 Router	3x10 RF	8+1 ³	uBR10012	Not described	Not described
Example: Cisco 3x10 RF Switch and Cisco uBR10012 Chassis	3x10 RF	8+1 ³	uBR10012	uBR10-LCP2-MC28C (eight)	Not described
Example: Cisco 3x10 RF Switches and Cisco uBR10012 Chassis	3x10 RF (two)	8+1 ³	uBR10012	UBR10-MC 5X20U or -S/D	Not described
Cisco uBR7246VXR Chassis Configuration Examples					
Example: Cisco 3x10 RF Switches and uBR7246VXR Chassis	3x10 RF (two)	4+1	uBR7246VXR (five)	uBR-MC28U/X (20)	Not described

1. Assume one Cisco RF Switch per example unless more are cited.
2. Assume one Cisco router chassis per example unless more are cited.
3. The term of "8+1 Redundancy" is often referred to as "7+1 Redundancy" in the field—physically, eight line cards in "8+1" mode are configured as seven Working line cards with one Protect line card. Therefore, "7+1 Redundancy" is the more physically accurate term. By contrast, "4+1 Redundancy" (predictably) refers to four Working line cards with one additional Protect line card.

Example: Cisco 3x10 RF Switch Modules in 8+1 Mode

The following is sample output for the **show module all** command from a Cisco RF Switch that has been configured for 8+1 Redundancy:

```
rfswitch> show module all
```

Module	Presence	Admin	Fault
1	online	0	ok
2	online	0	ok
3	online	0	ok
4	online	0	ok
5	online	0	ok
6	online	0	ok
7	online	0	ok
8	online	0	ok
9	online	0	ok
10	online	0	ok
11	online	0	ok
12	online	0	ok
13	online	0	ok

The Administrative State field (Admin) indicates the following potential states:

- 0 — Indicates normal Working state.
- 1-8 — Indicates that there has been a switchover and the corresponding module is in Protect mode, and the header is being protected. For example, an Admin state of 8 for Module 1 would indicate a switchover for port A (Module 1) on header 8 on the Cisco RF Switch. After a switchover, verify that this Admin state corresponds with the actual wiring on the Cisco RF Switch.
- 9—Indicates fault for the specified module.

The following is sample output for the **show config** command from a Cisco 3x10 RF Switch configured in 8+1 Redundancy mode:

```
rfswitch> show config

IP addr: 172.18.73.3
Subnet mask: 255.255.255.0
MAC addr: 00-03-8F-01-04-13

Gateway IP: 172.18.73.1
TFTP host IP: 172.18.73.2
TELNET inactivity timeout: 600 secs
Password: (none)

SNMP Community: private
SNMP Traps: Enabled
SNMP Trap Interval: 300 sec(s)
SNMP Trap Hosts: 1
    172.18.73.165

Card Protect Mode: 8+1
Protect Mode Reset: Disabled
Chassis Config: 13 cards
Watchdog Timeout: 20 sec(s)

Group definitions: 3
  ALL      0xffffffff
  GRP1     0xaa200000
  GRP2     0x55100000
```



Note

The **show config** command for the Cisco RF Switch contains the `Card Protect Mode` field. When this field displays 8+1, this indicates that the Cisco RF Switch is configured for N+1 Redundancy, where eight or less Working line cards are possible. This field may also display 4+1, where four or less Working line cards are possible.

Example: Cisco 3x10 RF Switch Modules in 4+1 Mode

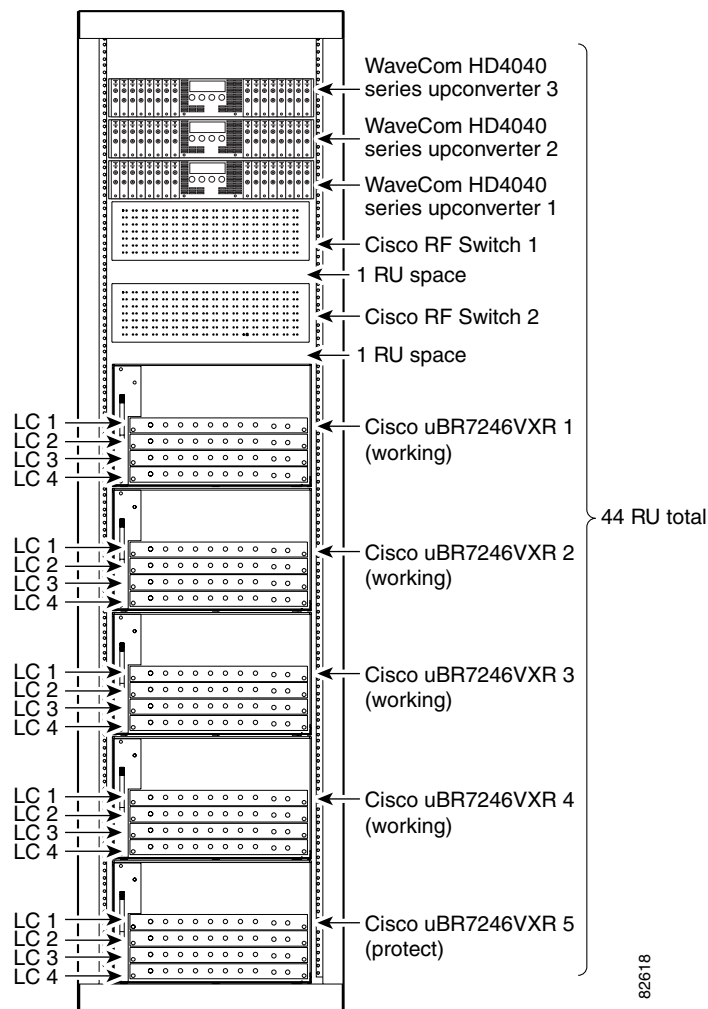
The following example configuration illustrates N+1 Redundancy using the following Cisco

- Two Cisco RF Switches (3x10) in 4+1 mode
- Five Cisco uBR7246VXR routers
- 20 Cisco uBR10K-MC28C cable interface line cards
- Three VCom HD4040 chassis containing 40 modules.

The physical layout is shown in Figure 8-4. A cabling document can be found at:

<http://www.cisco.com/univercd/cc/td/doc/product/cable/rfswitch/rfswvxc2.htm>

Figure 5 4+1 Redundancy Using Cisco MC28C Line Cards & Two Cisco RF Switches



The following physical stacking is assumed:

- IP address assignments start with 192.168.1.2 at the top, and continuing downward in sequence.
- The first Cisco RF Switch is interpreted by the Cisco CMTS to be two switches, as it is in the 4+1 mode (a & b), where a is slots 1-4 and b is slots 5-8.
- The second Cisco RF Switch is also interpreted by the Cisco CMTS to be two switches (a & b).

N+1 Configuration Example on the Working Cisco uBR7246VXR Router

```

version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname "WorkingVXR1"
!
boot system disk0:ubr7200-ik8s-mz.BC.28July03
no logging console
enable secret 5 $1$5YHG$mquxbcqzFoUUKhp/c9WT4/
!
cab modem remote-query 10 public
cab modulation-prof 2 request 0 16 0 8 qpsk scrambler 152 no-diff 64 fixed uw8
cab modulation-prof 2 initial 5 34 0 48 qpsk scrambler 152 no-diff 128 fixed uw16
cab modulation-prof 2 station 5 34 0 48 qpsk scrambler 152 no-diff 128 fixed uw16
cab modulation-prof 2 short 4 76 6 8 qpsk scrambler 152 no-diff 72 short uw8
cab modulation-prof 2 long 8 220 0 8 qpsk scrambler 152 no-diff 80 short uw8
cab modulation-prof 3 request 0 16 0 8 qpsk scrambler 152 no-diff 64 fixed uw16
cab modulation-prof 3 initial 5 34 0 48 qpsk scrambler 152 no-diff 128 fixed uw16
cab modulation-prof 3 station 5 34 0 48 qpsk scrambler 152 no-diff 128 fixed uw16
cab modulation-prof 3 short 7 76 7 8 16qam scrambler 152 no-diff 144 short uw16
cab modulation-prof 3 long 9 220 0 8 16qam scrambler 152 no-diff 160 short uw16
no cable qos permission create
no cable qos permission update
cable qos permission modems
no cable clock source-midplane
no cable clock force primary
no cable clock force secondary
!
cable config-file docsis.cm
frequency 453000000
service-class 1 max-upstream 10000
service-class 1 max-downstream 10000
service-class 1 max-burst 1522
!
ip subnet-zero
ip cef
!
ip host protect 192.168.1.7
ip host work2 192.168.1.6
ip name-server 171.68.226.120
!
ip dhcp pool MODEMS1
network 192.168.3.0 255.255.255.0
bootfile docsis.cm
next-server 192.168.3.5
default-router 192.168.3.5
option 7 ip 192.168.3.5
option 4 ip 192.168.3.5
option 2 hex 0000.0000
lease 2 3 4
!
ip dhcp pool PC
network 10.11.12.0 255.255.255.0
default-router 10.11.12.1
dns-server 171.68.226.120
lease 10 1 11
!
packetcable element_id 35417
!
interface FastEthernet0/0
ip address 192.168.1.7 255.255.255.0
no keepalive
speed auto
full-duplex
!
! This interface is used for HCCP traffic.
!
interface FastEthernet0/1
ip address 192.168.2.5 255.255.255.0
keepalive 1
!
! This is set to 1 second so if the cable was disconnected, this interface will fail over
within 3 seconds.
!
speed auto

```

```

full-duplex
!
interface Cable3/0
ip address 10.11.12.1 255.255.255.0 secondary
ip address 192.168.3.5 255.255.255.0
load-interval 30
keepalive 1
!
! The keepalive time is in seconds and the default is 10 seconds for HCCP code.
!
load-interval 30
cable downstream channel-id 0
cable bundle 1 master
!
! Interface bundling is supported as well as subinterfaces.
! Note: Interface bundles failover together.
!
cable downstream annex B
cable downstream modulation 64qam
cable downstream interleave-depth 32
cable downstream frequency 453000000
!
! This is downstream frequency, which used to be informational only when using an external
UPx. This must be set when using the MC28U cards with internal UPxs or when doing N+1
with MC28C cards, so that the Protect UPx knows which frequency to use.
!
cable upstream 0 frequency 24000000
!
! If doing dense mode combining, the upstream frequencies will need to be different. If
no two upstream ports are shared, the same frequency can be used.
!
cable upstream 0 power-level 0
cable upstream 0 channel-width 3200000
cable upstream 0 minislot-size 2
cable upstream 0 data-backoff automatic
cable upstream 0 modulation-profile 3
no cable upstream 0 shutdown

cable dhcp-giaddr policy
!
! This tells cable modems to get an IP address from the primary scope and CPEs to use the
secondary scope.
!
hccp 1 working 1
!
! This is the Working first group, member 1.
!
hccp 1 channel-switch 1 rfswl1a rfswitch-group 192.168.1.5 44440400 1
!
! This is IP add of Switch and it's protecting member 1 in the left side of Switch slot 1.
hccp 1 channel-switch 1 uc31 wavecom-hd 192.168.1.2 1 192.168.1.4 1
hccp 1 track FastEthernet0/1
!
! Tracking is enabled for the egress port in case the WAN-backhaul is disrupted. In this
instance, this cable interface would fail over to the Protect.
!
hccp 1 reverttime 120
!
! This is the time in minutes (+ 2 minute suspend) for the card to switch back to normal
mode if the fault has cleared. If a fault was initiated by a keepalive and you had a
fault on the Protect card, it would revert back after the suspend time & not wait the full
revert time.
!
interface Cable3/1
hccp 2 working 1
hccp 2 channel-switch 1 rfswl1a rfswitch-group 192.168.1.5 11110100 1
!
! This is the IP address of the Cisco RF Switch and its protecting member 1 in the right
side of Switch slot 1.
!
hccp 2 channel-switch 1 uc31 wavecom-hd 192.168.1.2 2 192.168.1.4 2
hccp 2 reverttime 120

interface Cable4/0
hccp 3 working 1
hccp 3 channel-switch 1 rfswl1b rfswitch-group 192.168.1.5 88880800 1
!
! This is the IP address of the Cisco RF Switch and its protecting member 1 in the left
side of Switch slot 5.

```

```

!
hccp 3 channel-switch 1 uc31 wavecom-hd 192.168.1.2 3 192.168.1.4 3
hccp 3 reverttime 120
!
interface Cable 4/1
hccp 4 working 1
hccp 4 channel-switch 1 rfsw1b rfswitch-group 192.168.1.5 22220200 1
!
! This is IP address of the Cisco RF Switch and its protecting member 1 in the right side of Switch slot 5.
!
hccp 4 channel-switch 1 uc31 wavecom-hd 192.168.1.2 4 192.168.1.4 4
hccp 4 reverttime 120

interface Cable5/0
hccp 5 working 1
hccp 5 channel-switch 1 rfsw2a rfswitch-group 192.168.1.6 44440400 1
hccp 5 channel-switch 1 uc31 wavecom-hd 192.168.1.2 5 192.168.1.4 5
hccp 5 reverttime 120
!
interface Cable 5/1
hccp 6 working 1
hccp 6 channel-switch 1 rfsw2a rfswitch-group 192.168.1.6 11110100 1
hccp 6 channel-switch 1 uc31 wavecom-hd 192.168.1.2 6 192.168.1.4 6
hccp 6 reverttime 120

interface Cable 6/0
hccp 7 working 1
hccp 7 channel-switch 1 rfsw2b rfswitch-group 192.168.1.6 88880800 1
hccp 7 channel-switch 1 uc31 wavecom-hd 192.168.1.2 7 192.168.1.4 7
hccp 7 reverttime 120

interface Cable 6/1
hccp 8 working 1
hccp 8 channel-switch 1 rfsw2b rfswitch-group 192.168.1.6 22220200 1
hccp 8 channel-switch 1 uc31 wavecom-hd 192.168.1.2 8 192.168.1.4 8
hccp 8 reverttime 120

router eigrp 2500
network 10.11.12.0 0.0.0.255
network 192.168.1.0
network 192.168.3.0
no auto-summary
no eigrp log-neighbor-changes
!
ip classless
ip route 0.0.0.0 0.0.0.0 192.168.1.254
ip route 192.168.1.0 255.255.255.0 FastEthernet0/0
ip route 192.168.2.0 255.255.255.0 FastEthernet0/1
no ip http server
!
cdp run
!
snmp-server community private RW
!
! This does not affect the HCCP communications between the Upconverter, Switch, and Router.
!
snmp-server community public RO
snmp-server enable traps tty
snmp-server manager
tftp-server disk0:
tftp-server disk1:
tftp-server disk1:rfsw250-fl-1935030e
tftp-server disk1:rfsw250-bf-1935022d
alias exec shb show hccp brief
alias exec shd show hccp detail
alias exec scm show cable modem
alias exec scr show cable modem remote
alias exec sm show cab modu
alias exec sch show cab hop
alias exec sc300 show cont c3/0 u0
alias exec sint300 show int c3/0 u0
alias exec scs show cable spec

```


N+1 Configuration Example on the Protect Cisco uBR7246VXR Router

```

version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname "ProtectVXR"
!
boot system disk0:ubr7200-ik8s-mz.BC.28Sept02
enable secret 5 $1$d1We$809Be9s21TGJ3IAV1X4Pa.
!
cab modem remote-query 10 public
cab modulation-prof 2 request 0 16 0 8 qpsk scrambler 152 no-diff 64 fixed uw8
cab modulation-prof 2 initial 5 34 0 48 qpsk scrambler 152 no-diff 128 fixed uw16
cab modulation-prof 2 station 5 34 0 48 qpsk scrambler 152 no-diff 128 fixed uw16
cab modulation-prof 2 short 4 76 6 8 qpsk scrambler 152 no-diff 72 short uw8
cab modulation-prof 2 long 8 220 0 8 qpsk scrambler 152 no-diff 80 short uw8
cab modulation-prof 3 request 0 16 0 8 qpsk scrambler 152 no-diff 64 fixed uw16
cab modulation-prof 3 initial 5 34 0 48 qpsk scrambler 152 no-diff 128 fixed uw16
cab modulation-prof 3 station 5 34 0 48 qpsk scrambler 152 no-diff 128 fixed uw16
cab modulation-prof 3 short 7 76 7 8 16qam scrambler 152 no-diff 144 short uw16
cab modulation-prof 3 long 9 220 0 8 16qam scrambler 152 no-diff 160 short uw16
no cable qos permission create
no cable qos permission update
cable qos permission modems
no cable clock source-midplane
no cable clock force primary
no cable clock force secondary
!
cable config-file docsis.cm
frequency 453000000
service-class 1 max-upstream 10000
service-class 1 max-downstream 10000
service-class 1 max-burst 1522
!
ip subnet-zero
ip cef
!
ip name-server 171.68.226.120
!
ip dhcp pool MODEMS1
network 192.168.3.0 255.255.255.0
bootfile docsis.cm
next-server 192.168.3.5
default-router 192.168.3.5
option 7 ip 192.168.3.5
option 4 ip 192.168.3.5
option 2 hex 0000.0000
lease 2 3 4
!
ip dhcp pool MODEMS2
network 192.168.5.0 255.255.255.0
bootfile docsis.cm
next-server 192.168.5.6
default-router 192.168.5.6
option 7 ip 192.168.5.6
option 4 ip 192.168.5.6
option 2 hex 0000.0000
lease 2 3 4
!
ip dhcp pool PC2
network 10.11.13.0 255.255.255.0
default-router 10.11.13.1
dns-server 171.68.226.120
lease 10 1 11
!
ip dhcp pool PC1
network 10.11.12.0 255.255.255.0
default-router 10.11.12.1
dns-server 171.68.226.120
lease 10 1 11
!
packetcable element_id 35417
!
interface FastEthernet0/0
ip address 192.168.1.11 255.255.255.0
no keepalive

```

```

speed auto
full-duplex
no cdp enable
!
interface FastEthernet0/1
ip address 192.168.2.11 255.255.255.0
keepalive 1
speed auto
full-duplex
no cdp enable
!
interface Cable3/0
no ip address
!
! There is no need to set the IP address because it'll come from the Working card via
SNMP.
!
no keepalive
! This is set by default to 10 seconds with the N+1 IOS code, but recommended to be
disabled on the Protect interface or set relatively high.
!
cable downstream annex B
cable downstream modulation 64qam
cable downstream interleave-depth 32
!
! The DS modulation and Interleave must be same on the Protect and Working of the same
group.
!
no shut
!
! The interface must be activated to start HCCP functionality. Do this last.
!
cable upstream 0 shutdown
!
! This will automatically become "no shutdown" (enabled) when a failover occurs.
!
hccp 1 protect 1 192.168.1.7
!
! This is the Protect for the first group. Remember to configure the Protect interface(s)
last; after the Working interfaces are configured. This is the HCCP first group and it's
protecting member 1 with member one's FE IP address.
!
hccp 1 channel-switch 1 rfsw1a rfswitch-group 192.168.1.5 44440400 1
!
! This is the IP address of the Switch and it's protecting member 1, which has a bitmap of
AA880800 in Switch slot 5.
!
hccp 1 channel-switch 1 uc31 wavecom-hd 192.168.1.2 1 192.168.1.4 1
!
! This is the IP address of upconverter and its module 1 (A) that is backing module 16 (P)
of the upconverter. This shows that one upconverter could have a module backing up a
module in a different chassis with a different IP address if need be.
!
hccp 1 protect 2 192.168.1.8
!
! This is the HCCP first group and it's protecting member 2 with its IP address.
!
hccp 1 channel-switch 2 rfsw1a rfswitch-group 192.168.1.5 44440400 2
hccp 1 channel-switch 2 uc31 wavecom-hd 192.168.1.2 1 192.168.1.4 9
hccp 1 protect 3 192.168.1.9
hccp 1 channel-switch 3 rfsw1a rfswitch-group 192.168.1.5 44440400 3
hccp 1 channel-switch 3 uc32 wavecom-hd 192.168.1.2 1 192.168.1.3 1
hccp 1 protect 4 192.168.1.10
hccp 1 channel-switch 4 rfsw1a rfswitch-group 192.168.1.5 44440400 4
hccp 1 channel-switch 4 uc32 wavecom-hd 192.168.1.2 1 192.168.1.3 9
hccp 1 timers 666 2000
hccp 1 timers <hellotime> <holdtime> This is for inter-chassis communication.
!
interface Cable3/1

hccp 2 protect 1 192.168.1.7
hccp 2 channel-switch 1 rfsw1a rfswitch-group 192.168.1.5 11110100 1
hccp 2 channel-switch 1 uc31 wavecom-hd 192.168.1.2 2 192.168.1.4 2
hccp 2 protect 2 192.168.1.8
hccp 2 channel-switch 2 rfsw1a rfswitch-group 192.168.1.5 11110100 2
hccp 2 channel-switch 2 uc31 wavecom-hd 192.168.1.2 2 192.168.1.4 10
hccp 2 protect 3 192.168.1.9
hccp 2 channel-switch 3 rfsw1a rfswitch-group 192.168.1.5 11110100 3
hccp 2 channel-switch 3 uc32 wavecom-hd 192.168.1.2 2 192.168.1.3 2

```

```
hccp 2 protect 4 192.168.1.10
hccp 2 channel-switch 4 rfswl1a rfswitch-group 192.168.1.5 11110100 4
hccp 2 channel-switch 4 uc32 wavecom-hd 192.168.1.2 2 192.168.1.3 10
hccp 2 timers 666 2000

interface Cable4/0

hccp 3 protect 1 192.168.1.7
hccp 3 channel-switch 1 rfswl1b rfswitch-group 192.168.1.5 88880800 1
hccp 3 channel-switch 1 uc31 wavecom-hd 192.168.1.2 3 192.168.1.4 3
hccp 3 protect 2 192.168.1.8
hccp 3 channel-switch 2 rfswl1b rfswitch-group 192.168.1.5 88880800 2
hccp 3 channel-switch 2 uc31 wavecom-hd 192.168.1.2 3 192.168.1.4 11
hccp 3 protect 3 192.168.1.9
hccp 3 channel-switch 3 rfswl1b rfswitch-group 192.168.1.5 88880800 3
hccp 3 channel-switch 3 uc32 wavecom-hd 192.168.1.2 3 192.168.1.3 3
hccp 3 protect 4 192.168.1.10
hccp 3 channel-switch 4 rfswl1b rfswitch-group 192.168.1.5 88880800 4
hccp 3 channel-switch 4 uc32 wavecom-hd 192.168.1.2 3 192.168.1.3 11
hccp 3 timers 666 2000

interface Cable4/1

hccp 4 protect 1 192.168.1.7
hccp 4 channel-switch 1 rfswl1b rfswitch-group 192.168.1.5 22220200 1
hccp 4 channel-switch 1 uc31 wavecom-hd 192.168.1.2 4 192.168.1.4 4
hccp 4 protect 2 192.168.1.8
hccp 4 channel-switch 2 rfswl1b rfswitch-group 192.168.1.5 22220200 2
hccp 4 channel-switch 2 uc31 wavecom-hd 192.168.1.2 4 192.168.1.4 12
hccp 4 protect 3 192.168.1.9
hccp 4 channel-switch 3 rfswl1b rfswitch-group 192.168.1.5 22220200 3
hccp 4 channel-switch 3 uc32 wavecom-hd 192.168.1.2 4 192.168.1.3 4
hccp 4 protect 4 192.168.1.10
hccp 4 channel-switch 4 rfswl1b rfswitch-group 192.168.1.5 22220200 4
hccp 4 channel-switch 4 uc32 wavecom-hd 192.168.1.2 4 192.168.1.3 12
hccp 4 timers 666 2000

interface Cable5/0

hccp 5 protect 1 192.168.1.7
hccp 5 channel-switch 1 rfsw2a rfswitch-group 192.168.1.6 44440400 1
hccp 5 channel-switch 1 uc31 wavecom-hd 192.168.1.2 5 192.168.1.4 5
hccp 5 protect 2 192.168.1.8
hccp 5 channel-switch 2 rfsw2a rfswitch-group 192.168.1.6 44440400 2
hccp 5 channel-switch 2 uc31 wavecom-hd 192.168.1.2 5 192.168.1.4 13
hccp 5 protect 3 192.168.1.9
hccp 5 channel-switch 3 rfsw2a rfswitch-group 192.168.1.6 44440400 3
hccp 5 channel-switch 3 uc32 wavecom-hd 192.168.1.2 5 192.168.1.3 5
hccp 5 protect 4 192.168.1.10
hccp 5 channel-switch 4 rfsw2a rfswitch-group 192.168.1.6 44440400 4
hccp 5 channel-switch 4 uc32 wavecom-hd 192.168.1.2 5 192.168.1.3 13
hccp 5 timers 666 2000

interface Cable5/1

hccp 6 protect 1 192.168.1.7
hccp 6 channel-switch 1 rfsw2a rfswitch-group 192.168.1.6 11110100 1
hccp 6 channel-switch 1 uc31 wavecom-hd 192.168.1.2 6 192.168.1.4 6
hccp 6 protect 2 192.168.1.8
hccp 6 channel-switch 2 rfsw2a rfswitch-group 192.168.1.6 11110100 2
hccp 6 channel-switch 2 uc31 wavecom-hd 192.168.1.2 6 192.168.1.4 14
hccp 6 protect 3 192.168.1.9
hccp 6 channel-switch 3 rfsw2a rfswitch-group 192.168.1.6 11110100 3
hccp 6 channel-switch 3 uc32 wavecom-hd 192.168.1.2 6 192.168.1.3 6
hccp 6 protect 4 192.168.1.10
hccp 6 channel-switch 4 rfsw2a rfswitch-group 192.168.1.6 11110100 4
hccp 6 channel-switch 4 uc32 wavecom-hd 192.168.1.2 6 192.168.1.3 14
hccp 6 timers 666 2000

interface Cable6/0

hccp 7 protect 1 192.168.1.7
hccp 7 channel-switch 1 rfsw2b rfswitch-group 192.168.1.6 88880800 1
hccp 7 channel-switch 1 uc31 wavecom-hd 192.168.1.2 7 192.168.1.4 7
hccp 7 protect 2 192.168.1.8
hccp 7 channel-switch 2 rfsw2b rfswitch-group 192.168.1.6 88880800 2
hccp 7 channel-switch 2 uc31 wavecom-hd 192.168.1.2 7 192.168.1.4 15
hccp 7 protect 3 192.168.1.9
hccp 7 channel-switch 3 rfsw2b rfswitch-group 192.168.1.6 88880800 3
```

```

hccp 7 channel-switch 3 uc32 wavecom-hd 192.168.1.2 7 192.168.1.3 7
hccp 7 protect 4 192.168.1.10
hccp 7 channel-switch 4 rfsw2b rfswitch-group 192.168.1.6 88880800 4
hccp 7 channel-switch 4 uc32 wavecom-hd 192.168.1.2 7 192.168.1.3 15
hccp 7 timers 666 2000

interface Cable6/1

hccp 8 protect 1 192.168.1.7
hccp 8 channel-switch 1 rfsw2b rfswitch-group 192.168.1.6 22220200 1
hccp 8 channel-switch 1 uc31 wavecom-hd 192.168.1.2 8 192.168.1.4 8
hccp 8 protect 2 192.168.1.8
hccp 8 channel-switch 2 rfsw2b rfswitch-group 192.168.1.6 22220200 2
hccp 8 channel-switch 2 uc31 wavecom-hd 192.168.1.2 8 192.168.1.4 16
hccp 8 protect 3 192.168.1.9
hccp 8 channel-switch 3 rfsw2b rfswitch-group 192.168.1.6 22220200 3
hccp 8 channel-switch 3 uc32 wavecom-hd 192.168.1.2 8 192.168.1.3 8
hccp 8 protect 4 192.168.1.10
hccp 8 channel-switch 4 rfsw2b rfswitch-group 192.168.1.6 22220200 4
hccp 8 channel-switch 4 uc32 wavecom-hd 192.168.1.2 8 192.168.1.3 16
hccp 8 timers 666 2000

router eigrp 2500
network 10.11.12.0 0.0.0.255
network 10.11.13.0 0.0.0.255
network 192.168.1.0
network 192.168.3.0
network 192.168.5.0
no auto-summary
no eigrp log-neighbor-changes
!
ip classless
ip route 0.0.0.0 0.0.0.0 192.168.1.254
ip route 192.168.1.0 255.255.255.0 FastEthernet0/0
ip route 192.168.2.0 255.255.255.0 FastEthernet0/1
no ip http server
!
cdp run
!
snmp-server community private RW
snmp-server community public RO
snmp-server enable traps tty
snmp-server enable traps cable
snmp-server manager
alias exec shb show hccp brief
alias exec shd show hccp detail
alias exec scm show cable modem
alias exec scr show cable modem remote
alias exec sm show cab modu
alias exec sch show cab hop
alias exec sc300 show cont c3/0 u0
alias exec sint300 show int c3/0 u0
alias exec scs show cable spec

```

Examples: Cisco 3x10 RF Switch with Cisco uBR10012 Chassis

The following output from the Cisco IOS **show running configuration** command illustrates the configuration of N+1 Redundancy using the following CMTS:

- One Cisco 3x10 RF Switch configured as two Working RF Switches in 4+1 mode
- One Cisco uBR10012 router
- Five Cisco UBR10-MC 5X20U or -S/D broadband processing engines (BPEs)

The Protection mode affects the bitmaps of the Cisco RF Switch and CMTS configuration.

**Note**

If you add one additional Cisco UBR10-MC 5X20U or -S/D BPE, the entire CMTS configuration below must be changed. Refer to the cabling in the following document for additional information:

- *Cabling the Cisco UBR10-MC 5X20U or -S/D Cable Interface Line Card*
http://www.cisco.com/univercd/cc/td/doc/product/cable/ubr10k/ubr10012/qsg/mc52_cbl.pdf

Summary Steps For This Configuration

1. Take the header that says RF Switch 2 (top Switch) and leave in slots 1, 2, 3, & 4.
2. Take the header that says RF Switch 1 and place in slots 5, 6, 7, & 8 of RF Switch 2.
3. Take the Protect from RF Switch 2 and put in Protect 2.
4. Take the Protect from RF Switch 1 and place in Protect 1 of RF Switch 2.
5. Once you get to five UBR10-MC 5X20U or -S/D BPEs, the bitmap configuration needs to be changed and the headers moved around from one Cisco RF Switch to the other. For example, the slot 5 header moves to the slot 1 header of Cisco RF Switch 1.

Additional Configuration Notes

- The configuration is labeled “`rfswa`” as pertaining to slots 1-4 and their respective Protect slot, which is Protect 2.
- Protect 1 covers slots 5-8 on the Cisco RF Switch and is labeled as “`rfswb`.” In the 4+1 mode the RF Switch slots 5-8 are considered to be slots 1-4 for configuration purposes.
- These configurations are for MAC interface switchovers. Bear in mind that the entire JIB (ASIC) switches over when circumstances require. DS channels 0 and 1 share the same ASIC, DS channels 2 and 3 share the same ASIC, and DS channel 4 is on its own ASIC. If an interface does not have HCCP configured, it will not switch over even if it does share the same JIB with an HCCP interface.
- If using the **keepalive** command on HCCP interfaces that share a common ASIC, Cisco recommends that you configure **no hccp g revertive** on the respective Protect interfaces. For additional information, refer to the topic [Disabling HCCP Revertive on Protect Cable Interfaces](#), page 224.

HCCP Working 1 Example

The following configuration example illustrates HCCP Working member 1 for five HCCP groups:

```
interface c8/0/0
hccp 1 working 1
hccp 1 channel-switch 1 rfsa rswitch-group 10.10.10.10 44440400 1

interface c8/0/1
hccp 2 working 1
hccp 2 channel-switch 1 rfsa rswitch-group 10.10.10.10 11110100 1

interface c8/0/2
hccp 3 working 1
hccp 3 channel-switch 1 rfsa rswitch-group 10.10.10.10 00005000 1
hccp 3 channel-switch 1 rfsb rswitch-group 10.10.10.10 0000a080 1

interface c8/0/3
hccp 4 working 1
hccp 4 channel-switch 1 rfsb rswitch-group 10.10.10.10 88880800 1

interface c8/0/4
hccp 5 working 1
hccp 5 channel-switch 1 rfsb rswitch-group 10.10.10.10 22220200 1
```

HCCP Working 2 Example

The following configuration example illustrates HCCP Working member 2 for five HCCP groups:

```
interface c8/1/0
hccp 1 working 2
hccp 1 channel-switch 2 rfsa rswitch-group 10.10.10.10 44440400 2

interface c8/1/1
hccp 2 working 2
hccp 2 channel-switch 2 rfsa rswitch-group 10.10.10.10 11110100 2

interface c8/1/2
hccp 3 working 2
hccp 3 channel-switch 2 rfsa rswitch-group 10.10.10.10 00005000 2
hccp 3 channel-switch 2 rfsb rswitch-group 10.10.10.10 0000a080 2

interface c8/1/3
hccp 4 working 2
hccp 4 channel-switch 2 rfsb rswitch-group 10.10.10.10 88880800 2

interface c8/1/4
hccp 5 working 2
hccp 5 channel-switch 2 rfsb rswitch-group 10.10.10.10 22220200 2
```

HCCP Working 3 Example

The following configuration example illustrates HCCP Working member 3 for five HCCP groups:

```
interface c7/0/0
 hccp 1 working 3
 hccp 1 channel-switch 3 rfsa rfswitch-group 10.10.10.10 44440400 3

interface c7/0/1
 hccp 2 working 3
 hccp 2 channel-switch 3 rfsa rfswitch-group 10.10.10.10 11110100 3

interface c7/0/2
 hccp 3 working 3
 hccp 3 channel-switch 3 rfsa rfswitch-group 10.10.10.10 00005000 3
 hccp 3 channel-switch 3 rfsb rfswitch-group 10.10.10.10 0000a080 3

interface c7/0/3
 hccp 4 working 3
 hccp 4 channel-switch 3 rfsb rfswitch-group 10.10.10.10 88880800 3

interface c7/0/4
 hccp 5 working 3
 hccp 5 channel-switch 3 rfsb rfswitch-group 10.10.10.10 22220200 3
```

HCCP Working 4 Example

The following configuration example illustrates HCCP Working member 4 for five HCCP groups:

```
interface c7/1/0
 hccp 1 working 4
 hccp 1 channel-switch 4 rfsa rfswitch-group 10.10.10.10 44440400 4

interface c7/1/1
 hccp 2 working 4
 hccp 2 channel-switch 4 rfsa rfswitch-group 10.10.10.10 11110100 4

interface c7/1/2
 hccp 3 working 4
 hccp 3 channel-switch 4 rfsa rfswitch-group 10.10.10.10 00005000 4
 hccp 3 channel-switch 4 rfsb rfswitch-group 10.10.10.10 0000a080 4

interface c7/1/3
 hccp 4 working 4
 hccp 4 channel-switch 4 rfsb rfswitch-group 10.10.10.10 88880800 4

interface c7/1/4
 hccp 5 working 4
```

HCCP Protect Interface Configuration Examples

The following examples illustrate the four HCCP Protect members for five HCCP groups:

```

interface c5/1/0
hccp 1 protect 1 10.10.10.1
hccp 1 channel-switch 1 rfsa rfsa-switch-group 10.10.10.10 44440400 1
hccp 1 protect 2 10.10.10.1
hccp 1 channel-switch 2 rfsa rfsa-switch-group 10.10.10.10 44440400 2
hccp 1 protect 3 10.10.10.1
hccp 1 channel-switch 3 rfsa rfsa-switch-group 10.10.10.10 44440400 3
hccp 1 protect 4 10.10.10.1
hccp 1 channel-switch 4 rfsa rfsa-switch-group 10.10.10.10 44440400 4

interface c5/1/1
hccp 2 protect 1 10.10.10.1
hccp 2 channel-switch 1 rfsa rfsa-switch-group 10.10.10.10 11110100 1
hccp 2 protect 2 10.10.10.1
hccp 2 channel-switch 2 rfsa rfsa-switch-group 10.10.10.10 11110100 2
hccp 2 protect 3 10.10.10.1
hccp 2 channel-switch 3 rfsa rfsa-switch-group 10.10.10.10 11110100 3
hccp 2 protect 4 10.10.10.1
hccp 2 channel-switch 4 rfsa rfsa-switch-group 10.10.10.10 11110100 4

interface c5/1/2
hccp 3 protect 1 10.10.10.1
hccp 3 channel-switch 1 rfsa rfsa-switch-group 10.10.10.10 00005000 1
hccp 3 channel-switch 1 rfsb rfsa-switch-group 10.10.10.10 0000a080 1
hccp 3 protect 2 10.10.10.1
hccp 3 channel-switch 2 rfsa rfsa-switch-group 10.10.10.10 00005000 2
hccp 3 channel-switch 2 rfsb rfsa-switch-group 10.10.10.10 0000a080 2
hccp 3 protect 3 10.10.10.1
hccp 3 channel-switch 3 rfsa rfsa-switch-group 10.10.10.10 00005000 3
hccp 3 channel-switch 3 rfsb rfsa-switch-group 10.10.10.10 0000a080 3
hccp 3 protect 4 10.10.10.1
hccp 3 channel-switch 4 rfsa rfsa-switch-group 10.10.10.10 00005000 4
hccp 3 channel-switch 4 rfsb rfsa-switch-group 10.10.10.10 0000a080 4

interface c5/1/3
hccp 4 protect 1 10.10.10.1
hccp 4 channel-switch 1 rfsb rfsa-switch-group 10.10.10.10 88880800 1
hccp 4 protect 2 10.10.10.1
hccp 4 channel-switch 2 rfsb rfsa-switch-group 10.10.10.10 88880800 2
hccp 4 protect 3 10.10.10.1
hccp 4 channel-switch 3 rfsb rfsa-switch-group 10.10.10.10 88880800 3
hccp 4 protect 4 10.10.10.1
hccp 4 channel-switch 4 rfsb rfsa-switch-group 10.10.10.10 88880800 4

interface c5/1/4
hccp 5 protect 1 10.10.10.1
hccp 5 channel-switch 1 rfsb rfsa-switch-group 10.10.10.10 22220200 1
hccp 5 protect 2 10.10.10.1
hccp 5 channel-switch 2 rfsb rfsa-switch-group 10.10.10.10 22220200 2
hccp 5 protect 3 10.10.10.1
hccp 5 channel-switch 3 rfsb rfsa-switch-group 10.10.10.10 22220200 3
hccp 5 protect 4 10.10.10.1
hccp 5 channel-switch 4 rfsb rfsa-switch-group 10.10.10.10 22220200 4

```


Example: Channel Switch Information from the Cisco uBR10012 Router

The following output from the **show hccp channel-switch** command illustrates typical information about the current channel switch activity on a Cisco uBR10012 router configured with a Cisco 3x10 RF Switch.

```
Router# show hccp channel-switch

Grp 1 Mbr 1 Working channel-switch:
  "uc" - enabled, frequency 555000000 Hz
  "rfswitch" - module 1, normal
  module 3, normal
  module 5, normal
  module 7, normal
  module 11, normal
Grp 2 Mbr 1 Working channel-switch:
  "uc" - enabled, frequency 555000000 Hz
  "rfswitch" - module 2, normal
  module 4, normal
  module 6, normal
  module 9, normal
  module 13, normal
Grp 1 Mbr 7 Protect channel-switch:
  "uc" - disabled, frequency 555000000 Hz
  "rfswitch" - module 1, normal
  module 3, normal
  module 5, normal
  module 7, normal
  module 11, normal
Grp 1 Mbr 5 Protect channel-switch:
  "uc" - disabled, frequency 555000000 Hz
  "rfswitch" - module 1, normal
  module 3, normal
  module 5, normal
  module 7, normal
  module 11, normal
```

Example: Cisco 3x10 RF Switch and Cisco uBR10012 Chassis



Note

This is the N+1 Redundancy configuration commonly cited in this document for Cisco 3x10 RF Switch examples (there are exceptions).

The following output from the **show run** command illustrates the configuration of N+1 Redundancy using the following CMTS:

- One Cisco 3x10 RF Switch in 8+1 mode
- One Cisco uBR10012 router
- Eight Cisco uBR10-LCP2-MC28C broadband processing engines (BPEs)

Router# **show run**

```
Current configuration : 8567 bytes
!
version 12.2
no parser cache
no service single-slot-reload-enable
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname uBR10k
!
boot system flash slot0: ubr10k-k8p6-mz.122-4.BC1b
logging rate-limit console all 10 except critical
enable secret 5 $1$.Dvy$fcPOhshUNjyfePH73FHRG.
!
no cable qos permission create
no cable qos permission update
cable qos permission modems
cable time-server
!
cable config-file docsis.cm
frequency 453000000
service-class 1 max-upstream 10000
service-class 1 max-downstream 10000
service-class 1 max-burst 1522
!
redundancy
main-cpu
auto-sync standard
facility-alarm intake-temperature major 49
facility-alarm intake-temperature minor 40
facility-alarm core-temperature major 53
facility-alarm core-temperature minor 45
card 1/0 1gigetherne-1
card 1/1 2cable-tccplus
card 2/0 1gigetherne-1
card 2/1 2cable-tccplus
card 5/0 2cable-mc28c
card 5/1 2cable-mc28c
card 6/0 2cable-mc28c
card 6/1 2cable-mc28c
card 7/0 2cable-mc28c
card 7/1 2cable-mc28c
card 8/0 2cable-mc28c
card 8/1 2cable-mc28c
ip subnet-zero
ip host rfswitch 2001 10.10.10.1
!
! This is set for console access from the uBR10012 router to the RF Switch.
! The IP address is for Loopback0.
!
```

```

ip dhcp pool MODEMS1
  network 172.25.1.0 255.255.255.0
  bootfile docsis.cm
  next-server 172.25.1.1
  default-router 172.25.1.1
  option 7 ip 172.25.1.1
  option 4 ip 172.25.1.1
  option 2 hex 0000.0000
  lease 2 3 4
!
ip dhcp pool MODEMS2
  network 172.25.2.0 255.255.255.0
  bootfile docsis.cm
  next-server 172.25.2.1
  default-router 172.25.2.1
  option 7 ip 172.25.2.1
  option 4 ip 172.25.2.1
  option 2 hex 0000.0000
  lease 2 3 4
!
ip dhcp-client network-discovery informs 2 discovers 2 period 15
!
! An internal DHCP server was used for testing in this example instead of external
! servers (cable helper, TOD, TFTP, etc.). External servers are recommended in a
! genuine production network.
!
interface Loopback0
  ip address 10.10.10.1 255.255.255.252
!
interface FastEthernet0/0/0
  ip address 10.97.1.8 255.255.255.0
  ip rip receive version 2
  no ip split-horizon
  no keepalive
!
interface GigabitEthernet1/0/0
  no ip address
  negotiation auto
!
interface GigabitEthernet2/0/0
  no ip address
  negotiation auto
!
interface Cable5/1/0
!
! This is the Protect interface for the first group. Remember to configure the
! Protect interface(s) last; after the Working interfaces are configured.
!
  no ip address
!
! There is no need to set the IP address because it comes from the Working card via SNMP.
!
  no keepalive
!
! This is set by default to 10 seconds with the N+1 IOS code, but should be disabled
! on the Protect interface or set to be relatively high.
!
  cable downstream annex B
  cable downstream modulation 64qam
  cable downstream interleave-depth 32
!
! The DS modulation and Interleave depth must be same on Protect and Working interfaces
! of the same group.
!
  cable upstream 0 shutdown
!
! This automatically becomes "no shut" (enabled) when a switchover occurs.
!
  cable upstream 1 shutdown
  cable upstream 2 shutdown
  cable upstream 3 shutdown
  cable dhcp-giaddr policy
  hccp 1 protect 1 10.10.10.1
!
! This is the HCCP first group and it is protecting member 1 with member 1's
! FE IP address. If it's intra-chassis, you can use the Loopback0 IP address.
!

```

```

hccp 1 channel-switch 1 uc wavecom-hd 10.97.1.21 2 10.97.1.21 16
!
! This is the IP address of upconverter and its module 2 (B) that is backing
! module 16 (P) of the upconverter. This shows that one upconverter could have
! a module backing up a module in a different chassis with a different IP address
! if need be. If this statement is not present when using 15BC2 IOS and above,
! IF-Muting is assumed and an external upconverter with snmp capability is not needed.
!
hccp 1 channel-switch 1 rfswitch rfswitch-group 10.97.1.20 AA200000 1
!
! This is the IP address of the Switch and it is protecting member 1, which has a
! bitmap of AA200000 in Switch slot 1.
!
hccp 1 protect 2 10.10.10.1
!
! This is the HCCP first group and it is protecting member 2 with its IP address.
!
hccp 1 channel-switch 2 uc wavecom-hd 10.97.1.21 2 10.97.1.21 14
!
! This is the IP address of the upconverter and its module 2 (B) that's backing
! module 14 (N).
!
hccp 1 channel-switch 2 rfswitch rfswitch-group 10.97.1.20 AA200000 2
!
! This is the IP address of the Switch and it is protecting member 2, with a
! bitmap of AA200000 in Switch slot 2.
!
hccp 1 protect 3 10.10.10.1
hccp 1 channel-switch 3 uc wavecom-hd 10.97.1.21 2 10.97.1.21 12
hccp 1 channel-switch 3 rfswitch rfswitch-group 10.97.1.20 AA200000 3
hccp 1 protect 4 10.10.10.1
hccp 1 channel-switch 4 uc wavecom-hd 10.97.1.21 2 10.97.1.21 10
hccp 1 channel-switch 4 rfswitch rfswitch-group 10.97.1.20 AA200000 4
hccp 1 protect 5 10.10.10.1
hccp 1 channel-switch 5 uc wavecom-hd 10.97.1.21 2 10.97.1.21 8
hccp 1 channel-switch 5 rfswitch rfswitch-group 10.97.1.20 AA200000 5
hccp 1 protect 6 10.10.10.1
hccp 1 channel-switch 6 uc wavecom-hd 10.97.1.21 2 10.97.1.21 6
hccp 1 channel-switch 6 rfswitch rfswitch-group 10.97.1.20 AA200000 6
hccp 1 protect 7 10.10.10.1
hccp 1 channel-switch 7 uc wavecom-hd 10.97.1.21 2 10.97.1.21 4
hccp 1 channel-switch 7 rfswitch rfswitch-group 10.97.1.20 AA200000 7
hccp 1 timers 5000 15000
!
! Cisco IOS command = hccp 1 timers <hellotime> <holdtime>
! This is mostly for inter-chassis communication, so set it high for the uBR10012 router
! as this can create extra CPU load.
!
interface Cable5/1/1
!
! This is the Protect interface for the second group.
!
no ip address
no keepalive
cable downstream annex B
cable downstream modulation 64qam
cable downstream interleave-depth 32
cable upstream 0 shutdown
cable upstream 1 shutdown
cable upstream 2 shutdown
cable upstream 3 shutdown
cable dhcp-giaddr policy
!
hccp 2 protect 1 10.10.10.1
hccp 2 channel-switch 1 uc wavecom-hd 10.97.1.21 1 10.97.1.21 15
hccp 2 channel-switch 1 rfswitch rfswitch-group 10.97.1.20 55100000 1
!
! Because this MAC domain is on right side of header, the bitmap in hexadecimal code
! is 55100000.
!
hccp 2 protect 2 10.10.10.1
hccp 2 channel-switch 2 uc wavecom-hd 10.97.1.21 1 10.97.1.21 13
hccp 2 channel-switch 2 rfswitch rfswitch-group 10.97.1.20 55100000 2
hccp 2 protect 3 10.10.10.1
hccp 2 channel-switch 3 uc wavecom-hd 10.97.1.21 1 10.97.1.21 11

```

```

hccp 2 channel-switch 3 rfswitch rfswitch-group 10.97.1.20 55100000 3
hccp 2 protect 4 10.10.10.1
hccp 2 channel-switch 4 uc wavecom-hd 10.97.1.21 1 10.97.1.21 9
hccp 2 channel-switch 4 rfswitch rfswitch-group 10.97.1.20 55100000 4
hccp 2 protect 5 10.10.10.1
hccp 2 channel-switch 5 uc wavecom-hd 10.97.1.21 1 10.97.1.21 7
hccp 2 channel-switch 5 rfswitch rfswitch-group 10.97.1.20 55100000 5
hccp 2 protect 6 10.10.10.1
hccp 2 channel-switch 6 uc wavecom-hd 10.97.1.21 1 10.97.1.21 5
hccp 2 channel-switch 6 rfswitch rfswitch-group 10.97.1.20 55100000 6
hccp 2 protect 7 10.10.10.1
hccp 2 channel-switch 7 uc wavecom-hd 10.97.1.21 1 10.97.1.21 3
hccp 2 channel-switch 7 rfswitch rfswitch-group 10.97.1.20 55100000 7
hccp 2 timers 5000 15000
!
interface Cable8/1/0
!
!   This is the Working interface for the first group.
!
ip address 10.192.5.1 255.255.255.0 secondary
ip address 172.25.1.1 255.255.255.0
!
!   Interface bundling is supported also as well as subinterfaces.
!
ip rip send version 2
ip rip receive version 2
keepalive 1
!
!   The keepalive time is in seconds and the default is 10 seconds for HCCP code.
!
cable downstream annex B
cable downstream modulation 64qam
cable downstream interleave-depth 32
cable downstream frequency 453000000
!
!   This is DS frequency, which used to be informational only when using an external
!   upconverter. This must be set when doing N+1, so the Protect upconverter knows
!   which frequency to use.
!
cable upstream 0 frequency 24000000
!
!   If doing dense mode combining, the upstream frequencies need to be different.
!   If no two US ports are shared, the same frequency can be used.
!
cable upstream 0 power-level 0
no cable upstream 0 shutdown
cable upstream 1 power-level 0
cable upstream 1 shutdown
cable upstream 2 power-level 0
cable upstream 2 shutdown
cable upstream 3 power-level 0
cable upstream 3 shutdown
cable dhcp-giaddr policy
!
!   This tells cable modems to get an IP address from the primary scope and CPES
!   to use the secondary scope.
!
hccp 1 working 1
!
!   This is Working member 1 of HCCP Group 1.
!
hccp 1 channel-switch 1 uc wavecom-hd 10.97.1.21 2 10.97.1.21 16
!
!   This is the IP address of the upconverter and its module 2 (B) that's backing
!   module 16 (P).
!
hccp 1 channel-switch 1 rfswitch rfswitch-group 10.97.1.20 AA200000 1
!
!   This is the IP address of the Switch & member 1, which has a bitmap of
!   AA200000 in Switch slot 1.
!
hccp 1 reverttime 120
!
!   This is the time in minutes (+ 2 minute suspend) for the card to switch back to
!   normal mode if the fault has cleared. If a fault was initiated by a keepalive

```

```

! and you had a fault on the Protect card, it would revert back after the suspend
! time and not await the full revert time.
!
interface Cable8/1/1
!
! This is the Working interface for the second HCCP group.
!
ip address 10.192.5.1 255.255.255.0 secondary
ip address 172.25.2.1 255.255.255.0
ip rip send version 2
ip rip receive version 2
keepalive 1
cable downstream annex B
cable downstream modulation 64qam
cable downstream interleave-depth 32
cable downstream frequency 453000000
cable upstream 0 frequency 24000000
cable upstream 0 power-level 0
no cable upstream 0 shutdown
cable upstream 1 power-level 0
cable upstream 1 shutdown
cable upstream 2 power-level 0
cable upstream 2 shutdown
cable upstream 3 power-level 0
cable upstream 3 shutdown
cable dhcp-giaddr policy
hccp 2 working 1
!
! This is Working member 1 of HCCP Group 2.
!
hccp 2 channel-switch 1 uc wavecom-hd 10.97.1.21 1 10.97.1.21 15
hccp 2 channel-switch 1 rfswitch rfswitch-group 10.97.1.20 55100000 1
!
! This is the IP address of the Switch & Member 1 of Group 2, which has a bitmap of
! 55100000 in Switch slot 1.
!
hccp 2 reverttime 120
!
ip classless
no ip http server
!
no cdp run
snmp-server community private RW
!
! This does not affect the HCCP communications between the Upconverter, Switch,
! the and uBR10012.
!
snmp-server enable traps cable
no cdp run
snmp-server manager
tftp-server server
tftp-server ios.cf alias ios.cf
!
line con 0
logging synchronous
line aux 0
no exec
transport input all
!
! The three lines above were used to console from the Auxiliary port of the uBR10012
! to the Switch.
!
line vty 0 4
session-timeout 400
password xx
login
endBuilding configuration...

```

Example: Cisco 3x10 RF Switches and Cisco uBR10012 Chassis

The following output from the **show run** command illustrates the configuration of N+1 Redundancy using the following CMTS:

- Two Cisco RF Switches, each in 8+1 mode
- Cisco uBR10012 router
- Cisco UBR10-MC 5X20U or -S/D broadband processing engines (BPEs)

Router# **show run**

```
Current configuration : 8567 bytes
!
version 12.2
no parser cache
no service single-slot-reload-enable
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname uBR10k
!
boot system flash slot0: ubr10k-k8p6-mz.122-15.BC1
logging rate-limit console all 10 except critical
enable secret 5 $1$.Dvy$fcPOhshUNjyfePH73FHRG
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
!
! Use this modulation profile if using current released BC3 IOS and 16-QAM is required.
! A-TDMA IOS has different modulation profiles and requirements.
!
no cable qos permission create
no cable qos permission update
cable qos permission modems
cable time-server
!
cable config-file docsis.cm
frequency 453000000
service-class 1 max-upstream 10000
service-class 1 max-downstream 10000
service-class 1 max-burst 1522
!
redundancy
main-cpu
auto-sync standard
facility-alarm intake-temperature major 49
facility-alarm intake-temperature minor 40
facility-alarm core-temperature major 53
facility-alarm core-temperature minor 45
card 1/0 1gigetherne-1
card 1/1 2cable-tccplus
card 2/0 1gigetherne-1
card 2/1 2cable-tccplus
card 5/0 5cable-mc520s-d
card 5/1 5cable-mc520s-d
card 6/0 5cable-mc520s-d
card 6/1 5cable-mc520s-d
card 7/0 5cable-mc520s-d
card 7/1 5cable-mc520s-d
card 8/0 5cable-mc520s-d
card 8/1 5cable-mc520s-d
ip subnet-zero
ip host rfswitch 2001 10.10.10.1
!
! This is set for console access from the 10012 router to the Switch.
! The IP address is for Loopback0.
!
ip dhcp pool MODEMS1
network 172.25.1.0 255.255.255.0
bootfile docsis.cm
```

```

next-server 172.25.1.1
default-router 172.25.1.1
option 7 ip 172.25.1.1
option 4 ip 172.25.1.1
option 2 hex 0000.0000
lease 2 3 4
!
ip dhcp pool MODEMS2
network 172.25.2.0 255.255.255.0
bootfile docsis.cm
next-server 172.25.2.1
default-router 172.25.2.1
option 7 ip 172.25.2.1
option 4 ip 172.25.2.1
option 2 hex 0000.0000
lease 2 3 4
!
ip dhcp-client network-discovery informs 2 discovers 2 period 15
!
! An internal DHCP server is used in this example instead of external servers
! (cable helper, TOD, TFTP, etc.). External servers are recommended in a genuine
! production network.
!
interface Loopback0
ip address 10.10.10.1 255.255.255.252
!
interface FastEthernet0/0/0
ip address 10.97.1.8 255.255.255.0
ip rip receive version 2
no ip split-horizon
no keepalive
!
interface GigabitEthernet1/0/0
no ip address
negotiation auto
!
interface GigabitEthernet2/0/0
no ip address
negotiation auto
!
! Sample Interface Config for N+1: (This assumes rfsw2 is on the top as shown in
! the RF Switch Cabling document). Other interfaces will be the same except a
! different member number for each HCCP group.
!
interface Cable5/1/0
!
! This is the Protect interface for the first HCCP group. It may be best to configure
! the Protect interface(s) last; after the Working interfaces are configured,
! or to keep the interface "shut" (disabled) until all configurations are completed.
!
no ip address
!
! There is no need to set the IP address because it comes from the Working card via SNMP.
!
no keepalive
!
! This is defaulted to 10 seconds with the N+1 IOS code, but should be disabled on
! the Protect interface or set relatively high.
!
cable downstream annex B
cable downstream modulation 64qam
cable downstream interleave-depth 32
!
! The DS modulation and Interleave must be the same on the Protect and Working interfaces
! of the same HCCP group. The Protect interface itself must be "no shut" (enabled)
! for HCCP to activate
!
cable downstream rf-shutdown
cable upstream 0 shutdown
!
! These interfaces automatically become "no shut" (enabled) when a switchover occurs.
!
cable upstream 1 shutdown
cable upstream 2 shutdown
cable upstream 3 shutdown
hccp 1 protect 1 10.10.10.1
!
! This is the first HCCP group and it is protecting member 1 with member 1's
! FE IP address. If it is intra-chassis, you can use the Loopback0 IP address.
!
hccp 1 channel-switch 1 rfsw2 rfswitch-group 10.97.1.20 AA200000 1
!
! This is the IP address of the RF Switch and it is protecting member 1, which
! has a bitmap of AA200000 in Switch slot 1.
!

```



```

hcp 1 protect 2 10.10.10.1
!
! This is the first HCCP group and it is protecting member 2 with the loopback
! IP address.
!
hcp 1 channel-switch 2 rfs2 rswitch-group 10.97.1.20 AA200000 2
!
! This is the IP address of the RF Switch and it is protecting member 2, with a
! bitmap of AA200000 in Switch slot 2.
!
hcp 1 protect 3 10.10.10.1
hcp 1 channel-switch 3 rfs2 rswitch-group 10.97.1.20 AA200000 3
hcp 1 protect 4 10.10.10.1
hcp 1 channel-switch 4 rfs2 rswitch-group 10.97.1.20 AA200000 4
hcp 1 protect 5 10.10.10.1
hcp 1 channel-switch 5 rfs2 rswitch-group 10.97.1.20 AA200000 5
hcp 1 protect 6 10.10.10.1
hcp 1 channel-switch 6 rfs2 rswitch-group 10.97.1.20 AA200000 6
hcp 1 protect 7 10.10.10.1
hcp 1 channel-switch 7 rfs2 rswitch-group 10.97.1.20 AA200000 7
!
! These channel-switch configurations can be copied and pasted into their respective
! Working interfaces.
!
hcp 1 timers 5000 15000
!
! Cisco IOS command = hcp 1 timers <hellotime> <holdtime>
! This is mostly for inter-chassis communication, so set it high for the uBR10012
! as this can create extra CPU load.
!
no hcp 1 revertive
!
interface Cable5/1/1
!
! This is the Protect interface for the second group.
!
no ip address
no keepalive
cable downstream annex B
cable downstream modulation 64qam
cable downstream interleave-depth 32
cable downstream rf-shutdown
cable upstream 0 shutdown
cable upstream 1 shutdown
cable upstream 2 shutdown
cable upstream 3 shutdown
!
hcp 2 protect 1 10.10.10.1
hcp 2 channel-switch 1 rfs2 rswitch-group 10.97.1.20 55100000 1
!
! Because this MAC domain is on right side of header, the bitmap in
! hexadecimal code is 55100000.
!
hcp 2 protect 2 10.10.10.1
hcp 2 channel-switch 2 rfs2 rswitch-group 10.97.1.20 55100000 2
hcp 2 protect 3 10.10.10.1
hcp 2 channel-switch 3 rfs2 rswitch-group 10.97.1.20 55100000 3
hcp 2 protect 4 10.10.10.1
hcp 2 channel-switch 4 rfs2 rswitch-group 10.97.1.20 55100000 4
hcp 2 protect 5 10.10.10.1
hcp 2 channel-switch 5 rfs2 rswitch-group 10.97.1.20 55100000 5
hcp 2 protect 6 10.10.10.1
hcp 2 channel-switch 6 rfs2 rswitch-group 10.97.1.20 55100000 6
hcp 2 protect 7 10.10.10.1
hcp 2 channel-switch 7 rfs2 rswitch-group 10.97.1.20 55100000 7
hcp 2 timers 5000 15000
no hcp 2 revertive

interface Cable5/1/2
!
! This is the Protect interface for the third group.
!
no ip address
no keepalive
cable downstream annex B
cable downstream modulation 64qam
cable downstream interleave-depth 32
cable downstream rf-shutdown
cable upstream 0 shutdown
cable upstream 1 shutdown
cable upstream 2 shutdown
cable upstream 3 shutdown
hcp 3 protect 1 10.10.10.1
hcp 3 channel-switch 1 rfs1 rswitch-group 10.97.1.19 00C80000 1
hcp 3 channel-switch 1 rfs2 rswitch-group 10.97.1.20 00C00000 1

```

```

!
! Because the third MAC domain will traverse both Switches, two statements are needed.
! The "00" in front of the bitmaps are dropped when viewing the running configuration.
!

```

```
no hccp 3 revertive
```

```
interface Cable5/1/3
```

```
!
! This is the Protect interface for the fourth group.
!

```

```

hccp 4 protect 1 10.10.10.1
hccp 4 channel-switch 1 rfsw1 rfswitch-group 10.97.1.19 AA200000 1
hccp 4 protect 2 10.10.10.1
hccp 4 channel-switch 2 rfsw1 rfswitch-group 10.97.1. 19 AA200000 2
hccp 4 protect 3 10.10.10.1
hccp 4 channel-switch 3 rfsw1 rfswitch-group 10.97.1. 19 AA200000 3
hccp 4 protect 4 10.10.10.1
hccp 4 channel-switch 4 rfsw1 rfswitch-group 10.97.1. 19 AA200000 4
hccp 4 protect 5 10.10.10.1
hccp 4 channel-switch 5 rfsw1 rfswitch-group 10.97.1. 19 AA200000 5
hccp 4 protect 6 10.10.10.1
hccp 4 channel-switch 6 rfsw1 rfswitch-group 10.97.1. 19 AA200000 6
hccp 4 protect 7 10.10.10.1
hccp 4 channel-switch 7 rfsw1 rfswitch-group 10.97.1. 19 AA200000 7
no hccp 4 revertive

```

```
interface Cable5/1/4
```

```
!
! This is the Protect interface for the fifth group.
!

```

```

hccp 5 protect 1 10.10.10.1
hccp 5 channel-switch 1 rfsw1 rfswitch-group 10.97.1.19 55100000 1
hccp 5 protect 2 10.10.10.1
hccp 5 channel-switch 2 rfsw1 rfswitch-group 10.97.1. 19 55100000 2
hccp 5 protect 3 10.10.10.1
hccp 5 channel-switch 3 rfsw1 rfswitch-group 10.97.1. 19 55100000 3
hccp 5 protect 4 10.10.10.1
hccp 5 channel-switch 4 rfsw1 rfswitch-group 10.97.1. 19 55100000 4
hccp 5 protect 5 10.10.10.1
hccp 5 channel-switch 5 rfsw1 rfswitch-group 10.97.1. 19 55100000 5
hccp 5 protect 6 10.10.10.1
hccp 5 channel-switch 6 rfsw1 rfswitch-group 10.97.1. 19 55100000 6
hccp 5 protect 7 10.10.10.1
hccp 5 channel-switch 7 rfsw1 rfswitch-group 10.97.1. 19 55100000 7

```

```

!
! Interface configurations continue as such for the remaining Protect interfaces.
!

```

```
interface Cable8/1/0
```

```
!
! This is the Working interface for the first group.
!

```

```

ip address 10.192.5.1 255.255.255.0 secondary
ip address 172.25.1.1 255.255.255.0

```

```
!
! Interface bundling is supported as are subinterfaces.
!

```

```

ip rip send version 2
ip rip receive version 2
keepalive 1

```

```

!
! The keepalive time is in seconds and the default is 10 seconds for HCCP code.
! Only set this value after modems have stabilized.
!

```

```

cable downstream annex B
cable downstream modulation 64qam
cable downstream interleave-depth 32
cable downstream frequency 453000000

```

```
!
! This is the DS frequency, which must be set for the internal upconverter to operate.
!

```

```

cable downstream channel-id 0
no cable downstream rf-shutdown

```

```
!
! This is needed to turn on the DS RF output.
!

```

```
cable upstream 0 frequency 24000000
```

```

!
! If doing dense mode combining, the upstream frequencies will need to be different.
! If no two US ports are shared, the same frequency can be used.
!

```

```

cable upstream 0 power-level 0
cable upstream 0 connector 0

```

```

!
cable upstream 0 channel-width 3200000
cable upstream 0 minislot-size 2
cable upstream 0 modulation-profile 22
no cable upstream 0 shutdown
.
.
.
cable dhcp-giaddr policy
!
! This tells cable modems to get an IP address from the primary scope and CPEs to use
! the secondary scope.
!
! hccp 1 working 1
!
! This is Working member 1 of HCCP Group 1.
!
hccp 1 channel-switch 1 rfs2 rfs2-group 10.97.1.20 AA200000 1
!
! This is the IP address of Switch & member 1, which has a bitmap of
! AA200000 in Switch slot 1.
!
hccp 1 reverttime 120
!
! This is the time in minutes (+ 2 minute suspend) for the card to switch back to
! normal mode if the fault has cleared. If a fault was initiated by a keepalive
! and you had a fault on the Protect card, it would revert back after the suspend
! time and not wait the full revert time.
!
interface Cable8/1/1
!
! This is the Working interface for the second HCCP group.
!
ip address 10.192.5.1 255.255.255.0 secondary
ip address 172.25.2.1 255.255.255.0
ip rip send version 2
ip rip receive version 2
keepalive 1
cable downstream annex B
cable downstream modulation 64qam
cable downstream interleave-depth 32
cable downstream frequency 453000000
cable downstream channel-id 1
no cable downstream rf-shutdown
cable upstream 0 frequency 24000000
cable upstream 0 power-level 0
cable upstream 0 connector 4
cable upstream 0 channel-width 3200000
cable upstream 0 minislot-size 22
cable upstream 0 modulation-profile 2
no cable upstream 0 shutdown
.
.
.
cable dhcp-giaddr policy
hccp 2 working 1
!
! This is Working member 1 of HCCP Group 2.
!
hccp 2 channel-switch 1 rfs2 rfs2-group 10.97.1.20 55100000 1
!
! This is the IP address of Switch & Member 1 of Group 2, which has a bitmap of
! 55100000 in Switch slot 1.
!
hccp 2 reverttime 120
!
interface Cable8/1/2
!
! This is the Working interface for the third HCCP group.
!
ip address 10.192.5.1 255.255.255.0 secondary
ip address 172.25.3.1 255.255.255.0
ip rip send version 2
ip rip receive version 2
keepalive 1
cable downstream annex B
cable downstream modulation 64qam
cable downstream interleave-depth 32
cable downstream frequency 453000000
cable downstream channel-id 2
no cable downstream rf-shutdown
cable upstream 0 frequency 24000000
cable upstream 0 power-level 0
cable upstream 0 connector 8

```

```

cable upstream 0 channel-width 3200000
cable upstream 0 minislot-size 2
cable upstream 0 modulation-profile 22
no cable upstream 0 shutdown
cable dhcp-giaddr policy
.
.
.
hccp 3 working 1
!
! This is the Working member 1 of HCCP Group 3.
!
hccp 3 channel-switch 1 rfsw1 rfswitch-group 10.97.1.19 00c80000 1
hccp 3 channel-switch 1 rfsw2 rfswitch-group 10. 97.1.1.20 00c00000 1
hccp 3 reverttime 120

interface Cable8/1/3
!
! This is the Working interface for the fourth HCCP group.
!
hccp 4 working 1
hccp 4 channel-switch 1 rfsw1 rfswitch-group 10.97.1.19 AA200000 1
hccp 4 reverttime 120

interface Cable8/1/4
!
! This is the Working interface for the fifth HCCP group.
!
hccp 5 working 1
hccp 5 channel-switch 1 rfsw1 rfswitch-group 10.97.1.19 55100000 1
hccp 5 reverttime 120

!
ip classless
no ip http server
!
no cdp run
snmp-server community private RW
!
! This does not affect the HCCP communications between the Switch and uBR10012.
!
snmp-server enable traps cable
no cdp run
snmp-server manager
tftp-server server
tftp-server ios.cf alias ios.cf
!
alias exec t configure terminal
alias exec scm show cable modem
alias exec scr sh cab mode remote
alias exec shb sh hccp br
alias exec shd sh hccp detail
alias exec shc sh hccp chan
!
line con 0
logging synchronous
line aux 0
no exec
transport input all
!
! The three lines above were used to console from the Auxiliary port of the uBR10012
! to the Switch.
!
line vty 0 4
session-timeout 400
password xx
login
endBuilding configuration...

```

Example: Cisco 3x10 RF Switches and uBR7246VXR Chassis

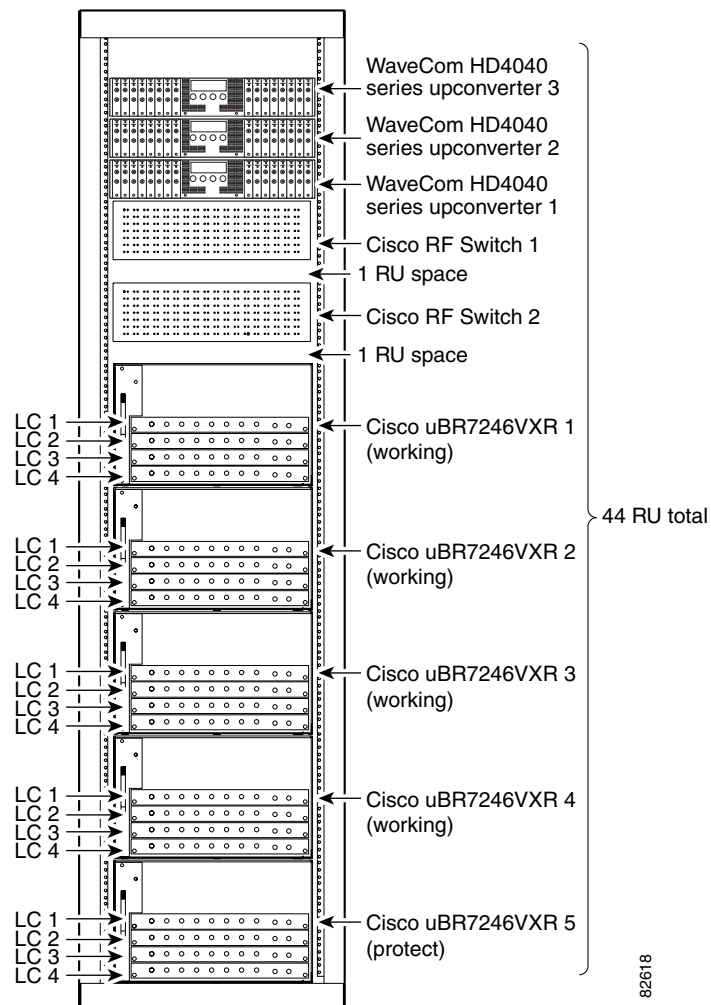
This is a sample N+1 configuration using the following Cisco CMTS:

- Two Cisco 3x10 RF Switches in 4+1 mode
- Five Cisco uBR7246VXR routers
- 20 uBR-MC28U/X line cards
- Three VCom HD4040 chassis containing 40 modules

The physical rack layout is shown below in Figure 6. A cabling document can be found on Cisco.com at:

<http://www.cisco.com/univercd/cc/td/doc/product/cable/rfswitch/rfswvxc2.htm>

Figure 6 Physical Stack: 4+1 Redundancy Using Five uBR7246VXR Chassis with Two Cisco 3x10 RF Switches and Three VCom Upconverters



The physical stack illustrated above assumes IP assignments starting with 192.168.1.2 from the top and continuing downward. Cisco RF Switch 1 is considered to be two switches because it will be in the 4+1 mode (a & b), where a contains slots 1-4 and b contains slots 5-8. The Cisco RF Switch 2 is also considered to be two switches (a & b).

HCCP Working uBR7246VXR Chassis 1

```

version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname "WorkingVXR1"
!
boot system disk0:ubr7200-ik8s-mz.BC.28July03
no logging console
enable secret 5 $1$5YHG$mquxabcqzFoUUKhp/c9WT4/
!
cab modem remote-query 10 public
cab modulation-prof 2 request 0 16 0 8 qpsk scrambler 152 no-diff 64 fixed uw8
cab modulation-prof 2 initial 5 34 0 48 qpsk scrambler 152 no-diff 128 fixed uw16
cab modulation-prof 2 station 5 34 0 48 qpsk scrambler 152 no-diff 128 fixed uw16
cab modulation-prof 2 short 4 76 6 8 qpsk scrambler 152 no-diff 72 short uw8
cab modulation-prof 2 long 8 220 0 8 qpsk scrambler 152 no-diff 80 short uw8
cab modulation-prof 3 request 0 16 0 8 qpsk scrambler 152 no-diff 64 fixed uw16
cab modulation-prof 3 initial 5 34 0 48 qpsk scrambler 152 no-diff 128 fixed uw16
cab modulation-prof 3 station 5 34 0 48 qpsk scrambler 152 no-diff 128 fixed uw16
cab modulation-prof 3 short 7 76 7 8 16qam scrambler 152 no-diff 144 short uw16
cab modulation-prof 3 long 9 220 0 8 16qam scrambler 152 no-diff 160 short uw16
no cable qos permission create
no cable qos permission update
cable qos permission modems
no cable clock source-midplane
no cable clock force primary
no cable clock force secondary
!
cable config-file docsis.cm
frequency 453000000
service-class 1 max-upstream 10000
service-class 1 max-downstream 10000
service-class 1 max-burst 1522
!
ip subnet-zero
ip cef
!
ip host protect 192.168.1.7
ip host work2 192.168.1.6
ip name-server 171.68.226.120
!
ip dhcp pool MODEMS1
network 192.168.3.0 255.255.255.0
bootfile docsis.cm
next-server 192.168.3.5
default-router 192.168.3.5
option 7 ip 192.168.3.5
option 4 ip 192.168.3.5
option 2 hex 0000.0000
lease 2 3 4
!
ip dhcp pool PC
network 10.11.12.0 255.255.255.0
default-router 10.11.12.1
dns-server 171.68.226.120
lease 10 1 11
!
packetcable element_id 35417
!
interface FastEthernet0/0
ip address 192.168.1.7 255.255.255.0
no keepalive
speed auto
full-duplex
!
! This interface is used for HCCP traffic.
!
interface FastEthernet0/1
ip address 192.168.2.7 255.255.255.0
keepalive 1
!
! Keepalive is set to 1 second so that if the cable is disconnected, this interface
! switches over within 3 seconds.
!
speed auto
full-duplex
!
interface Cable3/0

```

```

ip address 10.11.12.1 255.255.255.0 secondary
ip address 192.168.3.5 255.255.255.0
load-interval 30
keepalive 1
!
! The keepalive time is in seconds and the default is 10 seconds for HCCP code.
!
load-interval 30
cable downstream channel-id 0
cable bundle 1 master
!
! Interface bundling is supported as are subinterfaces.
! Note: Bundles switch over together.
!
cable downstream annex B
cable downstream modulation 64qam
cable downstream interleave-depth 32
cable downstream frequency 453000000
!
! This is DS frequency, which used to be informational only when using an external UPx.
! This must be set when using the MC28U cards with internal UPxs or when doing N+1 with
! MC28C cards, so the Protect UPx knows what frequency to use.
!
cable upstream 0 frequency 24000000
!
! If doing dense mode combining, the upstream frequencies will need to be different.
! If no 2 US ports are shared, the same frequency can be used.
!
cable upstream 0 power-level 0
cable upstream 0 channel-width 3200000
cable upstream 0 minislot-size 2
cable upstream 0 data-backoff automatic
cable upstream 0 modulation-profile 3
no cable upstream 0 shutdown

cable dhcp-giaddr policy
!
! This tells CMTs to get an IP address from the primary scope and CPEs to use the
! secondary scope.
!
hccp 1 working 1
!
! This is the working first group, member 1.
!
hccp 1 channel-switch 1 rfs1a rfs1-switch-group 192.168.1.5 44440400 1
!
! This is the IP address of the Switch and it's protecting member 1 in the left side
! of Switch slot 1.
!
hccp 1 channel-switch 1 uc31 wavecom-hd 192.168.1.2 1 192.168.1.4 1
!
! This is the IP address of upconverter and its module 1 (A) that is backing
! module 1 (A) of another upconverter. This shows that one upconverter could
! have a module backing up a module in a different chassis with a different IP address
! if need be. If this statement is not present when using 15BC2 IOS and later Cisco
! IOS releases, IF Muting is assumed to be enabled and an external upconverter with
! SNMP capability is not needed.
!
hccp 1 track FastEthernet0/1
!
! Tracking was enabled for the egress port in case the WAN-backhaul was disrupted.
! This cable interface would switch over to the Protect.
!
hccp 1 reverttime 120
!
! This is the time in minutes (+ 2 minute suspend) for the card to switch back to
! normal mode if the fault has cleared. If there is a fault on the Protect card,
! it reverts back after the suspend time & does not wait for the full revert time.
!
interface Cable3/1
hccp 2 working 1
hccp 2 channel-switch 1 rfs1a rfs1-switch-group 192.168.1.5 11110100 1
!
! This is the IP address of the Switch and it is protecting member 1 in the right side
! of Switch slot 1.
!
hccp 2 channel-switch 1 uc31 wavecom-hd 192.168.1.2 2 192.168.1.4 2
hccp 2 reverttime 120

interface Cable4/0
hccp 3 working 1
hccp 3 channel-switch 1 rfs1b rfs1-switch-group 192.168.1.5 88880800 1

```

```

!
! This is the IP address of the Switch and it is protecting member 1 in the left side
! of Switch slot 5.
!
hccp 3 channel-switch 1 uc31 wavecom-hd 192.168.1.2 3 192.168.1.4 3
hccp 3 reverttime 120
!
interface Cable 4/1
hccp 4 working 1
hccp 4 channel-switch 1 rfsw1b rfswitch-group 192.168.1.5 22220200 1
!
! This is the IP address of the Switch and it is protecting member 1 in the right side
! of Switch slot 5.
!
hccp 4 channel-switch 1 uc31 wavecom-hd 192.168.1.2 4 192.168.1.4 4
hccp 4 reverttime 120

interface Cable5/0
hccp 5 working 1
hccp 5 channel-switch 1 rfsw2a rfswitch-group 192.168.1.6 44440400 1
hccp 5 channel-switch 1 uc31 wavecom-hd 192.168.1.2 5 192.168.1.4 5
hccp 5 reverttime 120
!
interface Cable 5/1
hccp 6 working 1
hccp 6 channel-switch 1 rfsw2a rfswitch-group 192.168.1.6 11110100 1
hccp 6 channel-switch 1 uc31 wavecom-hd 192.168.1.2 6 192.168.1.4 6
hccp 6 reverttime 120

interface Cable 6/0
hccp 7 working 1
hccp 7 channel-switch 1 rfsw2b rfswitch-group 192.168.1.6 88880800 1
hccp 7 channel-switch 1 uc31 wavecom-hd 192.168.1.2 7 192.168.1.4 7
hccp 7 reverttime 120

interface Cable 6/1
hccp 8 working 1
hccp 8 channel-switch 1 rfsw2b rfswitch-group 192.168.1.6 22220200 1
hccp 8 channel-switch 1 uc31 wavecom-hd 192.168.1.2 8 192.168.1.4 8
hccp 8 reverttime 120

router eigrp 2500
network 10.11.12.0 0.0.0.255
network 192.168.1.0
network 192.168.3.0
no auto-summary
no eigrp log-neighbor-changes
!
ip classless
ip route 0.0.0.0 0.0.0.0 192.168.1.254
ip route 192.168.1.0 255.255.255.0 FastEthernet0/0
ip route 192.168.2.0 255.255.255.0 FastEthernet0/1
no ip http server
!
cdp run
!
snmp-server community private RW
!
! This does not affect the HCCP communications between the Upconverter, Switch, and 7200.
!
snmp-server community public RO
snmp-server enable traps tty
snmp-server manager
tftp-server disk0:
tftp-server disk1:
tftp-server disk1:rfsw250-fl-1935030e
tftp-server disk1:rfsw250-bf-1935022d
alias exec shb show hccp brief
alias exec shd show hccp detail
alias exec scm show cable modem
alias exec scr show cable modem remote
alias exec sm show cab modu
alias exec sch show cab hop
alias exec sc300 show cont c3/0 u0
alias exec sint300 show int c3/0 u0
alias exec scs show cable spec

```


HCCP Protect uBR7246VXR Chassis

```

version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname "ProtectVXR"
!
boot system disk0:ubr7200-ik8s-mz.BC.28July03
no logging console
enable secret 5 $1$5YHG$mquxbcqzFoUUKhp/c9WT4/
!
cab modem remote-query 10 public
cab modulation-prof 2 request 0 16 0 8 qpsk scrambler 152 no-diff 64 fixed uw8
cab modulation-prof 2 initial 5 34 0 48 qpsk scrambler 152 no-diff 128 fixed uw16
cab modulation-prof 2 station 5 34 0 48 qpsk scrambler 152 no-diff 128 fixed uw16
cab modulation-prof 2 short 4 76 6 8 qpsk scrambler 152 no-diff 72 short uw8
cab modulation-prof 2 long 8 220 0 8 qpsk scrambler 152 no-diff 80 short uw8
cab modulation-prof 3 request 0 16 0 8 qpsk scrambler 152 no-diff 64 fixed uw16
cab modulation-prof 3 initial 5 34 0 48 qpsk scrambler 152 no-diff 128 fixed uw16
cab modulation-prof 3 station 5 34 0 48 qpsk scrambler 152 no-diff 128 fixed uw16
cab modulation-prof 3 short 7 76 7 8 16qam scrambler 152 no-diff 144 short uw16
cab modulation-prof 3 long 9 220 0 8 16qam scrambler 152 no-diff 160 short uw16
no cable qos permission create
no cable qos permission update
cable qos permission modems
no cable clock source-midplane
no cable clock force primary
no cable clock force secondary
!
cable config-file docsis.cm
frequency 453000000
service-class 1 max-upstream 10000
service-class 1 max-downstream 10000
service-class 1 max-burst 1522
!
ip subnet-zero
ip cef
!
ip host protect 192.168.1.7
ip host work2 192.168.1.6
ip name-server 171.68.226.120
!
ip dhcp pool MODEMS1
network 192.168.3.0 255.255.255.0
bootfile docsis.cm
next-server 192.168.3.5
default-router 192.168.3.5
option 7 ip 192.168.3.5
option 4 ip 192.168.3.5
option 2 hex 0000.0000
lease 2 3 4
!
ip dhcp pool PC
network 10.11.12.0 255.255.255.0
default-router 10.11.12.1
dns-server 171.68.226.120
lease 10 1 11
!
packetcable element_id 35417
!
interface FastEthernet0/0
ip address 192.168.1.11 255.255.255.0
no keepalive
speed auto
full-duplex
no cdp enable
!
interface FastEthernet0/1
ip address 192.168.2.11 255.255.255.0
keepalive 1
speed auto
full-duplex

```

```

no cdp enable
!
interface Cable3/0
no ip address
!
! There is no need to set the IP address because it comes from the Working
! card via SNMP.
!
no keepalive
!
! This is set to default of 10 seconds with the N+1 IOS code, but recommended
! to be disabled on the Protect interface or set relatively high.
!
cable downstream annex B
cable downstream modulation 64qam
cable downstream interleave-depth 32
!
! The DS modulation, Annex mode, and Interleave must be same on the Protect and
! Working of the same group.
!
no shut
!
! The interface must be activated to start HCCP functionality. Do this configuration last.
!
cable upstream 0 shutdown
!
! This automatically becomes "no shut" (enabled) when a switchover occurs.
!
hccp 1 protect 1 192.168.1.7
!
! This is the Protect for the first group. Remember to configure the Protect
! interface(s) last; after the Working interfaces are configured. This is the
! HCCP first group and it is protecting member 1 with member 1's FE IP address.
!
hccp 1 channel-switch 1 rfsw1a rfswitch-group 192.168.1.5 44440400 1
!
! This is the IP address of the Switch and it is protecting member 1, which has a
! bitmap of 44440400 in Switch slot 1.
!
hccp 1 channel-switch 1 uc31 wavecom-hd 192.168.1.2 1 192.168.1.4 1
!
! This is the IP address of upconverter and its module 1 (A) that is backing
! module 1 (A) of another upconverter. This shows that one upconverter could have a
! module backing up a module in a different chassis with a different IP address if need
! be. If this statement is not present when using 15BC2 IOS and later Cisco
! IOS releases, IF Muting is assumed to be enabled and an external upconverter with
! SNMP capability is not needed.
!
hccp 1 protect 2 192.168.1.8
!
! This is the HCCP first group and it is protecting member 2 with its IP address.
!
hccp 1 channel-switch 2 rfsw1a rfswitch-group 192.168.1.5 44440400 2
hccp 1 channel-switch 2 uc31 wavecom-hd 192.168.1.2 1 192.168.1.4 9
hccp 1 protect 3 192.168.1.9
hccp 1 channel-switch 3 rfsw1a rfswitch-group 192.168.1.5 44440400 3
hccp 1 channel-switch 3 uc32 wavecom-hd 192.168.1.2 1 192.168.1.3 1
hccp 1 protect 4 192.168.1.10
hccp 1 channel-switch 4 rfsw1a rfswitch-group 192.168.1.5 44440400 4
hccp 1 channel-switch 4 uc32 wavecom-hd 192.168.1.2 1 192.168.1.3 9
hccp 1 timers 666 2000
hccp 1 timers
!
! Cisco IOS command = <hellotime> <holdtime>
! This is for inter-chassis communication.
!
interface Cable3/1

hccp 2 protect 1 192.168.1.7
hccp 2 channel-switch 1 rfsw1a rfswitch-group 192.168.1.5 11110100 1
hccp 2 channel-switch 1 uc31 wavecom-hd 192.168.1.2 2 192.168.1.4 2
hccp 2 protect 2 192.168.1.8
hccp 2 channel-switch 2 rfsw1a rfswitch-group 192.168.1.5 11110100 2
hccp 2 channel-switch 2 uc31 wavecom-hd 192.168.1.2 2 192.168.1.4 10
hccp 2 protect 3 192.168.1.9

```

```
hccp 2 channel-switch 3 rfsw1a rfswitch-group 192.168.1.5 11110100 3
hccp 2 channel-switch 3 uc32 wavecom-hd 192.168.1.2 2 192.168.1.3 2
hccp 2 protect 4 192.168.1.10
hccp 2 channel-switch 4 rfsw1a rfswitch-group 192.168.1.5 11110100 4
hccp 2 channel-switch 4 uc32 wavecom-hd 192.168.1.2 2 192.168.1.3 10
hccp 2 timers 666 2000

interface Cable4/0

hccp 3 protect 1 192.168.1.7
hccp 3 channel-switch 1 rfsw1b rfswitch-group 192.168.1.5 88880800 1
hccp 3 channel-switch 1 uc31 wavecom-hd 192.168.1.2 3 192.168.1.4 3
hccp 3 protect 2 192.168.1.8
hccp 3 channel-switch 2 rfsw1b rfswitch-group 192.168.1.5 88880800 2
hccp 3 channel-switch 2 uc31 wavecom-hd 192.168.1.2 3 192.168.1.4 11
hccp 3 protect 3 192.168.1.9
hccp 3 channel-switch 3 rfsw1b rfswitch-group 192.168.1.5 88880800 3
hccp 3 channel-switch 3 uc32 wavecom-hd 192.168.1.2 3 192.168.1.3 3
hccp 3 protect 4 192.168.1.10
hccp 3 channel-switch 4 rfsw1b rfswitch-group 192.168.1.5 88880800 4
hccp 3 channel-switch 4 uc32 wavecom-hd 192.168.1.2 3 192.168.1.3 11
hccp 3 timers 666 2000

interface Cable4/1

hccp 4 protect 1 192.168.1.7
hccp 4 channel-switch 1 rfsw1b rfswitch-group 192.168.1.5 22220200 1
hccp 4 channel-switch 1 uc31 wavecom-hd 192.168.1.2 4 192.168.1.4 4
hccp 4 protect 2 192.168.1.8
hccp 4 channel-switch 2 rfsw1b rfswitch-group 192.168.1.5 22220200 2
hccp 4 channel-switch 2 uc31 wavecom-hd 192.168.1.2 4 192.168.1.4 12
hccp 4 protect 3 192.168.1.9
hccp 4 channel-switch 3 rfsw1b rfswitch-group 192.168.1.5 22220200 3
hccp 4 channel-switch 3 uc32 wavecom-hd 192.168.1.2 4 192.168.1.3 4
hccp 4 protect 4 192.168.1.10
hccp 4 channel-switch 4 rfsw1b rfswitch-group 192.168.1.5 22220200 4
hccp 4 channel-switch 4 uc32 wavecom-hd 192.168.1.2 4 192.168.1.3 12
hccp 4 timers 666 2000

interface Cable5/0

hccp 5 protect 1 192.168.1.7
hccp 5 channel-switch 1 rfsw2a rfswitch-group 192.168.1.6 44440400 1
hccp 5 channel-switch 1 uc31 wavecom-hd 192.168.1.2 5 192.168.1.4 5
hccp 5 protect 2 192.168.1.8
hccp 5 channel-switch 2 rfsw2a rfswitch-group 192.168.1.6 44440400 2
hccp 5 channel-switch 2 uc31 wavecom-hd 192.168.1.2 5 192.168.1.4 13
hccp 5 protect 3 192.168.1.9
hccp 5 channel-switch 3 rfsw2a rfswitch-group 192.168.1.6 44440400 3
hccp 5 channel-switch 3 uc32 wavecom-hd 192.168.1.2 5 192.168.1.3 5
hccp 5 protect 4 192.168.1.10
hccp 5 channel-switch 4 rfsw2a rfswitch-group 192.168.1.6 44440400 4
hccp 5 channel-switch 4 uc32 wavecom-hd 192.168.1.2 5 192.168.1.3 13
hccp 5 timers 666 2000

interface Cable5/1

hccp 6 protect 1 192.168.1.7
hccp 6 channel-switch 1 rfsw2a rfswitch-group 192.168.1.6 11110100 1
hccp 6 channel-switch 1 uc31 wavecom-hd 192.168.1.2 6 192.168.1.4 6
hccp 6 protect 2 192.168.1.8
hccp 6 channel-switch 2 rfsw2a rfswitch-group 192.168.1.6 11110100 2
hccp 6 channel-switch 2 uc31 wavecom-hd 192.168.1.2 6 192.168.1.4 14
hccp 6 protect 3 192.168.1.9
hccp 6 channel-switch 3 rfsw2a rfswitch-group 192.168.1.6 11110100 3
hccp 6 channel-switch 3 uc32 wavecom-hd 192.168.1.2 6 192.168.1.3 6
hccp 6 protect 4 192.168.1.10
hccp 6 channel-switch 4 rfsw2a rfswitch-group 192.168.1.6 11110100 4
hccp 6 channel-switch 4 uc32 wavecom-hd 192.168.1.2 6 192.168.1.3 14
hccp 6 timers 666 2000

interface Cable6/0

hccp 7 protect 1 192.168.1.7
hccp 7 channel-switch 1 rfsw2b rfswitch-group 192.168.1.6 88880800 1
```

```

hccp 7 channel-switch 1 uc31 wavecom-hd 192.168.1.2 7 192.168.1.4 7
hccp 7 protect 2 192.168.1.8
hccp 7 channel-switch 2 rfsw2b rfswitch-group 192.168.1.6 88880800 2
hccp 7 channel-switch 2 uc31 wavecom-hd 192.168.1.2 7 192.168.1.4 15
hccp 7 protect 3 192.168.1.9
hccp 7 channel-switch 3 rfsw2b rfswitch-group 192.168.1.6 88880800 3
hccp 7 channel-switch 3 uc32 wavecom-hd 192.168.1.2 7 192.168.1.3 7
hccp 7 protect 4 192.168.1.10
hccp 7 channel-switch 4 rfsw2b rfswitch-group 192.168.1.6 88880800 4
hccp 7 channel-switch 4 uc32 wavecom-hd 192.168.1.2 7 192.168.1.3 15
hccp 7 timers 666 2000

interface Cable6/1

hccp 8 protect 1 192.168.1.7
hccp 8 channel-switch 1 rfsw2b rfswitch-group 192.168.1.6 22220200 1
hccp 8 channel-switch 1 uc31 wavecom-hd 192.168.1.2 8 192.168.1.4 8
hccp 8 protect 2 192.168.1.8
hccp 8 channel-switch 2 rfsw2b rfswitch-group 192.168.1.6 22220200 2
hccp 8 channel-switch 2 uc31 wavecom-hd 192.168.1.2 8 192.168.1.4 16
hccp 8 protect 3 192.168.1.9
hccp 8 channel-switch 3 rfsw2b rfswitch-group 192.168.1.6 22220200 3
hccp 8 channel-switch 3 uc32 wavecom-hd 192.168.1.2 8 192.168.1.3 8
hccp 8 protect 4 192.168.1.10
hccp 8 channel-switch 4 rfsw2b rfswitch-group 192.168.1.6 22220200 4
hccp 8 channel-switch 4 uc32 wavecom-hd 192.168.1.2 8 192.168.1.3 16
hccp 8 timers 666 2000

router eigrp 2500
 network 10.11.12.0 0.0.0.255
 network 10.11.13.0 0.0.0.255
 network 192.168.1.0
 network 192.168.3.0
 network 192.168.5.0
 no auto-summary
 no eigrp log-neighbor-changes
!
ip classless
ip route 0.0.0.0 0.0.0.0 192.168.1.254
ip route 192.168.1.0 255.255.255.0 FastEthernet0/0
ip route 192.168.2.0 255.255.255.0 FastEthernet0/1
no ip http server
!
cdp run
!
snmp-server community private RW
snmp-server community public RO
snmp-server enable traps tty
snmp-server enable traps cable
snmp-server manager
alias exec shb show hccp brief
alias exec shd show hccp detail
alias exec scm show cable modem
alias exec scr show cable modem remote

```

Additional References

Cisco supports N+1 Redundancy using the Cisco 3x10 RF Switch on the following Cisco CMTS platforms:

- Cisco uBR10012 Universal Broadband Router
- Cisco uBR7246VXR Universal Broadband Router

For additional information related to N+1 Redundancy, the Cisco RF switch, and the Cisco uBR10012 and uBR7246VXR routers, refer to the following references.

Related Documents

Related Topic	Document Title
Broadband Cable Command References	• <i>Cisco Broadband Cable Command Reference Guide</i> http://www.cisco.com/univercd/cc/td/doc/product/cable/bbccmref/index.htm • <i>Cisco RF Switch Firmware Command Reference Guide</i> http://lbg.cisco.com/push_targets1/ucdit/cc/td/doc/product/cable/rfswitch/rfcoms35.htm
Cisco RF Switches	• <i>Cisco RF Switch Documentation</i> Web page (complete documentation set) http://www.cisco.com/univercd/cc/td/doc/product/cable/rfswitch/index.htm • Cisco RF Switch Installation and Configuration Guide http://www.cisco.com/univercd/cc/td/doc/product/cable/rfswitch/icg/ • Cisco RF Switch Product Data Sheet http://www.cisco.com/univercd/cc/td/doc/pcat/rfswitch.htm • Field Notice—<i>uBR-RF-SW (N+1 Switch) Firmware Upgrade to Version 3.3 to Enable Setting of Default Gateway for Remote Software Upgrades</i> http://www.cisco.com/warp/public/770/fn19290.shtml
Cisco uBR7246VXR Universal Broadband Router	• <i>Cisco uBR7200 Series Universal Broadband Routers</i> Web page (complete documentation set) http://www.cisco.com/univercd/cc/td/doc/product/cable/cab_rout/index.htm
Cisco uBR10012 Universal Broadband Router	• <i>Cisco uBR10012 Universal Broadband Router</i> Web page (complete documentation set) http://www.cisco.com/univercd/cc/td/doc/product/cable/ubr10k/index.htm
High Availability References for Cisco Broadband Cable	• <i>Bitmap Calculator for N+1 Configuration with the Cisco RF Switch</i> (Microsoft Excel format) http://www.cisco.com/warp/public/109/BitMap.xls • Technical Note—<i>N+1 Tips and Configuration for the uBR 10012 Router with MC28C Cards</i> http://www.cisco.com/warp/public/109/n_1_ubr10k_19135_1.html • <i>CMTS Feature Guide—Configuring PacketCable on the Cisco CMTS</i> (with emphasis on the Cisco uBR7246VXR router) http://www.cisco.com/univercd/cc/td/doc/product/cable/cab_rout/cmtsfg/ufg_pkcb.htm

Related Topic	Document Title
DOCSIS and EuroDOCSIS	- Feature Module—<i>DOCSIS 1.1 for Cisco uBR7200 Series Universal Broadband Routers</i> http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121limit/121cx/docsis11.htm - CMTS Feature Guide—<i>Internal DOCSIS Configurator File Generator for the Cisco Cable Modem Termination System</i> http://www.cisco.com/univercd/cc/td/doc/product/cable/cab_rout/cmtsfg/ufgcfile.htm
Additional Broadband Cable Technical Reference	<i>Cisco Multiservice Broadband Cable Guide</i> http://www.cisco.com/en/US/products/hw/cable/prod_category_positioning_paper0900aec8006e98b.html - Cable Radio Frequency (RF) FAQs http://www.cisco.com/warp/public/109/cable_faq_rf.html

Standards

The Cisco uBR10012 router, Cisco uBR7246VXR router and the Cisco RF Switch each support N+1 redundancy in compliance with these industry standards:

- Data-Over-Cable Service Interface Specifications (DOCSIS):
 - DOCSIS 1.0 support for end-to-end cable telecommunications*
 - DOCSIS 1.1 support for end-to-end cable telecommunications*
- European DOCSIS (EuroDOCSIS)
- PacketCable

Refer to the your CMTS platform's release notes for additional information about standards supported by your specific CMTS equipment.

MIBs

Certain versions of Cisco RF Switch Firmware may increase the MIBs that support N+1 Redundancy on the Cisco CMTS. To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the [Cisco Network Management Software](#) web page (MIBs sections) on Cisco.com. MIBs information for the Cisco RF Switch is also summarized in the *Cisco RF Switch Firmware Command Reference Guide* (document cited above).

RFCs

No new or modified RFCs are supported by this feature.

Technical Assistance

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

Glossary

4+1 Redundancy Mode

4+1 redundancy describes the protection scheme in which a total of four cable interface line cards are configured to have three as Working and one as Protect. This is the required N+1 protection scheme for the Cisco uBR7246VXR router; this protection scheme is optional for the Cisco uBR10012 router. Typically, the Cisco RF switch in the 4+1 mode is functioning as two 4+1 switches independently.

8+1 Redundancy Mode

8+1 redundancy describes the protection scheme in which a total of eight cable interface line cards are configured to have seven as Working and one as Protect. This is the default N+1 protection scheme for the Cisco uBR10012 router.

Active RP

Active Route Processor (RP), also known as primary RP. The RP that controls the system, runs the routing protocols, and presents the system management interface.

CMTS

Cable Modem Termination System. A router or a bridge, typically located at the cable headend. Any DOCSIS-compliant headend cable router, such as the Cisco uBR7246VXR or Cisco uBR10012 universal broadband routers.

CPE

Customer Premises Equipment. Terminating equipment, such as terminals, telephones, and modems, supplied by the telephone company, installed at customer sites, and connected to the telephone company network. Can also refer to any telephone equipment residing on the customer site.

DOCSIS

Data-over-Cable Service Interface Specifications. Defines technical specifications for equipment at both subscriber locations and cable operators' headends. Adoption of DOCSIS will accelerate the deployment of data-over-cable services and will ensure interoperability of equipment throughout system operators' infrastructures.

Downstream (DS)

Frequency multiplexed band in a CATV channel that distributes signals from a headend facility (CMTS) to subscribers (cable modems).

EHSA

Enhanced High System Availability. Processor redundancy scheme that reduces switchover time by requiring that the redundant processor be running in hot standby mode.

EuroDOCSIS

European Data-over-Cable Service Interface Specifications.

HCCP

Hot-standby Connection-to-Connection Protocol. The Cisco Hot Standby Connection-to-Connection Protocol (HCCP) maintains all necessary DOCSIS or EuroDOCSIS state information-including service identifier (SID), service flow, and Media Access Control (MAC) and IP information-that enables a Protect line card to completely replace a Working line card when needed.

HCCP Group

Hot-standby Connection-to-Connection Protocol group. An HCCP group is a logical bundling of Cisco RF Switch cable interfaces. After you complete the definition of all required HCCP groups, you then assign each HCCP group a status of Working or Protect, according to your network topology.

IF Muting

Cisco's proprietary feature that supports non-SNMP upconverters (internal, integrated or external) in N+1 protection schemes. When used with either of Cisco's RF Switches, IF Muting allows for full N+1 Redundancy on both the Cisco uBR10012 and the Cisco uBR7246VXR CMTS.

N+1 Redundancy

Redundancy scheme in which one cable interface line card in Protect state provides support for N cable interface line cards in Working state. Common N+1 topologies are as follows:

- 8+1 Redundancy—Protection scheme in which eight cable interface line cards are configured as seven Working and one Protect line card). This protection scheme is also referred to as 7+1 Redundancy, which is more physically accurate than is 8+1.
- 4+1 Redundancy—Protection scheme in which four Working line cards are supported by one Protect line card.

NRU

N+1 Redundancy Unit. The NRU provides an Ethernet interface that allows the Cisco CMTS to be controlled remotely via SNMP. NRU also provides a management console port that allows configuration, software downloading, and additional functions.

Redundancy

In internetworking, Redundancy refers to the hardware and software duplication of Working devices, services or connections so that the redundant (Protect) devices, services, or connections can immediately take over in the event of a Working failure (switchover). Redundancy applies whether that switchover from Working to Protect is unexpected or manually initiated. See also [N+1 Redundancy](#).

RF

Radio Frequency. Generic term referring to frequencies that correspond to radio transmissions, that is wireless communications with frequencies below 300 GHz. Cable TV and broadband networks use RF technology.

RF Switch Module

The Cisco RF switch module is a switching matrix that allows flexibility in the routing of RF signals between "N" Working RF cable interface line cards and one Protect RF cable interface line card. The RF Switch header has 14 ports labeled with letters. Each header screws into a slot in the Cisco RF Switch. A Cisco RF Switch module contains all the active relays for a particular port for all slots. Each RF switch module supports the full frequency range specified by DOCSIS and EuroDOCSIS standards. For additional module information, refer to "[Cisco RF Switch Modules](#)" section on page 231.

RF Upconverter

An upconverter device is used to convert the 44 MHz intermediate frequency (IF) output to the assigned slot. In North America, carrier frequencies in the forward plant are assigned between 54-860 MHz. After upconversion, the signal is combined with other analog TV or digital TV signals and sent to the transmit input of a fiber transceiver.

Data passing through the cable interface line card is converted to an IF signal and then run through an upconverter to transform the signal to RF. This RF signal is then sent down the line to the user's cable modem. Downstream cable interface commands configure the frequency, symbol rate, compression, and modulation of the downstream signal.

An RF upconverter is also used for downstream RF frequency shifting. The upconverter in the Cisco CMTS has an Ethernet interface that allows the CMTS to be controlled remotely via SNMP. Two types of upconverters are commonly used with the Cisco CMTS:

- VCom HD4040 chassis (one) with 16 modules
- GI C6U upconverter units (two) with two modules each

RPR+

Route Processor Redundancy Plus. When two route processors (RPs) are installed in a Cisco uBR10012 router chassis, one RP acts as the active (primary) RP, and the other acts as a standby (backup) RP. If the active RP fails, or is removed from the system, the standby RP detects the failure and initiates a switchover. During a switchover, the standby RP assumes control of the router, connects with the network interfaces, and activates the local network management interface and system console.

SNMP

Simple Network Management Protocol. Network management protocol used almost exclusively in TCP/IP networks. SNMP provides a means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security.

Standby RP

Standby route processor (RP), also known as the secondary RP. The route processor (RP) that waits in protective support of the active or primary RP in the case of failure.

Upconverter

See RF Upconverter.

Upstream (US)

Set of frequencies used to send data from a subscriber (cable modem) to the headend (CMTS).

**Note**

Refer to [Internetworking Terms and Acronyms](#) for terms not included in this glossary.

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, TeleRouter, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0502R)

Copyright © 2003 Cisco Systems, Inc. All rights reserved.



Configuring PacketCable on the Cisco CMTS

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

Feature Specifications for PacketCable Operations

Feature History	
Release	Modification
12.2(8)BC2	This feature was introduced on the Cisco uBR7246VXR router.
12.2(11)BC1	Support was added for version 3 of the PacketCable DQoS specification (PKT-SP-DQOS-I03-020116) and for configuring the Event Message Element ID for the Cisco uBR7246VXR router.
12.2(11)BC2	Support was added for the packetcable authorize vanilla-docsis-mta command, which allows both PacketCable and non-PacketCable DOCSIS UGS service flows when PacketCable is enabled. The show packetcable global command was also enhanced to show whether non-PacketCable UGS service flows are enabled, and the T2 and T5 timers were removed from the display to conform to the requirements of the PacketCable Engineering Change Notice (ECN) 02148.
12.2(15)BC1	Support was added for the Cisco uBR10012 router. In addition, several debug packetcable commands have been added or enhanced.
12.2(15)BC2	Support was added for the show packetcable event command.
12.3(9a)BC	Supported was added for Packet Cable 1.0 with CALEA on the Cisco uBR10012 router and the Cisco uBR10-MC5X20S/U broadband processing engine (BPE).
Supported Platforms	
Cisco uBR7246VXR and Cisco uBR10012 universal broadband routers	

Finding Support Information for Platforms and Cisco IOS Software Images

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



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

Copyright © 2003 Cisco Systems, Inc. All rights reserved.

Contents

- [Prerequisites for PacketCable Operations, page 300](#)
- [Restrictions for PacketCable Operations, page 300](#)
- [Information About PacketCable Operations, page 301](#)
- [How to Configure PacketCable Operations, page 306](#)
- [Monitoring and Maintaining PacketCable Operations, page 314](#)
- [Configuration Examples, page 314](#)
- [Additional References, page 318](#)
- [Glossary, page 321](#)

Prerequisites for PacketCable Operations

- To support PacketCable operations on the Cisco uBR7246VXR universal broadband router, the router must be running Cisco IOS Release 12.2(8)BC2 or a later 12.2 BC release.
- To support PacketCable operations on the Cisco uBR10012 universal broadband router, the router must be running Cisco IOS Release 12.2(15)BC1 or a later 12.2 BC release.
- To support PacketCable 1.0 and the Communications Assistance for Law Enforcement Act (CALEA) intercept capabilities, a Cisco uBR7246VXR broadband router must be running Cisco IOS Release 12.2(11)BC2 or a later 12.2 BC release. A Cisco uBR10012 broadband router must be running Cisco IOS Release 12.2(15)BC1 or a later 12.2 BC release.

Restrictions for PacketCable Operations

- Cisco IOS Release 12.2(11)BC1 supports version 3 of the PacketCable DQoS specification (PKT-SP-DQOS-I03-020116).
- To avoid packet drops of voice calls, the Cisco CMTS should be using the default token bucket configuration (**cable downstream rate-limit token-bucket shaping**). Packet drops are guaranteed to occur when the **shaping** option is not used (**cable downstream rate-limit token-bucket**).
- Supports only embedded multimedia terminal adapter (E-MTA) clients. Standalone MTA (S-MTA) clients are not supported.
- PacketCable operations can be configured together with HCCP N+1 redundancy, but the PacketCable states are not synchronized between the Working and Protect interfaces. If a switchover occurs, existing voice calls continue, but when the user hangs up, PacketCable event messages are not generated because the Protect interface is not aware of the previous call states. However, new voice calls can be made and proceed in the normal fashion.
- The 200,000 Hz channel width cannot be used on upstreams that support PacketCable voice calls, or on any upstreams that use Unsolicited Grant Service (UGS) or UGS with Activity Detection (UGS-AD) service flows. Using this small a channel width with voice and other UGS/UGS-AD service flows results in calls being rejected because of “DSA MULTIPLE ERRORS”.

Information About PacketCable Operations

This section provides an overview and other information about PacketCable operations, the components of a PacketCable network, and how they interact with the other components of a DOCSIS cable networks.

- [Feature Overview, page 301](#)
- [PacketCable Network Components, page 301](#)
- [Dynamic Quality of Service, page 302](#)
- [Benefits, page 304](#)

Feature Overview

PacketCable is a program initiative from Cablelabs and its associated vendors to establish a standard way of providing packet-based, real-time video and other multimedia traffic over hybrid fiber-coaxial (HFC) cable networks. The PacketCable specification is built upon the Data-over-Cable System Interface Specifications (DOCSIS) 1.1, but it extends the DOCSIS protocol with several other protocols for use over noncable networks, such as the Internet and the public switched telephone network (PSTN).

This allows PacketCable to be an end-to-end solution for traffic that originates or terminates on a cable network, simplifying the task of providing multimedia services over an infrastructure composed of disparate networks and media types. It also provides an integrated approach to end-to-end call signaling, provisioning, quality of service (QoS), security, billing, and network management.

Cisco IOS Release 12.2(11)BC1 supports the PacketCable 1.0 specifications and the Communications Assistance for Law Enforcement Act (CALEA) intercept capabilities of the PacketCable 1.1 specifications.

PacketCable Network Components

A PacketCable network contains a number of components. Some components are the same as those that exist in a DOCSIS 1.1 network, while other components are new entities that create the end-to-end infrastructure that the PacketCable network needs to establish calls. Wherever possible, the PacketCable components and protocols build on existing protocols and infrastructures to simplify implementation and interoperability.

- **Cable modem (CM)**—A customer premises equipment (CPE) device that connects to a DOCSIS 1.0 or DOCSIS 1.1 cable network. All DOCSIS cable modems provide high-speed data connectivity to the Internet, while other cable modems can provide additional features, such as telephone connectivity.
- **Cable Modem Termination System (CMTS)**—A headend-based router that connects a DOCSIS cable network to the IP backbone network. The CMTS controls the DOCSIS 1.1 MAC layer and enforces the quality of service (QoS) limits that the cable operator guarantees to its subscribers. A typical CMTS services between several hundred and several thousand cable modems. The Cisco uBR7246VXR and Cisco uBR10012 routers operate as the CMTS in the PacketCable network.

**Note**

See the DOCSIS 1.1 specifications for information about CM and CMTS operations.

- **Multimedia terminal adapter (MTA)**—A CPE device that connects telephones and other end-user devices to the PacketCable network. The PacketCable specification defines two MTA types, an embedded MTA (E-MTA) and a standalone MTA (S-MTA). The E-MTA is an MTA integrated into a DOCSIS 1.1 cable modem, while the S-MTA is a separate MTA that requires a DOCSIS 1.1 cable modem to connect to the cable network.



Note Cisco IOS Release 12.2 BC supports only embedded MTA devices.

- **Call management server (CMS)**—A centrally located server that provides the signaling functions that allow MTAs to establish calls over the network. The CMS uses the Network-based call signaling (NCS) protocol to provide authentication and authorization, call routing, and support for special features such as three-way calling. A PacketCable network could have multiple CMS servers, depending on its size and complexity.



Note The CMS implements several protocols on top of the Common Open Policy Service (COPS) protocol to communicate with the rest of the PacketCable network.

- **Gate controller (GC)**—A server that controls the establishment of gates in the PacketCable network. A gate is a logical entity in the CMTS that ensures that a service flow is authorized for the QoS features it is requesting. A separate gate controls the upstream and downstream directions of a service flow. When a call is established, the GC instructs the CMTS to create each gate and supplies the set of authorized parameters for each gate, which the CMTS uses to authorize the QoS requests that the MTA is making for the call. The GC is also responsible for coordinating the creation of the two sets of gates at each end of the call so that the call can be authorized and established.



Note A PacketCable network can contain multiple GCs, although only one server at a time is in control of any particular call. Typically, the same workstation provides both the CMS and GC servers.

- **Record keeping server (RKS)**—Billing server that collects the information about each call as it is made. The RKS uses the Remote Authentication Dial-In User Service (RADIUS) protocol to collect the billing data from the CMTS and other PacketCable servers. The RKS generates a call data record (CDR) for every call and forwards that information to the appropriate application server at the service provider's data processing center for further processing.

Dynamic Quality of Service

A key feature of a PacketCable network is a dynamic quality of service (DQoS) capability that is similar to the dynamic services provided by DOCSIS 1.1. However, DOCSIS 1.1 DQoS authorizes and provisions services only in the cable network and does not reserve the resources needed to propagate a call from one endpoint to another across the network.

The PacketCable DQoS extends the DOCSIS 1.1 services across the entire network, so that resources can be dynamically authorized and provisioned from one endpoint to another. This prevents possible theft-of-service attacks and guarantees customers the services they are authorized to use.

**Note**

PacketCable 1.0 requires that DOCSIS 1.1 be used for resource reservation within the cable network for E-MTA clients. The PacketCable specifications allow the optional use of the Resource Reservation Protocol (RSVP) for S-MTA clients, but Cisco IOS Release 12.2(11)BC1 does not support RSVP for access reservations.

Two-Stage Resource Reservation Process

The PacketCable DQoS model uses a two-stage resource reservation process, in which resources are first reserved and then committed. This allows a bidirectional reservation process that ensures that resources are available at both endpoints of the connection before actually placing the call.

When an MTA makes a call request, the local CMTS communicates with the gate controller to authorize the call's resources. After the resources are authorized, the CMTS reserves the local resources while it negotiates with the remote end for the resources that are required at that end.

**Note**

The CMTS uses DOCSIS 1.1 Dynamic Service Addition (DSA) messages to reserve the resources, and then uses Dynamic Service Change (DSC) messages to commit the resources.

When all required resources are available, the local CMTS and remote CMTS both commit the resources, allowing traffic to flow. Usage accounting and billing do not begin until the remote MTA picks up and the call is actually in progress.

The DQoS model ensures that both endpoints of a call, as well as the backbone network, have reserved the same bandwidth, and that the bandwidth is reserved only while the call is in progress. When a call terminates, all portions of the network can release the call's resources and make them available for other users.

Making a Call Using DQoS

DOCSIS 1.1 networks use service flows to implement different QoS policies, but service flows exist only within the cable network. To control the service flows and to extend them across the entire network, a PacketCable network creates and maintains "gates."

A gate is a logical entity created on the CMTS at each side of a connection that authorizes and establishes a particular DQoS traffic flow. The CMTS communicates with the gate controller to coordinate the creation of matching gates at each side of the connection.

Gates are unidirectional, so separate gates are required for the downstream and upstream traffic flows. The same gate ID, however, is usually used for the downstream and upstream gates for a call. Each CMTS maintains its own set of gates, so a bidirectional traffic flow requires four gates to be created, two gates on the local CMTS and two gates on the remote CMTS.

For a typical call, gates progress through the following stages to create a DQoS traffic flow:

1. The local MTA makes a call request, and the gate controller sends a Gate-Allocation command to the CMTS, which creates a gate in response and puts it into the Allocated state.
2. The call management server, which might be the same server as the gate controller, parses the call request to translate the destination phone number into the appropriate destination gateway.
3. The gate controller verifies that the MTA making the call request is authorized for the required resources and sends a Gate-Set command to the CMTS, which puts the gate into the Authorized state.

4. The CMTS on each side of the connection reserves the local resources needed for the call, putting the gate into the Reserved state.
5. As the remote CMTS and local CMTS perform gate coordination, their respective gates get put into the Local_Committed and Remote_Committed states.
6. When both sides have reserved all required resources, each CMTS puts its gates into the Committed state, allowing traffic to flow.

Benefits

The PacketCable feature offers the following benefits to service providers and their customers:

Integrated Services on a Cable Network

PacketCable allows cable operators the ability to offer multimedia, real-time services, in addition to data connectivity, across their entire network. These services could include basic telephony with lifeline support, as well as telephony that offers competitive extended calling services. Operators can deploy new services while heavily leveraging their existing network infrastructures.

The widespread use of IP as the standard transport mechanism for data networks today is enabling many advanced Internet applications such as multimedia e-mail, real-time chat, streaming media (including music and video), and videoconferencing. The PacketCable initiative provides the network architecture for a cable operator to deliver these services quickly and economically.

Standardized Provisioning

PacketCable provides a standardized, efficient method to provision IP services for individual subscribers, because PacketCable specifications define a uniform, open, and interoperable network. Cable operators are assured of standardized provisioning and the associated lower costs of deployment.

Interoperability

Customer premises equipment (CPE) devices account for a major portion of the capital expense in deploying a VoIP solution at a cable plant. The PacketCable specifications ensure that vendors will build MTA clients that support the voice and other services that cable operators plan to deploy. Because these CPE devices are based on existing DOCSIS-compliant cable modems, time and cost of development is minimized.

Interoperability with the other components of the PacketCable network is also guaranteed because of the standards-based approach to the specifications. Any PacketCable-certified component will be able to interoperate within a network that conforms to the PacketCable standards.

Secure Architecture

Because PacketCable is built upon the security features available in DOCSIS 1.1, cable operators will be assured of networks that are secure from end to end, with a high standard of security that prevents the most common theft-of-service attacks. The comprehensive, standards-based PacketCable specifications are designed to create a network that is as secure as the public switched telephone network (PSTN).

CALEA Support

The PacketCable architecture was designed to accommodate the 1994 Communications Assistance for Law Enforcement Act (CALEA), which requires telecommunications carriers to assist law-enforcement agencies in conducting court-ordered electronic surveillance. PacketCable networks will be able to provide the two types of information that a carrier must provide, depending on the type of court order:

- Call-identifying information—The carrier must provide the call-identifying information for calls to or from an intercept target. For telephone calls, this information includes the phone numbers called by the target or calling the target.
- Call content—The carrier must provide the content of calls to or from an intercept target. For telephone calls, this real-time content is the voice conversation.

How to Configure PacketCable Operations

See the following sections for configuration tasks for the PacketCable feature. Each task is required unless otherwise identified as optional.

- [Enabling PacketCable Operation, page 306](#)
- [Disabling PacketCable Operation, page 307](#)
- [Configuring PacketCable Operation \(Optional\), page 308](#)
- [Enabling Both PacketCable and Non-PacketCable UGS Service Flows, page 309](#)
- [Verifying PacketCable Configuration, page 311](#)
- [Configuring RADIUS Accounting for RKS Servers, page 311](#)

Enabling PacketCable Operation

To enable PacketCable operation, use the following commands beginning in user EXEC mode. This is a required procedure.

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `packetcable`
4. `exit`

DETAILED STEPS

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

	Command or Action	Purpose
Step 3	packetcable Example: Router(config)# packetcable Router(config)#	Enables PacketCable operation on all cable interfaces.
Step 4	exit Example: Router(config)# exit Router#	Exits global configuration mode.

Disabling PacketCable Operation

To disable PacketCable operation, use the following commands beginning in user EXEC mode. This procedure is required only when you no longer want the Cisco CMTS to support PacketCable signaling.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **no packetcable**
4. **exit**

DETAILED STEPS

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

	Command or Action	Purpose
Step 3	no packetcable Example: Router(config)# no packetcable Router(config)#	Disables PacketCable operation on all cable interfaces.
Step 4	exit Example: Router(config)# exit Router#	Exits global configuration mode.

Configuring PacketCable Operation (Optional)

To configure the different parameters that affect PacketCable operations, use the following commands beginning in user EXEC mode. All of these procedures are optional, because each parameter is set to a default that is appropriate for typical PacketCable operations.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **packetcable element-id** *n*
4. **packetcable gate maxcount** *n*
5. **packetcable timer T0** *timer-value*
6. **packetcable timer T1** *timer-value*
7. **packetcable timer T2** *timer-value*
8. **packetcable timer T5** *timer-value*
9. **exit**

DETAILED STEPS

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

	Command or Action	Purpose
Step 3	packetcable element-id <i>n</i> Example: Router(config)# packetcable element-id 23 Router(config)#	Configures the Event Message Element ID for the Cisco CMTS. The valid range for <i>n</i> is 0 to 99999. If you do not manually configure the Element ID, the CMTS defaults to a random value between 0 and 99,999 when PacketCable operations are enabled.
Step 4	packetcable gate maxcount <i>n</i> Example: Router(config)# packetcable gate maxcount 524288 Router(config)#	Sets the maximum number of gate IDs to be allocated in the gate database on the Cisco CMTS. The valid range for <i>n</i> is 1 to 1048576, with a default value of 1048576 (which is 1024 * 1024).
Step 5	packetcable timer T0 <i>timer-value</i> Example: Router(config)# packetcable timer T0 40000 Router(config)#	Sets the T0 timer in milliseconds. The valid range is 1 to 1,000,000,000 milliseconds, with a default value of 30000 milliseconds (30 seconds).
Step 6	packetcable timer T1 <i>timer-value</i> Example: Router(config)# packetcable timer T1 300000 Router(config)#	Sets the T1 timer in milliseconds. The valid range is 1 to 1,000,000,000 milliseconds, with a default value of 200000 milliseconds (200 seconds).
Step 7	packetcable timer T2 <i>timer-value</i> Example: Router(config)# packetcable timer T2 3000 Router(config)#	Sets the T2 timer in milliseconds. The valid range is 1 to 1,000,000,000 milliseconds, with a default value of 2000 milliseconds (2 seconds).
Step 8	packetcable timer T5 <i>timer-value</i> Example: Router(config)# packetcable timer T5 1000 Router(config)#	Sets the T5 timer in milliseconds. The valid range is 1 to 1,000,000,000 milliseconds, with a default value of 500 milliseconds. Note The T5 timer should always be several times smaller than the T2 timer.
Step 9	exit Example: Router(config)# exit Router#	Exits global configuration mode.

Enabling Both PacketCable and Non-PacketCable UGS Service Flows

By default, when PacketCable operations are enabled using the **packetcable** command, cable modems must follow the PacketCable protocol when requesting Unsolicited Grant Service (UGS) service flows. This prevents DOCSIS cable modems that do not support PacketCable operations from using DOCSIS-style UGS service flows.

If you have a mixed network that contains both PacketCable and non-PacketCable DOCSIS CMs, you can use the **packetcable authorize vanilla-docsis-mta** command to enable both types of UGS service flows. This is an optional procedure.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **packetcable**
4. **packetcable authorize vanilla-docsis-mta**
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable Router#	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal Router(config)#	Enters global configuration mode.
Step 3	packetcable Example: Router(config)# packetcable Router(config)#	Enables PacketCable operations.
Step 4	packetcable authorize vanilla-docsis-mta Example: Router(config)# packetcable authorize vanilla-docsis-mta Router(config)#	Enables the use of DOCSIS-style UGS service flow requests.
Step 5	exit Example: Router(config)# exit Router#	Exits global configuration mode.

**Tip**

Use the **show packetcable global** command to display whether non-PacketCable UGS service flows have been enabled.

Verifying PacketCable Configuration

To verify the PacketCable configuration, use the **show packetcable global** command in privileged EXEC mode, which displays whether PacketCable operations are enabled, as well as the values for the Element ID, the maximum number of gates, and the different CMTS-based DQoS timers.

```
Router# show packetcable global

Packet Cable Global configuration:
Enabled      : Yes
Element-ID: 12456
Max Gates   : 1048576
Allow non-PacketCable UGS
Default Timer value -
  T0        : 30000 msec
  T1        : 300000 msec

Router#
```

Configuring RADIUS Accounting for RKS Servers

To configure the Cisco CMTS so that it can communicate with the RKS servers using the RADIUS protocol, use the following commands beginning in user EXEC mode. This is a required procedure.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa group server radius *group-name***
5. **server {*hostname* | *ip-address*} [auth-port *udp-port*] [acct-port *udp-port*]**
6. **exit**
7. **aaa accounting network default start-stop group radius group *group-name***
8. **radius-server host {*hostname* | *ip-address*} [auth-port *port-number*] [acct-port *port-number*] [timeout *seconds*] [retransmit *retries*] key 0000000000000000**
9. **radius-server vsa send accounting**
10. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable Router#	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal Router(config)#	Enters global configuration mode.
Step 3	aaa new-model Example: Router(config)# aaa new-model Router(config)#	Enables the authentication, authorization, and accounting (AAA) access control model.
Step 4	aaa group server radius group-name Example: Router(config)# aaa group server radius packetcable Router(config-sg-radius)#	Creates a group of RADIUS servers for authentication and enters RADIUS group configuration mode. The value of <i>group-name</i> is a unique, arbitrary string that identifies this group.
Step 5	server {hostname ip-address} [auth-port udp-port] [acct-port udp-port] Example: Router(config-sg-radius)# server radius-server1 Router(config-sg-radius)#	Specifies the host name or IP address for the RADIUS server that is providing the RKS services. You can optionally specify the following: • acct-port udp-port = UDP port for the accounting server. The valid range is 0 to 65536, with a default of 1812. • auth-port udp-port = UDP port for the authentication server. The valid range is 0 to 65536, with a default of 1813. Note Repeat this command as needed to enter multiple RADIUS servers. The Cisco CMTS uses the servers in the order given with this command.
Step 6	exit Example: Router(config-sg-radius)# exit Router(config)#	Exits RADIUS group configuration mode.

	Command or Action	Purpose
Step 7	aaa accounting network default start-stop group radius group <i>group-name</i> Example: Router(config)# aaa accounting network default start-stop group radius group packetcable Router(config)#	Enables AAA services using the group of RADIUS servers that are defined in the previously created group. The <i>group-name</i> parameter should be the same name specified in Step 4 .
Step 8	radius-server host {hostname ip-address} [auth-port port-number] [acct-port port-number] [timeout seconds] [retransmit retries] key 0000000000000000 Example: Router(config)# radius-server host radius-server1 key 0000000000000000 Router(config)#	Specifies a RADIUS host. Use the same values for <i>hostname</i> or <i>ip-address</i> as for one of the servers specified in Step 5 . If you also specified the auth-port or acct-port values in Step 5 , you must also specify those here, as well. The key value is required and must be 16 ASCII zeros, as shown. You can optionally specify the following: • timeout seconds = Time interval (in seconds) that the router waits for the RADIUS server to reply before retransmitting. The valid range is 1 to 1000, with a default of 5. • retransmit retries = Number of times a RADIUS request is re-sent to a server, if that server is not responding or responding slowly. The valid range is 1 to 100, with a default of 3. Note Repeat this command for each RADIUS server entered in Step 5 .
Step 9	radius-server vsa send accounting Example: Router(config)# radius-server vsa send accounting Router(config)#	Configures the Cisco CMTS to recognize and use accounting-related vendor-specific attributes (VSA).
Step 10	exit Example: Router(config)# exit Router#	Exits global configuration mode.

Monitoring and Maintaining PacketCable Operations

To display and maintain information about current PacketCable operations, use one or more of the following commands:

Command	Purpose
Router# show packetcable gate counter commit	Displays the total number of gates that the Cisco CMTS has put into the Committed state since the Cisco CMTS was last reset or since the counter was last cleared.
Router# clear packetcable gate counter commit	Clears the total number of gates that the Cisco CMTS has put into the Committed state, setting the counter to zero.
Router# show packetcable gate [downstream upstream] {summary gate-id}	Displays information about one or more gates that are currently active on the Cisco CMTS. You can display a summary for all currently active gates, for all downstream or all upstream gates, or you can display detailed information about a specific gate. • downstream = Displays only gates for the downstream direction. • upstream = Displays only gates for the upstream direction. • summary = Displays summary information for the gates, including the gate ID, subscriber IP address, gate controller IP address, and current state. • gate-id = Displays detailed information for a specific gate ID. Both downstream and upstream gates are displayed unless you also specify either the downstream or upstream options.
Router# show packetcable event {df-group radius-server rks-group}	Displays information the PacketCable event message (EM) servers: • df-group—Displays information about the Communications Assistance for Law Enforcement Act (CALEA) Delivery Function (DF) server groups that are configured on the router. • radius-server—Displays information about the EM Remote Authentication Dial In User Service (RADIUS) servers that are configured on the router. • rks-group—Displays information about the Record Keeping Server (RKS) groups that are configured on the router.

Configuration Examples

This section provides the following configuration examples:

- [Typical PacketCable Configuration](#)

Typical PacketCable Configuration

This section provides a typical configuration for a Cisco uBR7246VXR universal broadband router that has been configured for PacketCable operations, using default parameters. To use this configuration, you must change the IP addresses for the RADIUS and RKS servers to match the addresses for the servers in your network.

```

!
version 12.2
no parser cache
no service pad
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
no service password-encryption
service internal
service udp-small-servers max-servers no-limit
service tcp-small-servers max-servers no-limit
!
hostname Router
!
no logging rate-limit
aaa new-model
!
!
aaa group server radius a
 server 10.9.62.12 auth-port 1813 acct-port 1812
 server 10.9.62.13 auth-port 1813 acct-port 1812
!
aaa accounting network default start-stop group radius group a
aaa session-id common
enable password <delete>
!
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 5 request 0 16 2 8 qpsk scrambler 152 no-diff 64 fixed uw16
cable modulation-profile 5 initial 5 34 0 48 qpsk scrambler 152 no-diff 128 fixed uw16
cable modulation-profile 5 station 5 34 0 48 qpsk scrambler 152 no-diff 128 fixed uw16
cable modulation-profile 5 short 6 78 7 8 16qam scrambler 152 no-diff 144 shortened uw16
cable modulation-profile 5 long 8 220 0 8 16qam scrambler 152 no-diff 160 shortened uw16
cable qos profile 5 max-burst 1200
cable qos profile 5 max-downstream 2000
cable qos profile 5 max-upstream 128
cable qos profile 5 priority 5
cable qos profile 5 privacy
cable qos profile 7 guaranteed-upstream 87
cable qos profile 7 max-upstream 87
cable qos profile 7 privacy
no cable qos permission create
no cable qos permission update
cable qos permission modems
cable qos permission enforce 5
cable time-server
no cable privacy accept-self-signed-certificate
ip subnet-zero
!
!
no ip domain-lookup
ip domain-name cisco.com
ip host tftp 10.8.8.8

```

```

ip host cnr 10.9.62.17
!
packetcable
packetcable element-id 12456
!
!
!
interface Tunnel0
 ip address 10.55.66.3 255.255.255.0
 load-interval 30
 tunnel source FastEthernet1/0
 tunnel destination 172.27.184.69
!
interface Tunnel10
 ip address 10.0.1.1 255.255.0.0
!
interface FastEthernet0/0
 ip address 10.9.60.10 255.255.0.0
 no ip redirects
 no ip mroute-cache
 full-duplex
!
interface FastEthernet1/0
 ip address 172.22.79.44 255.255.254.0
 no ip redirects
 no ip mroute-cache
 full-duplex
!
interface Cable3/0
 ip address 10.3.1.33 255.255.255.0 secondary
 ip address 10.4.1.1 255.255.255.0 secondary
 ip address 10.4.1.33 255.255.255.0 secondary
 ip address 10.3.1.1 255.255.255.0
 ip helper-address 10.9.62.17
 load-interval 30
 no keepalive
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream frequency 55500000
 cable upstream 0 modulation-profile 2
 no cable upstream 0 shutdown
 cable upstream 1 frequency 12000000
 cable upstream 1 power-level 0
 cable upstream 1 channel-width 3200000
 cable upstream 1 data-backoff automatic
 cable upstream 1 modulation-profile 2
 cable upstream 1 shutdown
 cable upstream 2 frequency 16000000
 cable upstream 2 power-level 0
 cable upstream 2 channel-width 3200000
 cable upstream 2 data-backoff automatic
 cable upstream 2 modulation-profile 2
 no cable upstream 2 shutdown
 cable upstream 3 frequency 20000000
 cable upstream 3 power-level 0
 cable upstream 3 channel-width 3200000
 cable upstream 3 data-backoff automatic
 cable upstream 3 modulation-profile 2
 no cable upstream 3 shutdown
 cable upstream 4 frequency 24000000
 cable upstream 4 power-level 0
 cable upstream 4 channel-width 3200000
 cable upstream 4 data-backoff automatic

```

```
no cable upstream 4 shutdown
cable upstream 5 frequency 28000000
cable upstream 5 power-level 0
cable upstream 5 channel-width 3200000
cable upstream 5 data-backoff automatic
cable upstream 5 modulation-profile 2
no cable upstream 5 shutdown
cable dhcp-giaddr policy
!
router eigrp 48849
 network 1.0.0.0
 network 10.0.0.0
 auto-summary
 no eigrp log-neighbor-changes
!
ip default-gateway 10.9.0.1
ip classless
ip route 0.0.0.0 0.0.0.0 172.22.78.1
ip route 10.8.0.0 255.255.0.0 10.9.0.1
ip route 192.168.80.0 255.255.255.0 Tunnel0
ip route 192.168.80.0 255.255.255.0 172.27.184.69
ip route 10.255.254.254 255.255.255.255 10.9.0.1
no ip http server
ip pim bidir-enable
!
!
cdp run
!
!
radius-server host 10.9.62.12 auth-port 1813 acct-port 1812 key 0000000000000000
radius-server retransmit 3
radius-server vsa send accounting
!
line con 0
 exec-timeout 0 0
 privilege level 15
line aux 0
line vty 0 4
 session-timeout 33
 exec-timeout 0 0
 password <deleted>
!
ntp clock-period 17179976
ntp server 1.9.35.8
end
```

Additional References

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

Related Documents

Related Topic	Document Title
AAA and RADIUS Configuration	For complete information on configuring the AAA and RADIUS servers, which are required for communication with the RKS servers, see the “Authentication, Authorization, and Accounting (AAA)” chapter in the <i>Cisco IOS Security Configuration Guide</i>, Release 12.2 at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/index.htm
Cable Command Reference Guide	For syntax and usage information on the cable-specific commands used in this chapter, see the “Cisco Cable Modem Termination System Commands” chapter of the <i>Cisco Broadband Cable Command Reference Guide</i> at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/cable/bbcmref/bbcmts.htm
DHCP Configuration	To configure the DHCP server onboard the Cisco CMTS, see the “Configuring DHCP” chapter in the “IP Addressing and Services” section of the <i>Cisco IOS IP and IP Routing Configuration Guide</i>, Release 12.2 at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipr_c/index.htm For information on all DHCP commands, see the “DHCP Commands” chapter in the <i>Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services</i>, Release 12.2 at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipras_r/index.htm

Related Topic	Document Title
DOCSIS 1.1	To configure the Cisco uBR7200 series router for DOCSIS 1.1 operations, see the <i>DOCSIS 1.1 for Cisco uBR7200 Series Universal Broadband Routers</i> document at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121limit/121cx/docsis11.htm
NTP or SNTP Configuration	To configure the Cisco CMTS to use Network Time Protocol (NTP) or Simple Network Time Protocol (SNTP) to set its system clock, see the “Performing Basic System Management” chapter in the “System Management” section of the <i>Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2</i> , at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/ffun_c/fcfprt3/fcf012.htm

Standards

Standards ¹	Title
ITU X.509 V3	<i>International Telecommunications Union (ITU) X.509 Version 3.0 standard</i>
PKT-EM-I03-011221	<i>PacketCable™ Event Message Specification</i>
PKT-SP-DQOS-I03-020116	<i>PacketCable™ Dynamic Quality-of-Service Specification</i>
PKT-SP-EC-MGCP-I04-011221	<i>PacketCable™ Network-Based Call Signaling Protocol Specification</i>
PKT-SP-ESP-I01-991229	<i>PacketCable™ Electronic Surveillance Specification</i>
PKT-SP-ISTP-I02-011221	<i>PacketCable™ Internet Signaling Transport Protocol (ISTP) Specification</i>
PKT-SP-PROV-I03-011221	<i>PacketCable™ MTA Device Provisioning Specification</i>
PKT-SP-SEC-I05-020116	<i>PacketCable™ Security Specification</i>
PKT-TR-ARCH-V01-991201	<i>PacketCable™ 1.0 Architecture Framework Technical Report</i>
Note The PacketCable 1.0 specifications are available on the Packetcable website at http://packetcable.com/specifications.html .	
SP-BPI+-I08-020301	<i>Baseline Privacy Interface Plus Specification</i>
SP-RFIV1.1-I09-020830	<i>Data-over-Cable Service Interface Specifications Radio Frequency Interface Specification, version 1.1</i>

1. Not all supported standards are listed.

MIBs

MIBs ¹	MIBs Link
No new or changed MIBs are supported by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

1. Not all supported MIBs are listed.

RFCs

RFCs ¹	Title
RFC 1321	<i>The MD5 Message-Digest Algorithm</i>
RFC 1510	<i>The Kerberos Network Authentication Service (V5)</i>
RFC 2138	<i>Remote Authentication Dial In User Service (RADIUS)</i>
RFC 2205	<i>Resource ReSerVation Protocol (RSVP)</i>
RFC 2327	<i>SDP: Session Description Protocol</i>
RFC 2748	<i>The COPS (Common Open Policy Service) Protocol</i>

1. Not all supported RFCs are listed.

Technical Assistance

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

Glossary

- **AAA**—Authentication, authorization, and accounting.
- **CM**—Cable modem.
- **CMS**—Call management server.
- **CMTS**—Cable Modem Termination System.
- **COPS**—Common Open Policy Service Protocol.
- **DCS**—Distributed call signaling.
- **DQoS**—Dynamic quality of service
- **E-MTA**—Embedded multimedia terminal adapter. An MTA device that is integrated with a cable modem.
- **Element ID**—Unique ID that is statically assigned to every PacketCable element within a PacketCable network or domain.
- **GC**—Gate controller.
- **Gate**—Virtual policy control entity that controls a service flow's access to QoS services.
- **MTA**—Multimedia terminal adapter. A CPE device that implements DCS or NCS signaling and provides an interface that allows customer equipment to access PacketCable services.
- **NCS**—Network-based call signaling.
- **QoS**—Quality of service.
- **RADIUS**—Remote Authentication Dial-In User Service.
- **RKS**—Record Keeping Server.
- **RSVP**—Resource reservation protocol.
- **SDP**—Session Description Protocol.

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, TeleRouter, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0502R)



Point-to-Point Protocol over Ethernet Termination on the Cisco CMTS

This chapter describes the PPPoE Termination feature, which allows service providers to extend their existing PPP dial-up provisioning systems to users on cable networks by encapsulating the PPP packets within Ethernet MAC frames.

Feature Specifications for PPPoE Termination

Feature History

Release	Modification
Release 12.1(5)T	This feature was introduced for the Cisco uBR7200 series routers. Note The Cisco IOS Release 12.1T and 12.2T trains are no longer supported for the Cisco uBR7200 series routers.
Release 12.2(4)BC1a	This feature was supported on the 12.2BC train for the Cisco uBR7100 series and Cisco uBR7246VXR routers.
Release 12.2(8)BC1	Support was added for SNMP support with the CISCO-PPPOE-MIB.
Release 12.2(8)BC2	Support was added for bundled cable interfaces.

Supported Platforms

Cisco uBR7100 series, Cisco uBR7246VXR router



Note

The PPPoE Termination feature is not supported on the Cisco uBR10012 universal broadband router in any Cisco IOS software release. The PPPoE Termination is also not supported on any Cisco CMTS router when running Cisco IOS Release 12.1 EC.

Finding Support Information for Platforms and Cisco IOS Software Images

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

Contents

This document includes the following major sections:

- [Prerequisites for PPPoE Termination, page 324](#)
- [Restrictions for PPPoE Termination, page 324](#)
- [Information About PPPoE Termination, page 325](#)
- [How to Configure the PPPoE Termination Feature, page 327](#)
- [Monitoring the PPPoE Termination Feature, page 342](#)
- [Configuration Examples for PPPoE Termination, page 342](#)
- [Additional References, page 348](#)
- [Glossary, page 350](#)

Prerequisites for PPPoE Termination

The PPPoE Termination feature has the following prerequisites:

- The PPPoE Termination feature is supported only on the Cisco uBR7100 series and Cisco uBR7246VXR universal broadband routers.
- The Cisco CMTS router must be running Cisco IOS Release 12.2(4)BC1a or later release. In addition, to support the PPPoE Termination feature, the software image name must include the IP+ feature set (the letters “i” and “s” must appear in the software image name).
- To support PPPoE Termination on bundled cable interfaces, the Cisco CMTS router must be running Cisco IOS Release 12.2(8)BC2 or later release.
- Client software must support the PPPoE Termination protocol. If the computer operating system does not include such support, the user can use client software such as WinPoet.
- If planning on a large number of PPPoE sessions and traffic, increase the size of the packet hold queues on the WAN interfaces (ATM, DPT, Gigabit Ethernet, etc.), using the **hold-queue packet-size {in | out}** command. For example:

```
Router(config)# interface gigabitethernet 1/0
Router(config-if)# hold-queue 4096 in
Router(config-if)# hold-queue 4096 out
Router(config-if)#
```

Restrictions for PPPoE Termination

The PPPoE Termination feature has the following restrictions and limitations:

- The PPPoE Termination feature is only supported on the Cisco uBR7100 series routers and Cisco uBR7246VXR router, using Cisco IOS Release 12.2(4)BC1a or later. It is not supported on the Cisco uBR10012 router.
- The PPPoE Termination feature is not supported on any Cisco CMTS router when using Cisco IOS Release 12.1 EC.
- PPPoE Forwarding is not supported on any Cisco CMTS.

- [Table 4](#) shows the absolute maximum number of PPPoE sessions supported on the Cisco uBR7100 series routers, and on the Cisco uBR7246VXR router when using different processor cards.

Table 4 *Absolute Maximum Number of PPPoE Sessions*

Processor	Absolute Maximum Number of PPPoE Sessions
Cisco uBR7100 series	4000
NPE-225	4000
NPE-300 ¹	4000
NPE-400	8000
NPE-G1	10000

1. The NPE-300 processor reached its end-of-life milestone on August 15, 2001.

**Note**

The maximum number of active, simultaneous PPPoE sessions is much less (approximately 600 to 800), depending on the number of amount of memory onboard the processor card, the type of cable interface cards being used, the bandwidth being consumed by each user, and the router's configuration.

Information About PPPoE Termination

This section describes the PPPoE Termination feature:

- [Feature Overview, page 325](#)
- [Benefits, page 326](#)

Feature Overview

The Point-to-Point Protocol over Ethernet (PPPoE) feature supports PPPoE on cable interfaces, allowing service providers to extend their existing PPP dial-up provisioning systems to users on cable networks. When PPPoE Termination is enabled, the Cisco CMTS encapsulates PPP packets in Ethernet frames within PPPoE sessions.

When the Cisco CMTS receives PPPoE traffic from PPPoE sessions that are initiated by the user's PC, the Cisco CMTS either terminates the PPPoE sessions on the cable interface or transmits the PPPoE traffic through a secure tunnel connection, depending on the Cisco CMTS configuration. The following are the most typical configurations:

- Internet access—For residential customers and other users who want only basic Internet access, traffic is sent out on the WAN interface as standard IP packets. The service provider can use the same provisioning systems as they use for their dial-up users and other broadband users. The PPPoE session exists only between the cable modem and Cisco CMTS, simplifying network management and configuration.
- Secure corporate access—For businesses or telecommuters, traffic is forwarded over a Layer 2 point-to-point Tunneling Protocol (L2TP) tunnel to a L2TP network server (LNS) to create secure corporate intranet access. Cable modem users can access company resources as if they were directly connected to the corporate network, without compromising network security. This tunnel can be built over whatever interface is being used with the corporate site (Ethernet, ATM, and so forth).

When using the L2TP tunnel configuration, the Cisco CMTS acts as the L2TP Access Concentrator (LAC), or Network Access Server (NAS). The endpoint of the tunnel is the LNS, which can be a router such as a Cisco 6400 Carrier-Class Broadband Aggregator.

When the cable modem, acting as a bridge, receives its PPPoE session traffic, it forwards the traffic on to the hosts and other customer premises equipment (CPE) devices that are connected behind it. Users at these hosts or CPE devices can use standard PPP to log on to the cable network and obtain their IP addresses and other network information. Users can automate this procedure by using a router that supports PPPoE or by using standard PPPoE software, such as WinPoet.

User names and passwords can be included in the Cisco CMTS configuration, or the service provider can use the same Remote Authentication Dial-In User Service (RADIUS) authentication servers as they use for their dial-up and digital subscriber line (DSL) users. For example, the Cisco Subscriber Registration Center (CSRC) provides an Access Registrar that provides RADIUS server authentication.

The PPPoE Termination feature supports simultaneous use of PPPoE clients and Dynamic Host Configuration Protocol (DHCP) clients behind the same cable modems. Subscribers can use PPPoE for their initial log on to the cable network, and then use DHCP to allow their other PCs and other hosts to obtain IP addresses for network access.

**Note**

The Cisco CMTS routers do not support PPPoE Forwarding, which receives PPPoE packets from an incoming interface and forwards them out on an outgoing interface. The Cisco uBR7100 series routers do automatically forward PPPoE traffic when configured for MxU bridging mode (which is supported only on Cisco IOS Release 12.1 EC), but this is a consequence of the bridging configuration and not due to any PPPoE support.

Benefits

The PPPoE Termination feature provides the following benefits to cable service providers and their partners and customers:

- PPPoE complements and does not interfere with the standard DOCSIS registration and authentication procedures that are used for cable modems.
- PPPoE can be used on existing customer premise equipment, by extending the PPP session over the bridged Ethernet LAN to the PC (host).
- PPPoE preserves the point-to-point session used by ISPs in a dial-up model, without requiring an intermediate set of IP communications protocols.
- Service providers can use their existing dial-up PPP provisioning and authentication systems for users on the cable network.
- PPPoE supports the security features, such as Challenge Handshake Authentication Protocol (CHAP) and Password Authentication Protocol (PAP), that are built into PPP systems.
- Service providers can support both PPPoE clients and DHCP-based hosts behind the same cable modem.

How to Configure the PPPoE Termination Feature

This section describes the following tasks that are needed to implement the PPPoE Termination feature. All procedures are required, depending on the router's configuration.

- [Enabling VPDN Operations on the Cisco CMTS, page 327](#)
- [Configuring a Virtual Template on the Cisco CMTS, page 329](#)
- [Configuring a VPDN Group for PPPoE Sessions, page 332](#)
- [Configuring a VPDN Group for L2TP Tunnel Initiation on the Cisco CMTS, page 334](#)
- [Enabling PPPoE on a Cable Interface, page 336](#)
- [Configuring a Cisco Router as LNS, page 338](#)
- [Clearing PPPoE Sessions, page 340](#)
- [Enabling SNMP Traps for Active PPPoE Sessions, page 341](#)

Enabling VPDN Operations on the Cisco CMTS

Use the following commands, starting in user EXEC mode, to enable virtual private dialup network (VPDN) operations on the Cisco CMTS router that is acting an L2TP access concentrator (LAC). This procedure must be done before performing any of the other configuration procedures.

**Note**

This procedure also must be performed on the Cisco router that is acting as the L2TP network server (LNS).

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **buffers small {initial | max-free | permanent} 1024**
4. **vpdn enable**
5. **vpdn logging**
6. **username *user-name* password {0 | 7} *password***
7. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable Router#	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal Router(config)#	Enters global configuration mode.
Step 3	buffers small {initial max-free permanent} 1024 Example: Router(config)# buffers small initial 1024 Router(config)# buffers small max-free 1024 Router(config)# buffers small permanent 1024 Router(config)#	(Optional) Increases the size of the buffers on the router that are used for small packets to account for the larger number of keepalive packets that are sent during PPPoE sessions. Note Repeat this command for each type of small packet buffers.
Step 4	vpdn enable Example: Router(config)# vpdn enable Router(config)#	Enables virtual private dial-up networking (VPDN).
Step 5	vpdn logging Example: Router(config)# vpdn logging Router(config)#	(Optional) Enable logging for VPDN operations. Logging is automatically disabled by default (no vpdn logging) when you enable VPDN. Use this command to enable logging.
Step 6	username user-name password [level] password Example: Router(config)# username pppoe-user1@client.com password 0 pppoe-password Router(config)#	Specifies a username and password for each user to be granted PPPoE access: <i>user-name</i> = Username that the user uses to log in. <i>level</i> = (Optional) Encryption level for the password. The valid values are 0 (default, the following password is not encrypted) and 7 (the following password is encrypted—this option is typically used only when cutting and pasting configurations from other routers). <i>password</i> = Password that the above user must use to log in and create a PPPoE user session. Note This step is not required if you are using an external server, such as a RADIUS server, to perform user authentication.

	Command or Action	Purpose
Step 7	exit	Exits global configuration mode.
	Example: Router(config)# exit Router#	

Configuring a Virtual Template on the Cisco CMTS

Use the following commands, starting in user EXEC mode, to create and configure a virtual template on the Cisco CMTS router when it is acting as a LAC. This procedure is required because the Cisco CMTS uses the virtual template to configure the virtual interfaces it creates for each individual PPPoE session.



Note

At least one virtual template must be created on the router to support PPPoE sessions from cable modem users.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface virtual-template** *number*
4. **ip unnumbered** *interface*
5. **ip mtu 1492**
6. **keepalive** [*period* [*retries*]]
7. **peer default ip address pool** *name*
8. **ppp authentication** { **chap** | **ms-chap** | **pap** }
9. **ppp timeout authentication** *response-time*
10. **ppp timeout retry** *timeout*
11. **no logging event link-status**
12. **no cdp enable**
13. **exit**
14. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable Router#	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal Router(config)#	Enters global configuration mode.
Step 3	interface virtual-template <i>number</i> Example: Router(config)# interface virtual-template 1 Router(config-if)#	Select the number of the virtual-template interface to be configured and enters interface configuration mode. Note You can create up to 200 virtual interfaces on each router.
Step 4	ip unnumbered <i>interface</i> Example: Router(config-if)# ip unnumbered Ethernet2/0 Router(config-if)#	Enables the virtual template interfaces to process IP packets by using the IP address of the specified interface, as opposed to assigning a unique IP address to each virtual interface.
Step 5	ip mtu 1492 Example: Router(config-if)# ip mtu 1492 Router(config-if)#	Configures the maximum transmission unit (MTU) size to 1492 bytes to allow for the eight additional header bytes used by the PPP and PPPoE encapsulation.
Step 6	keepalive <i>period</i> [<i>retries</i>] Example: Router(config-if)# keepalive 60 10 Router(config-if)#	(Optional) Specifies how often and how many times the router should send keepalive messages on the virtual interface without receiving a response before bringing down the tunnel protocol and ending that particular PPPoE session. <i>period</i> = Specifies how long, in seconds, the router should send a keepalive message and wait for a response. The valid range is 0 to 32767 seconds, with a default of 10. <i>retries</i> = (Optional) Specifies the number of times the router will resend a keepalive packet without receiving a response. The valid range is 1 to 255, with a default of 5. Note Increasing the keepalive period and number of retries might be necessary when supporting a large number of PPPoE sessions.

	Command or Action	Purpose
Step 7	peer default ip address pool <i>name</i> [<i>name2</i> ...] Example: Router(config-if)# peer default ip address pool local Router(config-if)#	(Optional) Defines one or more pools of addresses to be used when assigning IP addresses to the PPPoE clients.
Step 8	ppp authentication { chap ms-chap pap } Example: Router(config-if)# ppp authentication chap Router(config-if)#	Defines the authentication method to be used for PPPoE sessions: • chap = Challenge Handshake Authentication Protocol • ms-chap = Microsoft's version of CHAP • pap = Password Authentication Protocol
Step 9	ppp timeout authentication <i>response-time</i> Example: Router(config-if)# ppp timeout authentication 10 Router(config-if)#	(Optional) Specifies the maximum time, in seconds, that the router should wait for a response to a PPP authentication packet. The valid range is 0 to 255 seconds, with a default of 10 seconds. Note Increase this timeout if PPPoE sessions begin failing due to timeout errors.
Step 10	ppp timeout retry <i>timeout</i> Example: Router(config-if)# ppp timeout retry 5 Router(config-if)#	(Optional) Specifies the maximum time, in seconds, that the router should wait for a response during PPP negotiation. The valid range is 1 to 255 seconds, with a default of 2 seconds. Note Increase this timeout if PPPoE sessions begin failing due to timeout errors.
Step 11	no logging event link-status Example: Router(config-if)# no logging event link-status Router(config-if)#	(Optional) Disables sending unnecessary link up and link down event messages to the router's event log. These messages would otherwise be sent each time a PPPoE session begins and ends.
Step 12	no cdp enable Example: Router(config-if)# no cdp enable Router(config-if)#	(Optional) Disables the use of the Cisco Discovery Protocol (CDP) on the virtual interface. This protocol is unnecessary on a virtual interface for PPPoE sessions.
Step 13	exit Example: Router(config-if)# exit Router(config)#	Exits interface configuration mode.
Step 14	exit Example: Router(config)# exit Router#	Exits global configuration mode.

Configuring a VPDN Group for PPPoE Sessions

Use the following commands, starting in user EXEC mode, to create and configure a virtual private dialup network (VPDN) group on the Cisco CMTS router that is acting an L2TP access concentrator (LAC). The router uses the VPDN group to configure the PPPoE sessions it creates for cable modem users. This step is required on the Cisco CMTS.



Note

You can create only one VPDN group to support PPPoE sessions.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vpdn-group** *number*
4. **accept-dialin**
5. **protocol pppoe**
6. **virtual-template** *number*
7. **exit**
8. **lcp renegotiation** {**always** | **on-mismatch**}
9. **pppoe limit per-mac** *number*
10. **pppoe limit max-sessions** *number-of-sessions* [**threshold-sessions** *number*]
11. **exit**
12. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable Router#	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal Router(config)#	Enters global configuration mode.
Step 3	vpdn-group <i>name</i> Example: Router(config)# vpdn-group 1 Router(config-vpdn)#	Creates a VPDN group with the specified name or number and enters VPDN-group configuration mode.

	Command or Action	Purpose
Step 4	<pre>Router(config-vpdn)# accept-dialin</pre> Example: <pre>Router(config-vpdn)# accept-dialin Router(config-vpdn-acc-in)#</pre>	Configures the router to accept tunneled PPP/PPPoE connections from the LAC and enters VPDN accept dialin configuration mode.
Step 5	<pre>Router(config-vpdn)# protocol pppoe</pre> Example: <pre>Router(config-vpdn)# protocol pppoe Router(config-vpdn-acc-in)#</pre>	Configures the VPDN group to use the PPPoE protocol.
Step 6	<pre>virtual-template <i>number</i></pre> Example: <pre>Router(config-vpdn-acc-in)# virtual-template 1 Router(config-vpdn-acc-in)#</pre>	Specifies the number of the virtual-interface template to be used when configuring a PPPoE session. Note This should be the same virtual-interface template defined in Configuring a Virtual Template on the Cisco CMTS, page 329.
Step 7	<pre>exit</pre> Example: <pre>Router(config-vpdn-acc-in)# exit Router(config-vpdn)#</pre>	Exits VPDN accept dialin configuration mode.
Step 8	<pre>lcp renegotiation {always on-mismatch}</pre> Example: <pre>Router(config-vpdn)# lcp renegotiation always Router(config-vpdn)#</pre>	(Optional) Specifies whether the Cisco CMTS, acting as the LNS, can renegotiate the PPP Link Control Protocol (LCP) with the router acting as the LAC: • always = Always allows the Cisco CMTS to renegotiate the connection. • on-mismatch = The Cisco CMTS can renegotiate the connection only when a configuration mismatch is discovered between the LNS and LAC. The default is that the LNS should not be able to renegotiate the connection.
Step 9	<pre>pppoe limit per-mac <i>number</i></pre> Example: <pre>Router(config-vpdn)# pppoe limit per-mac 1 Router(config-vpdn)#</pre>	(Optional) Specifies the maximum number of PPPoE sessions that can originate from each MAC address. The valid range is 1 to 5000, with a default of 100. For cable users, Cisco recommends a maximum of 1 PPPoE session per MAC address. Note This command is not available until after you have configured the group for the PPPoE protocol in Step 5.

	Command or Action	Purpose
Step 10	pppoe limit max-sessions <i>number-of-sessions</i> [threshold-sessions <i>number</i>] Example: Router(config-vpdn)# pppoe limit max-sessions 1000 threshold-sessions 750 Router(config-vpdn)#	(Optional) Specifies the number of PPPoE sessions supported on the router: <i>number</i> = Specifies the maximum number of PPPoE sessions that can be established at any one time on the router. The valid range is 1 to 5000, with a default of 100. threshold-sessions <i>number</i> = (Optional) Specifies the threshold for active PPPoE sessions. If the number of sessions exceeds this value, an SNMP trap can be sent. The valid range is 1 to 5000, and the default equals the <i>number-of-sessions</i> value. Note This command is not available until after you have configured the group for the PPPoE protocol in Step 5.
Step 11	exit Example: Router(config-vpdn)# exit Router(config)#	Exits VPDN-group configuration mode.
Step 12	exit Example: Router(config)# exit Router#	Exits global configuration mode.

Configuring a VPDN Group for L2TP Tunnel Initiation on the Cisco CMTS

Use the following commands, starting in user EXEC mode, to create and configure a virtual private dialup network (VPDN) group on the Cisco CMTS router that is acting as a when it is acting an L2TP access concentrator (LAC), so that it can create an L2TP tunnel with the L2TP network server (LNS).



Note

This step is required when you are using L2TP tunneling with PPPoE sessions. In this configuration, you must create at least one VPDN group to support the PPPoE sessions and at least one other VPDN group to support the L2TP tunnel.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vpdn-group** *number*
4. **request-dialin**
5. **protocol l2tp**
6. **domain** *domain-name*
7. **exit**

8. **initiate-to ip** *ip-address*
9. **local name** *pppoe-username*
10. **no l2tp tunnel authentication**
11. **exit**
12. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable Router#	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal Router(config)#	Enters global configuration mode.
Step 3	vpdn-group <i>number</i> Example: Router(config)# vpdn-group 2 Router(config-vpdn)#	Creates the VPDN group with the specified number and enters VPDN-group configuration mode.
Step 4	Router(config-vpdn) # request-dialin Example: Router(config-vpdn) # request-dialin Router(config-vpdn-req-in) #	Configures the router to initiate L2TP tunnel requests and enters VPDN request dialin configuration mode.
Step 5	protocol l2tp Example: Router(config-vpdn-req-in) # protocol l2tp Router(config-vpdn-req-in) #	Configures the VPDN group for the L2TP protocol.
Step 6	domain <i>domain-name</i> Example: Router(config-vpdn-req-in) # domain client.com Router(config-vpdn-req-in) #	Specifies that this VPDN group should be used to create PPPoE sessions for clients requesting access from the specified domain name.
Step 7	exit Example: Router(config-vpdn-req-in) # exit Router(config-vpdn) #	Exits VPDN request dialin configuration mode.

	Command or Action	Purpose
Step 8	initiate-to ip <i>ip-address</i> Example: Router(config-vpdn)# initiate-to ip 10.10.10.2 Router(config-vpdn)#	Establishes the IP address for the termination point of the L2TP tunnel that is used by PPPoE clients using this VPDN group.
Step 9	local name <i>pppoe-username</i> Example: Router(config-vpdn)# local name PpPoE-UseR Router(config-vpdn)#	Specifies the username to be used for authentication on the VPDN group.
Step 10	no l2tp tunnel authentication Example: Router(config-vpdn)# no l2tp tunnel authentication Router(config-vpdn)#	Disables authentication for the creation of the L2TP tunnel (but continues to authenticate individual user sessions).
Step 11	exit Example: Router(config-vpdn)# exit Router(config)#	Exits VPDN-group configuration mode.
Step 12	exit Example: Router(config)# exit Router#	Exits global configuration mode.

Enabling PPPoE on a Cable Interface

Use the following commands, starting in user EXEC mode, to enable PPPoE on a specific cable interface on the Cisco CMTS router when it is acting an L2TP access concentrator (LAC).

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface cable** *x/y*
4. **pppoe enable**
5. **hold-queue** *n* **in**
6. **hold-queue** *n* **out**
7. **exit**
8. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable Router#	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal Router(config)#	Enters global configuration mode.
Step 3	interface cable <i>x/y</i> Example: Router(config)# interface cable 4/0 Router(config-if)#	Enters cable interface configuration mode for the specified cable interface:
Step 4	pppoe enable Example: Router(config-if)# pppoe enable Router(config-if)#	Enables PPPoE on the interface, allowing PPPoE sessions to be created through that interface. (The pppoe enable command is not available until you enable VPDN operations, using the vpdn enable command as shown in the procedure given in the “Enabling VPDN Operations on the Cisco CMTS” section on page 327.) Note Enabling PPPoE on a cable interface also automatically enables it on all subinterfaces.
Step 5	hold-queue <i>n</i> in Example: Router(config-if)# hold-queue 1000 in Router(config-if)#	(Optional) Specify the maximum number of data packets that can be stored in the input queue during PPPoE sessions. The valid range is 0 to 65535 packets, with a default of 75. Note To support a large number of simultaneous PPPoE sessions, set the input queue value to at least 1000 packets to avoid dropped packets.
Step 6	hold-queue <i>n</i> out Example: Router(config-if)# hold-queue 1000 out Router(config-if)#	(Optional) Specify the maximum number of data packets that can be stored in the output queue during PPPoE sessions. The valid range is 0 to 65535 packets, with a default of 40. Note To support a large number of simultaneous PPPoE sessions, set the output queue value to at least 1000 packets to avoid dropped packets.
Note		Repeat Step 3 through Step 6 for each cable interface that supports PPPoE sessions.

	Command or Action	Purpose
Step 7	exit Example: Router(config-if)# exit Router(config)#	Exits interface configuration mode.
Step 8	exit Example: Router(config)# exit Router#	Exits global configuration mode.

Configuring a Cisco Router as LNS

Use the following commands, starting in user EXEC mode, to enable and configure a Cisco router, such as the Cisco 6400, to act as the L2TP network server (LNS), so that it can terminate the L2TP tunnels initiated by the Cisco CMTS router when it is acting an L2TP access concentrator (LAC).



Note

Before performing this procedure on the LNS router, you must also enable VPDN operations, using the procedure given in the [“Enabling VPDN Operations on the Cisco CMTS” section on page 327](#). In addition, you must also create and configure a virtual-interface template, using the procedure given in the [“Configuring a Virtual Template on the Cisco CMTS” section on page 329](#).

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vpdn-group** *number*
4. **accept-dialin**
5. **protocol l2tp**
6. **virtual-template** *number*
7. **exit**
8. **terminate-from hostname** *hostname*
9. **no l2tp tunnel authentication**
10. **exit**
11. **virtual-template** *number* **pre-clone** *number*
12. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable Router#	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal Router(config)#	Enters global configuration mode.
Step 3	vpdn-group <i>number</i> Example: Router(config)# vpdn-group 1 Router(config-vpdn)#	Select the VPDN group number and enters VPDN-group configuration mode.
Step 4	accept-dialin Example: Router(config-vpdn)# accept-dialin Router(config-config-vpdn-acc-in)#	Configures the router to accept dial-in calls and enters VPDN accept dialin configuration mode.
Step 5	protocol l2tp Example: Router(config-vpdn-acc-in)# protocol pppoe Router(config-vpdn-acc-in)#	Configures the VPDN group for the L2TP protocol so that it can access the PPPoE server.
Step 6	virtual-template <i>number</i> Example: Router(config-vpdn-acc-in)# virtual-template 1 Router(config-vpdn-acc-in)#	Specifies the number of the virtual-interface template to be used when configuring a PPPoE session. Note Specify the number of a virtual-interface template that has been created using the procedure given in the “Configuring a Virtual Template on the Cisco CMTS” section on page 329.
Step 7	exit Example: Router(config-vpdn-acc-in)# exit Router(config-vpdn)#	Exits VPDN accept dialin configuration mode.
Step 8	terminate-from hostname <i>hostname</i> Example: Router(config-vpdn)# terminate-from hostname ciscocmts-router Router(config-vpdn)#	Configures this group so that it terminates L2TP tunnels from the specified hostname. The <i>hostname</i> should be the host name for the Cisco CMTS that is configured for PPPoE termination.

	Command or Action	Purpose
Step 9	no l2tp tunnel authentication Example: Router(config-vpdn)# no l2tp tunnel authentication Router(config-vpdn)#	Disables authentication for the creation of the L2TP tunnel (but continues to authenticate individual user sessions).
Step 10	exit Example: Router(config-vpdn)# exit Router(config)#	Exits VPDN-group configuration mode.
Step 11	virtual-template number pre-clone number Example: Router(config)# virtual-template 1 pre-clone 2000 Router(config)#	(Optional) Creates the specified number of virtual interfaces in advance, which can speed up the bring up of individual sessions and reduce the load on the router's processor when a large number of sessions come online at the same time. <i>number</i> = Number of virtual interfaces to be created in advance. This value should match the total number of PPPoE sessions that the router is expected to support. Note Pre-cloning is not recommended when using virtual subinterfaces.
Step 12	exit Example: Router(config)# exit Router#	Exits global configuration mode.

Clearing PPPoE Sessions

To clear all PPPoE sessions for a particular MAC address, use the **clear cable host** command:

```
Router# clear cable host mac-address
Router#
```

The following example shows a PPPoE session for a particular host being cleared:

```
Router# show interface c3/0 modem 0

SID   Priv bits  Type      State      IP address  method  MAC address
1      00         modem     offline    3.18.1.5    dhcp    0030.80bc.2303
1      00         host      offline    3.18.1.5    pppoe   0010.2937.b254

Router# clear cable host 0010.2937.b254

Router# show interface c3/0 modem 0

SID   Priv bits  Type      State      IP address  method  MAC address
1      00         modem     offline    3.18.1.5    dhcp    0030.80bc.2303

Router#
```

Enabling SNMP Traps for Active PPPoE Sessions

In Cisco IOS Release 12.2(8)BC1 and later releases, you can enable SNMP traps to inform you when the number of active PPPoE sessions exceeds a threshold value, using the following procedure.



Note

Configure the threshold value using the **threshold-sessions** option for the **pppoe limit max-sessions** command when configuring the VPDN group for PPPoE sessions. For more information about PPPoE traps, see the CISCO-PPPOE-MIB.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server enable traps pppoe**
4. **exit**



Note

To enable SNMP traps, you must also configure the router to support SNMP sessions and specify at least one SNMP manager to receive the SNMP traps.

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable Router#	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal Router(config)#	Enters global configuration mode.
Step 3	snmp-server enable traps pppoe Example: Router(config)# snmp-server enable traps pppoe Router(config)#	Enables SNMP traps to be sent whenever the number of active sessions exceeds a user-configurable threshold.
Step 4	exit Example: Router(config)# exit Router#	Exits global configuration mode.

Monitoring the PPPoE Termination Feature

To display users who have registered with the Cisco CMTS using PPPoE, use the **show interface cable modem** command:

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

SID	Priv bits	Type	State	IP address	method	MAC address
1	00	host	unknown		pppoe	00e0.f7a4.5171
1	00	modem	up	10.100.2.35	dhcp	0050.7302.3d81
2	00	modem	up	10.100.2.34	dhcp	0050.7302.3d85

```
Router#
```

To display the virtual-template interface number being used by a PPPoE client, use the **show vpdn session** command.

```
Router# show vpdn session
```

```
L2TP Tunnel and Session Information Total tunnels 1 sessions 1
```

LocID	RemID	Remote Name	State	Remote Address	Port	Sessions
34854	14116	R7732-07-ISP1	est	135.1.1.1	1701	1

LocID	RemID	TunID	Intf	Username	State	Last Chg	Fastswitch
2	56	34854	Vi1	pppl@ispl.com	est	00:02:11	enabled

```
%No active L2F tunnels
```

```
%No active PPTP tunnels
```

```
PPPoE Tunnel and Session Information Total tunnels 1 sessions 1
```

```
PPPoE Tunnel Information
```

```
Session count: 1
```

```
PPPoE Session Information
```

SID	RemMAC	LocMAC	Intf	VASt	OIntf	VLAN/ VP/VC
1	0050.da80.c13e	0005.00e0.8c8b	Vi1	UP	Ca8/0/1	

```
Router#
```

To display the current VPDN domains, use the **show vpdn domain** command:

```
Router# show vpdn domain
```

Tunnel	VPDN Group
domain:ispl.com	2 (L2TP)

```
Router#
```

Configuration Examples for PPPoE Termination

This section lists the following sample configurations for the PPPoE Termination feature:

- [PPPoE Termination on a Cisco CMTS without L2TP Tunneling, page 343](#)
- [PPPoE Termination on a Cisco CMTS with L2TP Tunneling, page 344](#)
- [PPPoE Client Configuration on a Cisco Router, page 346](#)

- [PPPoE Configuration for the L2TP Network Server, page 346](#)

PPPoE Termination on a Cisco CMTS without L2TP Tunneling

The following configuration configures the Cisco CMTS router to perform PPPoE termination. Traffic from the cable modem users is then sent out over the router's WAN interfaces as IP packets, allowing basic Internet access.

```
version 12.2
!
hostname ubr-pppoe
!
ip cef
no ip domain-lookup
ip domain-name client.com
vpdn enable
no vpdn logging
!
! VPDN group 1 configures the router to accept PPPoE connections and specifies the
! virtual template to be used to configure the virtual interfaces that are created
! for each PPPoE session.
!
vpdn-group 1
 accept-dialin
  protocol pppoe
  virtual-template 1
  pppoe limit per-mac 100
!
! Increase size of small buffers to account for keepalive packets for PPPoE sessions
buffers small permanent 1024
buffers small max-free 1024
buffers small initial 1024
!
interface Ethernet1/0
 ip address 10.100.0.1 255.255.255.0
 ip route-cache flow
 half-duplex
!
! "pppoe enable" command must be configured on each cable interface that is to accept
! PPPoE sessions, but you do not need to configure this command on subinterfaces
interface Cable6/0
 no ip address
 no keepalive
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream frequency 589250000
 no cable upstream 0 shutdown
 cable upstream 1 frequency 35008000
 cable upstream 1 power-level 0
 no cable upstream 1 shutdown
 no cable upstream 2 shutdown
 pppoe enable
!
interface Cable6/0.1
 ip address 10.1.1.1 255.255.255.0 secondary
 ip address 10.10.1.1 255.255.255.0
 cable helper-address 10.100.0.100
 no cable proxy-arp
 cable dhcp-giaddr policy
!
```

```

interface Cable6/0.2
ip address 10.1.2.1 255.255.255.0 secondary
ip address 10.10.2.1 255.255.255.0
cable dhcp-giaddr policy
cable helper-address 10.100.0.100
!
interface Cable6/0.3
ip address 10.1.3.1 255.255.255.0
cable source-verify
cable dhcp-giaddr policy
cable helper-address 10.100.0.100
!
! Virtual Template 1 configures the virtual interfaces that will be used
! for PPPoE sessions
interface Virtual-Template1
ip unnumbered Ethernet1/0
ip mtu 1492
ip pim sparse-mode
peer default ip address pool default
ppp authentication chap
no logging event link-status
no cdp enable
!

```

PPPoE Termination on a Cisco CMTS with L2TP Tunneling

The following configuration configures the Cisco CMTS router to perform PPPoE termination. Traffic received from the cable modem users is sent over the L2TP tunnel to the router that is acting as the L2TP Network Server (LNS).

```

version 12.2
!
hostname ubr-pppoe-l2tp
!
! User name/password sent to LNS to create the L2TP tunnel.
username cmts-user password 0 cmts-password
! User name/password used by LNS to authenticate tunnel creation
username lns-user password 0 lns-password
! User name/password for a PPPoE user - typically this information
! is configured on the RADIUS authentication servers.
username pppoe-user@client.com password 0 user-password
ip cef
no ip domain-lookup
ip domain-name client.com
vpdn enable
no vpdn logging
!
! VPDN group 1 configures the router to accept PPPoE connections and specifies the
! virtual template to be used to configure the virtual interfaces that are created
! for each PPPoE session.
!
vpdn-group 1
accept-dialin
protocol pppoe
virtual-template 1
pppoe limit per-mac 100
!
! VPDN group 2 configures the group to be used for the L2TP tunnel to the
! LNS (at the IP address of 10.10.15.2) which will be used for PPPoE
! sessions from clients using the domain name as "client.com".
vpdn-group 2

```



```
request-dialin
protocol l2tp
domain client.com
initiate-to ip 10.10.15.2
local name ubr-pppoe-l2tp
no l2tp tunnel authentication
!
! Increase size of small buffers to account for keepalive packets for PPPoE sessions
buffers small permanent 1024
buffers small max-free 1024
buffers small initial 1024
!
interface Ethernet1/0
ip address 10.100.0.1 255.255.255.0
ip route-cache flow
half-duplex
!
! "pppoe enable" command must be configured on each cable interface that is to accept
! PPPoE sessions, but you do not need to configure this command on subinterfaces
interface Cable6/0
no ip address
no keepalive
cable downstream annex B
cable downstream modulation 64qam
cable downstream interleave-depth 32
cable downstream frequency 589250000
no cable upstream 0 shutdown
cable upstream 1 frequency 35008000
cable upstream 1 power-level 0
no cable upstream 1 shutdown
no cable upstream 2 shutdown
pppoe enable
!
interface Cable6/0.1
ip address 10.1.1.1 255.255.255.0 secondary
ip address 10.10.1.1 255.255.255.0
cable helper-address 10.100.0.100
no cable proxy-arp
cable dhcp-giaddr policy
!
interface Cable6/0.2
ip address 10.1.2.1 255.255.255.0 secondary
ip address 10.10.2.1 255.255.255.0
cable dhcp-giaddr policy
cable helper-address 10.100.0.100
!
interface Cable6/0.3
ip address 10.1.3.1 255.255.255.0
cable source-verify
cable dhcp-giaddr policy
cable helper-address 10.100.0.100
!
! Virtual Template 1 configures the virtual interfaces that will be used
! for PPPoE sessions
interface Virtual-Template1
ip unnumbered Ethernet1/0
ip mtu 1492
ip pim sparse-mode
peer default ip address pool default
ppp authentication chap
no logging event link-status
no cdp enable
```

PPPoE Client Configuration on a Cisco Router

The following configuration configures a Cisco router that supports PPPoE to act as a PPPoE client. This router connects to the cable modem and performs the PPPoE authentication with the Cisco CMTS that is performing the PPPoE termination.



Note

This configuration is for the Cisco 1600 router and needs to be adjusted to fit the interfaces that might be present on other types of routers.

```
!
vpdn enable
no vpdn logging
!
vpdn-group 1
 request-dialin
 protocol pppoe
!
!
interface Ethernet0
 no ip address
 pppoe enable
 pppoe-client dial-pool-number 1
!
interface Dialer1
 mtu 1492
 ip address negotiated
 ip nat outside
 encapsulation ppp
 dialer pool 1
 ppp chap hostname joeuser@client.com
 ppp chap password 7 12139CA0C041104
!
ip nat inside source list 1 interface Dialer1 overload

ip route 0.0.0.0 0.0.0.0 Dialer1
!
access-list 1 permit any
```

PPPoE Configuration for the L2TP Network Server

The following sample configuration shows a Cisco router being configured to act as the L2TP Network Server (LNS). This router terminates the L2TP tunnel from the Cisco CMTS and forwards the traffic from the PPPoE sessions to the corporate network.

```
!
hostname lns-router
!
! User name/password for the LNS itself
username lns-user password 0 lns-password
! User name/password for the Cisco CMTS
username cmts-user password 0 cmts-password
! Username and password for the PPPoE client - typically this information is
! configured on the RADIUS authentication servers
username pppoe-user@client.com password 0 user-password
!
ip subnet-zero
ip cef
ip domain-name client.com
```

```
!  
vpdn enable  
no vpdn logging  
!  
vpdn-group 1  
  accept-dialin  
  protocol l2tp  
  virtual-template 1  
  terminate-from hostname ubr-pppoe-l2tp  
  no l2tp tunnel authentication  
!  
! Allows the LNS to preconfigure virtual templates  
! for the PPPoE sessions, allowing the sessions to come up faster  
virtual-template 1 pre-clone 2000  
!  
interface loopback 0  
ip address 9.10.7.1 255.255.255.0  
!  
!  
interface Virtual-Template1  
  ip unnumbered loopback 0  
  ip mroute-cache  
  ip mtu 1492  
  peer default ip address pool pool-1 pool-2  
!  
ip local pool pool-1 9.10.7.3 9.10.7.254  
ip local pool pool-2 9.10.8.1 9.10.8.254
```

Additional References

For additional information related to configuring PPPoE Termination on the Cisco CMTS, refer to the following references:

Related Documents

Related Topic	Document Title
Configuring PPP over Ethernet	Configuring Broadband Access: PPP and Routed Bridge Encapsulation, Cisco IOS Wide-Area Networking Configuration Guide, Release 12.2, at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fwan_c/wcfppp.htm
Enabling SNMP Traps for PPPoE Active Sessions	<i>PPPoE Session-Count MIB</i> , at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ftpscmib.htm
Configuring Virtual Private Networks (VPNs)	Configuring Virtual Private Networks, Cisco IOS Dial Service Configuration Guide: Network Services, Release 12.1, at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/dialns_c/index.htm
CMTS Command Reference	<i>Cisco Broadband Cable Command Reference Guide</i> , at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/cable/bbcmref/index.htm
Cisco IOS Release 12.2 Command Reference	Cisco IOS Release 12.2 Configuration Guides and Command References, at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/index.htm

Standards

Standards ¹	Title
SP-RFIV1.1-I08-020301	Data-Over-Cable Service Interface Specifications Radio Frequency Interface Specification, version 1.1 (http://www.cablemodem.com)

1. Not all supported standards are listed.

MIBs

MIBs ¹	MIBs Link
CISCO-PPPOE-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

1. Not all supported MIBs are listed.

RFCs

RFCs ¹	Title
RFC 1483	Multiprotocol Encapsulation over ATM Adaptation Layer 5
RFC 2516	A Method for Transmitting PPP Over Ethernet (PPPoE)
RFC 2865	Remote Authentication Dial In User Service (RADIUS)
RFC 2866	RADIUS Accounting

1. Not all supported RFCs are listed.

Technical Assistance

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

Glossary

L2F—Layer 2 Forwarding. The L2F protocol is a Cisco-proprietary standard for a tunneling mechanism that transports link-layer frames, such as PPP, that are used by higher-layer protocols. These tunnels allow the provider to separate the initial dialup servers from the corporate gateways, without compromising network security.

L2TP—Layer 2 Tunneling Protocol (L2TP). An extension to the Point-to-point (PPP) protocol and a fundamental building block for virtual private networks (VPN). L2TP combines the best features of Cisco's Layer 2 Forwarding (L2F) protocol and Microsoft's Point-to-Point Tunneling (PPTP). L2TP is an Internet Engineering Task Force (IETF) standard.

LAC—L2TP access concentrator. The LAC is one endpoint of the L2TP tunnel and is a peer to the LNS. The LAC forwards packets between the LNS and the remote systems (such as cable modems), using the L2TP tunnel protocol. Typically, the Cisco CMTS acts as the LAC.

LNS—L2TP network server. The LNS is the destination endpoint for the L2TP tunnel and is a peer to the LAC. The LNS terminates the PPP sessions from the remote systems (such as cable modems) that it receives through the L2TP tunnel initiated by the LAC.

NAS—Network Access Server. This device provides temporary, on-demand network access to users. In Cisco's PPPoE implementation, the NAS functions are provided by the LAC.

Peer—Router or device that participates as an endpoint in IPSec and IKE.

PPP—Point-to-Point Protocol. A protocol developed for dial-up users to extend the IP network over serial interfaces and dial-up lines, allowing for automatic configuration of the user's IP address and other network information.

PPPoE—Point-to-Point Protocol over Ethernet. This protocol encapsulates PPP packets within Ethernet MAC frames, so that network users can be authenticated and configured using the same PPP systems that are used for point-to-point users (such as dial-up or DSL users).

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, TeleRouter, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0502R)



Spectrum Management for the Cisco CMTS

This chapter describes the spectrum management features supported by the Cisco Cable Modem Termination System (CMTS) universal broadband routers. Spectrum management support is divided into two main groups:

- guided and scheduled spectrum management features (supported in software)
- intelligent and advanced spectrum management features (supported in hardware only on specific cable interfaces)

Feature History for Spectrum Management for the Cisco CMTS

Release	Modification
Release 11.3(9)NA, Release 12.0(6)SC, and Release 12.1(2)EC	Guided and scheduled spectrum management was introduced on Cisco uBR7200 series routers.
Release 12.1(2)EC	Support was added for intelligent spectrum management on the Cisco uBR-MC16S cable interface card on the Cisco uBR7200 series router.
Release 12.1(5)EC	Support was added for guided and scheduled spectrum management on Cisco uBR7100 series routers.
Release 12.1(10)EC1, Release 12.2(4)BC1	The SNR algorithm was corrected to display a more accurate value for upstreams.
Release 12.1(7)CX, Release 12.2(4)BC1	Support was added for advanced spectrum management on the Cisco uBR-MC16S cable interface card on Cisco uBR7200 series routers.
Release 12.2(4)BC1	Support was added for guided and scheduled spectrum management on Cisco uBR10012 routers.
Release 12.2(8)BC2	Support was added for intelligent and advanced spectrum management on the Cisco uBR-LCP2-MC16S cable interface card on the Cisco uBR10012 router.
Release 12.2(11)BC3	Support was added for the cable spectrum-group shared command on the Cisco uBR-LCP2-MC16S card on the Cisco uBR10012 router.
Release 12.2(15)BC1	Support was added for guided and scheduled spectrum management on the Cisco uBR-MC5X20S cable interface line card.

Release 12.2(15)BC2	This release added the following support: • Support was added for intelligent and advanced spectrum management on the Cisco uBR-MC16U/X and Cisco uBR-MC28U/X cable interface line cards. • Support was added for guided and scheduled spectrum management on the Cisco uBR-MC5X20U card. • The maximum number of spectrum groups was increased from 32 to 40 groups per router. • The number of predefined modulation profiles was increased.
Release 12.3(9)BC	This release added the following support: • Spectrum management support with the Cisco Broadband Troubleshooter (CBT) 3.2 for the Cisco MC5X20S/U Broadband Processing Engine (BPE).

Finding Support Information for Platforms and Cisco IOS Software Images

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

Contents

- [Prerequisites for Spectrum Management, page 354](#)
- [Restrictions for Spectrum Management, page 356](#)
- [Information About Spectrum Management, page 362](#)
- [How to Configure Spectrum Management, page 382](#)
- [Monitoring Spectrum Management, page 406](#)
- [Configuration Examples, page 411](#)
- [Additional References, page 426](#)



Note

This chapter provides configuration information but not a complete command reference. For complete information on the commands used in this chapter, see the *Cisco Cable Modem Termination System Commands* chapter in the *Cisco Broadband Cable Command Reference Guide*.

Prerequisites for Spectrum Management

- The appropriate Cisco IOS release for the desired features. For a list of supported Cisco IOS releases by feature, see [Table 5 on page 356](#).
- Guided and scheduled spectrum management features require one of the following Cisco CMTS routers, and one or more of the indicated cable interfaces:
Cisco uBR7100 series (all models)

Cisco uBR7200 series router and one or more of the following cable interfaces:

- Cisco uBR-MC11C
- Cisco uBR-MC12C
- Cisco uBR-MC14C
- Cisco uBR-MC16C/E/S/U/X
- Cisco uBR-MC28C/U/X

Cisco uBR10012 router and one or more of the following cable interfaces:

- Cisco uBR-LCP2-MC16C/E/S
- Cisco uBR-LCP2-MC28C
- Cisco uBR-MC5X20S/U

- Intelligent and advanced spectrum management (hardware-based, CNR frequency hopping) requires the following Cisco CMTS routers and one of more of the indicated cable interfaces:

Cisco uBR7200 series router and one or more of the following cable interfaces:

- Cisco uBR-MC16S/U/X
- Cisco uBR-MC28U/X

Cisco uB10012 router and the following cable interface:

- Cisco uBR-LCP2-MC16S

- Ensure that your network is designed to support reliable broadband data transmission. At minimum, your network must include:
 - A Dynamic Host Configuration Protocol (DHCP) server to assign IP addresses to cable modems or set-top boxes on the hybrid fiber-coaxial (HFC) network. This can be a server on the WAN side of the Cisco uBR7200 series router or a Cisco CMTS router that has been configured to act as the DHCP server.
 - If you are not using the Cisco uBR7100 series router with integrated upconverter, you must install the appropriate IF-to-RF external upconverter between the Cisco CMTS router and the combiner.



Note The term “combiner” refers to all cables, amplifiers, and taps at the headend or cable distribution center that connect the Cisco CMTS router to the HFC network.

- Diplex filters installed in the downstream RF path between the cable modems and the cable interface cards in the router. RG-59 headend coaxial cable with the maximum braid available (60 percent + 40 percent braid), double foil, and the correct connector for this cable.
- Avoid frequencies with known ingress problems such as amateur radio bands or short-wave bands.
- Avoid hostile spectrums below 20 MHz.
- When designing your channel plan, allow extra bands for frequency hopping.
- Place upstream ports in the same combiner group in a shared spectrum group.
- Use the receive power level setting to perform slight equalization adjustments.
- Due to the nature of CATV technology, upstream noise management is a significant issue. We recommend that you follow the rigorous North American plant maintenance procedures that are documented in the *NCTA Supplement on Upstream Transport Issues* to adjust return amplifiers and lasers.

Restrictions for Spectrum Management

This section describes the restrictions for the following spectrum management features:

- [Cisco uBR10012 Router and Cisco IOS Release 12.2\(8\)BC2 Support, page 357](#)
- [Cisco IOS Releases and Cable Interface Line Card Support, page 356](#)
- [DOCSIS Cable Modem Test Analyzer, page 358](#)
- [Dynamic Upstream Modulation, page 358](#)
- [Fixed-Frequency Spectrum Groups with Advanced Spectrum Management, page 358](#)
- [Limitations on Upstream Modulation Parameters for PacketCable VoIP Calls, page 359](#)
- [HCCP 1+1 and N+1 Redundancy Support, page 359](#)
- [Intelligent and Advanced Spectrum Management Support, page 360](#)

Cisco IOS Releases and Cable Interface Line Card Support

The guided and scheduled spectrum management features are available for all currently supported cable interface line cards. These features were released in phases. [Table 5](#) summarizes the individual features in this basic spectrum management feature set, and the initial Cisco IOS software releases that introduced them.

Table 5 *Summary of Guided and Scheduled Spectrum Management Features by Release*

Feature	Cisco IOS Release Supported
Traffic Shaping, page 371 Upstream Traffic Shaping, page 371 Downstream Traffic Shaping, page 372	12.1(2)EC1, 12.2(4)BC1, and later releases
Dynamic Upstream Modulation (SNR-based), page 374 Guided Frequency Hopping, page 373 Time-Scheduled Frequency Hopping, page 374	12.1(3a)EC1, 12.0(13)SC, 12.2(4)BC1, and later releases
Input Power Levels, page 376	12.0(6)SC, 12.1(2)EC1, 12.2(4)BC1, and later releases

The intelligent and advanced spectrum management features were also released in phases. [Table 6](#) shows the minimum software releases that are needed for these features on the cable interface line cards that support them.

Table 6 *Minimum Cisco IOS Releases for Intelligent and Advanced Spectrum Management Support*

Cable Interface Line Card	Minimum Cisco IOS Release
Cisco uBR7200 Series Routers	
Cisco uBR-MC16S	12.1(7)EC (intelligent features) 12.2(8)BC2 (advanced features)
Cisco uBR-MC16U/X	12.2(15)CX, 12.2(15)BC2
Cisco uBR-MC28U/X	12.2(15)CX, 12.2(15)BC2

Table 6 Minimum Cisco IOS Releases for Intelligent and Advanced Spectrum Management Support

Cable Interface Line Card	Minimum Cisco IOS Release
Cisco uBR10012 Router	
Cisco uBR-LCP2-MC16S	12.2(8)BC2

Cisco uBR10012 Router and Cisco IOS Release 12.2(8)BC2 Support

The Cisco uBR10012 router using the Cisco uBR-LCP2-MC16S cable interface line card and Cisco IOS Release 12.2(8)BC2 has the following restrictions and limitations:

- Frequency hopping is based on the carrier-to-noise ratio (CNR) and the correctable FEC error and uncorrectable FEC error values. A channel will frequency hop if the CNR falls below the configurable threshold AND either the correctable or uncorrectable FEC error values exceed the configurable threshold values.

Use the **cable upstream threshold** command to change these values. In Cisco IOS Release 12.2(8)BC2, the CNR threshold for the primary modulation profile defaults to 25 dB. The CNR threshold for the secondary modulation profile defaults to 15 dB. The correctable FEC error threshold defaults to 1 percent of total packets received, and the uncorrectable FEC error threshold defaults to 1 percent of total packets received.



Note

In releases previous to Cisco IOS Release 12.2(8)BC2, the channel would hop if either the CNR fell below the configurable threshold OR either the correctable or uncorrectable FEC error values exceeded the configurable threshold values. If you are using only one modulation profile (QPSK), you might need to reduce the CNR threshold value and increase the correctable FEC error value to prevent undesired frequency hopping.

- Fixed-frequency spectrum groups are not supported.
- Shared spectrum groups are not supported.
- In Cisco IOS Release 12.2(8)BC2, the short and long grant bursts of the pre-configured **mix** and **qam-16** modulation profiles (see the **cable modulation-profile** command) default to a unique word offset of 8 (uw8). These values should be changed to **uw16** for optimal performance. This can be done with the following commands:

```
cable modulation-profile n short 6 75 6 8 16qam scrambler 152 no-diff 144
fixed uw16
cable modulation-profile n long 8 220 0 8 16qam scrambler 152 no-diff 160
fixed uw16
```



Note

This default was tracked by caveat CSCdx35070 and was fixed in Cisco IOS Release 12.1(19)EC1 and Cisco IOS Release 12.2(11)BC3.

- When using Cisco IOS Release 12.2(8)BC2, in rare situations, using CLI commands to configure the Cisco uBR-LCP2-MC16 card could result in the error message “Resources are busy with other msg requests. Try later.” The workaround is to repeat the same configuration command again until the error disappears.

DOCSIS Cable Modem Test Analyzer

Cisco IOS Release 12.2(8)BC2 through Release 12.2(11)BC3 support the DOCSIS Cable Modem Test Analyzer (DCMTA) software from Acterna Corp. This spectrum management tool is designed for troubleshooting ingress and other problems on the return path in real time, not for ongoing monitoring of the upstream spectrum.

In Cisco IOS Release 12.2(15)BC1 and later releases, the Acterna DCMTA tool is no longer supported. The Cisco Broadband Troubleshooter (CBT), release 3.0 or later, replaces the DCMTA tool. For more information, see the Cisco Broadband Troubleshooter documentation, at the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/cable/trblshtr/index.htm>

Dynamic Upstream Modulation

- The Cisco router has one preconfigured (primary) modulation profile that defines a typical profile for QPSK modulation. To use the Dynamic Upstream Modulation feature, you must create a second modulation profile that has a higher modulation scheme than the preconfigured profile.
- Upstream modulation profiles are assigned to upstream ports and affect all cable modems on those upstream ports.
- Modulation profiles affect the physical layer of the cable network, so only trained technicians who are familiar with the DOCSIS specifications should create modulation profiles.
- When using the Dynamic Upstream Modulation feature with Voice over IP (VoIP) services, frequent changes to the upstream modulation or channel width could briefly impact the quality of voice calls.
- The Dynamic Upstream Modulation feature operates differently on the Cisco uBR-MC16S cable interface line card than on other supported cable interface line cards. See the description of this feature in the “[Guided and Scheduled Spectrum Management](#)” section on page 370 and the “[Intelligent and Advanced Hardware-Based Spectrum Management](#)” section on page 376 for more information.

Fixed-Frequency Spectrum Groups with Advanced Spectrum Management

When using cable interface line cards that support advanced spectrum management (such as Cisco uBR-16C/S/U and Cisco uBR-MC28U/X), do not configure fixed-frequency spectrum groups by specifying a single frequency using the **cable spectrum-group frequency** command (for example, **cable spectrum-group 3 frequency 7600000**). If single-frequency spectrum groups are desired, configure a band with a starting and ending range, which, along with the desired channel width, specifies the desired center frequency. In this situation, you must also configure a static channel width so that the Dynamic Upstream Modulation feature does not attempt to hop to a different frequency using a smaller channel width.

For example, to specify a center frequency of 7.6 MHz with a 3.2 MHz channel width, specify a starting frequency of 6.0 MHz (7.6 MHz - 1.6 MHz) and an ending frequency of 9.2 MHz (7.6 MHz + 1.6 MHz):

```
CMTS(config)# cable spectrum-group 15 band 6000000 9200000
CMTS(config)# interface cable 6/0
CMTS(config-if)# cable upstream 0 channel-width 3200000 3200000
CMTS(config-if)# cable upstream 0 spectrum-group 15
```

**Note**

Cisco IOS Release 12.2(8)BC2 does not support spectrum groups with fixed frequencies on the Cisco uBR10012 router.

Limitations on Upstream Modulation Parameters for PacketCable VoIP Calls

When PacketCable support is enabled on the Cisco CMTS to provide Voice over IP (VoIP) support, the following combinations of upstream modulation parameters should not be used, because the channel width is too small to allow the upstream MAC scheduler to provide sufficient grants for reliable VoIP communications.

[Table 7](#) lists the modulation, channel width, and minislot size parameters that should not be used when an upstream is providing support for PacketCable VoIP calls:

Table 7 Unsupported Upstream Parameter Combinations for VoIP Calls

Modulation ¹	Channel Width	Minislot Size
QPSK	200 KHz	32, 64, 128
QPSK	400 KHz	16, 32, 64
16-QAM	400 KHz	32, 64, 128
16-QAM	400 KHz	16, 32, 64

1. The above combinations assume that you are using one of the predefined QPSK and 16-QAM upstream modulations (see the **cable modulation-profile** command). Although it is possible to fine-tune the modulations for VoIP support by manually specifying each of the burst parameters, this should be done only by engineers who are very knowledgeable about RF issues.

We recommend configuring upstreams that are being used for PacketCable operations and VoIP calls for a channel width that is larger than 400 KHz. (These channel widths and upstream parameter combinations can still be used, however, for best-effort data communications.)

HCCP 1+1 and N+1 Redundancy Support

HCCP redundancy requires that the Working and Protect cable interface line cards be identical. This ensures that the Protect interface supports the same exact configuration as the Working interface. When protecting cards that support intelligent and advanced spectrum management (Cisco uBR-MC16S/U/X and Cisco uBR-MC28U/X), a switchover preserves the spectrum management configuration, and the Protect interface initially uses the same upstream frequency as the Working interface. However, the Protect interface does not begin using the advanced spectrum management features until the system stabilizes, so as to avoid any unnecessary frequency hops or channel width changes.

In addition, the only exception to the rule that like cards must protect like cards is that the Cisco uBR-16C and Cisco uBR-MC16S cards can be used to protect one another. This configuration, however, has the limitations on the use of intelligent and advanced spectrum management that are listed in [Table 8](#):

Table 8 *Switchover Operation for Advanced Spectrum Management Configurations*

Working Cable Interface	Protect Cable Interface	Operation After Switchover
Cisco uBR-MC16C	Cisco uBR-MC16S	The protect card uses the same upstream frequency as the working card, but after the system stabilizes, the protect card begins using the advanced spectrum management features that are configured on the protect CMTS.
Cisco uBR-MC16S	Cisco uBR-MC16C	The protect card uses the same upstream frequency as the working card. If the upstream becomes unstable, the protect card performs only guided frequency hopping.

For example, if a Cisco uBR-MC16S is configured as the Working interface and a Cisco uBR-MC16C is configured as the Protect interface, the Cisco uBR-MC16S can be configured for advanced spectrum management features. If a switchover occurs, the Cisco uBR-MC16C comes online using the same upstream frequency configuration, but the Cisco uBR-MC16C can use only guided frequency hopping to correct any future upstream problems. If another switchover occurs, and the Cisco uBR-MC16S comes back online, it again uses the advanced spectrum management features that have been configured.

Intelligent and Advanced Spectrum Management Support

- Cable interfaces must use standard DOCSIS or EuroDOCSIS frequency ranges to support the intelligent and advanced spectrum management features. You cannot use these features when using the extended Japanese frequency ranges (70 MHz to 860 MHz for downstream interfaces, and 5 MHz to 55 MHz for upstream interfaces).
- Intelligent and advanced spectrum management features are supported only in the DOCSIS 1.0 and DOCSIS 1.1 Time Division Multiple Access (TDMA) mode of operation. These features cannot be used when a cable interface is operating in the DOCSIS 2.0 mixed and Advanced TDMA (A-TDMA) modes of operation.
- Intelligent and advanced spectrum management is not currently supported on the Cisco uBR-MC5X20S/U cable interface line cards in Cisco IOS Release 12.2(15)BC2.
- Upstream channels must meet the CNR and carrier-to-ingress power ratio values given in the DOCSIS specifications. The minimum value for both parameters is 25 dB in the 5–42 MHz frequency range.
- The intelligent and advanced Spectrum Management features do not support shared spectrum groups, requiring that each upstream port on the Cisco uBR-MC16S line card must have its own RF domain (a unique set of non-overlapping frequencies).
- HCCP 1+1 redundancy is not supported on any cable interface line card that has defined spectrum groups, which typically is the normal configuration for advanced spectrum management.
- If you are using only one modulation profile and are using a software release prior to Cisco IOS Release 12.2(8)BC2, you probably will need to change the CNR and FEC threshold parameters from their default values to prevent undesired frequency hopping. This is because in these releases, a frequency hop would occur if just one of the measured values (CNR value, correctable FEC counter, or uncorrectable FEC counter) crosses the configured threshold value. Reducing the CNR threshold or increasing one of the FEC threshold values would limit the number of frequency hops.

This situation no longer occurs in Cisco IOS Release 12.2(8)BC2 and later releases, because a frequency hop can occur only when both the CNR value and one of the FEC counters falls below its threshold value. See the [“Advanced Spectrum Management Features” section on page 377](#) for more information.

Information About Spectrum Management

Spectrum management allows a Cisco Cable Modem Termination System (CMTS) to sense both downstream and upstream plant impairments, report them to a management entity, and automatically correct them where possible. The spectrum management feature performs these functions without reducing throughput or latency and without creating additional packet overhead on the radio frequency (RF) plant.

In particular, because the cable interfaces on the Cisco CMTS router receives upstream packets, it can directly detect upstream transmission errors. The router can also indirectly monitor the condition of the plant by keeping a record of modem state changes, such as the number and frequency of cable modems that are “flapping” (modems that either miss a station maintenance message or that go offline and then come back online).

**Note**

For more information about the cable modem flapping and how to monitor the cable modem flap list, see the chapter “[Flap List Troubleshooting for the Cisco CMTS](#)” in this guide.

Spectrum management can prevent long-term service interruptions caused by upstream noise events in the cable plant. It is also used for fault management and troubleshooting the cable network. When cable modems are detected to go online and offline by flap detectors, the cable operators can look at the flap list and spectrum tables to determine the possible causes.

Due to the nature of cable television (CATV) technology, upstream noise management is a significant issue. Frequency bands must have a sufficient carrier-to-noise ratio (CNR) and carrier-to-ingress power ratio to support the transmission of quadrature phase-shift keying (QPSK) and quadrature amplitude modulation (QAM) data. The Data-over-Cable Service Interface Specifications (DOCSIS) set the minimum value for both of these ratios to 25 dB in the 5-MHz to 42-MHz frequency range. If the CNR drops below 25 dB on a particular channel due to noise, the cable modem on that channel degrades and can drop off the hybrid fiber-coaxial (HFC) network.

This overview contains the following subsections:

- [Spectrum Management Measurements, page 363](#)—Provides an overview of fundamental concepts and terms that are used in spectrum management.
- [Upstream Signal Channel Overview, page 366](#)—Describes how signals are sent and how changes occur in upstream channels.
- [Upstream Segments and Combiner Groups, page 367](#)—Describes sparse and dense segments and combiner groups.
- [Frequency Management Policy, page 368](#)—Describes the types of noise impairments and how to counteract ingress noise with spectrum groups and frequency hopping.
- [Guided and Scheduled Spectrum Management, page 370](#)—Describes the following Guided and Scheduled spectrum management features: traffic shaping, frequency hopping capabilities, dynamic upstream modulation (SNR-based), and input power levels.
- [Intelligent and Advanced Hardware-Based Spectrum Management, page 376](#)—Describes spectrum management features that are supported by a number of cable interface line cards that have onboard spectrum management hardware. These features include a real-time spectrum analyzer, CNR-based, proactive frequency hopping, and a more robust dynamic upstream modulation.

Spectrum Management Measurements

Measuring the signal-to-noise ratio (SNR) and carrier-to-noise ratio (CNR) are the major ways of determining the quality of a downstream or upstream signal. The following sections provide an overview of these two ratios, as well as explaining the differences between them, and some additional values that might be useful:

- [Signal and Carrier Noise Ratios, page 363](#)
- [Differences Between the SNR and CNR Values, page 364](#)
- [Additional Measurements, page 365](#)

Signal and Carrier Noise Ratios

Measuring the SNR and CNR of a downstream or upstream is the first step in determining the quality of the signal, and whether spectrum management needs to be performed to correct any errors. The following are brief descriptions of these two values:

- **Signal-to-Noise Ratio (SNR)**—An estimate of signal strength that is done on the upstream after ingress noise cancellation is performed. This means the SNR takes into account a variety of modulation impairments, including frequency response distortions (such as in-channel amplitude tilt and ripple), group delay, microreflections, and phase noise. The SNR is a good gauge of the overall end-to-end quality of the cable network, because it includes the impact that the transmitter circuitry, receiver circuitry, and transmission media have on the upstream signal.

**Note**

The SNR value was incorrectly calculated in early Cisco IOS software images, reporting a value that was 4 dB larger than expected. This defect (reported as caveat CSCdv78225) was corrected in Cisco IOS Release 12.1(10)EC1 and Release 12.2(4)BC1, and later releases. For more information, see Field Notice 44400, at the following URL:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_field_notice09186a00801adb75.shtml

- **Carrier-to-Noise Ratio (CNR)**—A ratio of the measured modulated power, in dB, on the upstream (before ingress noise cancellation is done) that compares the channel power to the noise power. This measurement is usually provided only by an external spectrum analyzer, but the cable interface line cards that support intelligent and advanced hardware spectrum management features can provide two types of CNR measurement:
 - **CNR measured for a particular upstream**—An overall CNR for all of the cable modems on an upstream, as determined by measuring the RF power at the cable interface's upstream receiver. This value is always just a snapshot in time for a particular upstream. The cable interface measures the RF power at a time when no bursts are expected from the cable modems, but it can be skewed by a small number of cable modems that are experiencing or creating signal problems.
 - **Per-modem CNR**—A CNR for a particular cable modem, as measured by the signal strength of the modem's burst transmissions at the cable interface's upstream receiver. The per-modem CNR measurement is a very accurate measure of a particular cable modem's signal, but you should not use a single modem's CNR to make assumptions about other cable modems on that upstream or about the upstream itself. However, you can get a good picture of the upstream's signal quality by polling the CNR for a number of cable modems over a representative time period.

**Tip**

Changing the channel width has a direct impact on CNR. Doubling the channel width (for example, from 400 KHz to 800 KHz) decreases the CNR for an upstream by approximately 3 dB. Cutting the channel width in half (for example, from 3.2 MHz to 1.6 MHz) increases the CNR for an upstream by approximately 3 dB.

Differences Between the SNR and CNR Values

In a perfect network, such as a test lab where the only impairment is additive white Gaussian noise (AWGN), you can expect the CNR and SNR values to be comparable throughout all of the allowable power levels and frequency ranges. In a live network, however, it is expected that the SNR value should be a few dB lower than the CNR value, given that the SNR value takes into account noise impairments and distortions that are not accounted for by the CNR power measurements.

In general, when the CNR value is in the 15 to 25 dB range, you can expect the SNR value to have a comparable value. The difference between the SNR and CNR values is expected to be larger when the CNR value falls outside of the 15 to 25 dB range.

[Table 9](#) provides a comparison for the SNR and CNR values, listing the major reasons for why the SNR and CNR values might diverge on an active network that is passing live traffic:

Table 9 Comparison of SNR and CNR in a DOCSIS Cable Network

Signal-to-Noise (SNR)	Carrier-to-Noise (CNR)
Post-detection measurement of the RF signal.	Pre-detection measurement of the RF signal.
Measurement of the RF frequency domain	Measurement of the baseband domain.
Includes the effect of signal distortions and impairments on the signal. These include: • Group delay in the channel such as occurs during operation near the diplexer band edge. • Channel amplitude variation and echoes. • Data collisions. • Microreflections. • Narrow band ingress in the channel. • Non-linearities in the cable plant. • Phase noise. • Poor selection of the preamble. • Poor symbol fidelity in a cable modem's transmissions, despite a good SNR value. • Unrecoverable carrier offsets. • Unrecoverable symbol timing offsets.	Measures only the RF modulated carrier power versus noise power.
Provides an indication of overall, end-to-end network quality (what the transmitter, receiver, and transmission media are doing to the signal).	Provides an indication of network performance (what the transmission media or network is doing to the signal).

Table 9 Comparison of SNR and CNR in a DOCSIS Cable Network (continued)

Signal-to-Noise (SNR)	Carrier-to-Noise (CNR)
Average over time with current data traffic patterns, useful for tracking long-term trends in signal quality.	Real-time spectrum analysis.
Reflects the CNR value as part of its value.	Does not reflect the SNR value as part of its value.
Averaged over 10,000 symbols, and an accurate reading requires that short and long grants are being transferred.	Unaffected by the type of traffic being transmitted.
Does not use packets with uncorrectable FEC errors to determine its value. Bursts of uncorrectable errors, therefore, could result in a deceptively high SNR value.	Unaffected by uncorrectable FEC packet bursts.
DOCSIS specifications do not define any required SNR values for upstreams and downstreams.	Minimum downstream CNR of 35 dB in a 6 MHz band (44 dB in DOCSIS 2.0 for 8 MHz band) Minimum upstream CNR of 25 dB (22 dB in DOCSIS 2.0)

Additional Measurements

In addition to SNR and CNR values, you should be aware of and monitor the following indicators of signal quality:

- **Modulation Error Ratio (MER)**—A measure of RF signal strength, in dB, which is similar to the SNR value for an upstream, in that it includes distortions and signal impairments such as phase noise and group delay. However, the MER is preferred for data networks, because it also includes additional factors that affect the signal, such as analog-to-digital and digital-to-analog conversions, rounding errors, and phase jitter. For this reason, the DOCSIS 2.0 RF specification adds a requirement for the minimum MER value for a signal, supplementing the existing CNR minimum requirements.

. A simple formula for calculating the MER value for an upstream is:

$$\text{MER} = 20 \times \log (\text{RMS error magnitude} / \text{average symbol magnitude})$$

You can also calculate the Error Vector Modulation (EVM) to find the equivalent value expressed as a percentage of noise on an upstream:

$$\text{EVM} = \text{Average error magnitude} / \text{Max symbol magnitude} * 100$$

See the DOCSIS 2.0 specification for more complete information on calculating and using the MER value.

- **Forward Error Correction (FEC) Counters**—Counters that keep track of how many correctable and uncorrectable FEC errors occur on the upstream. The FEC error counters are useful for tracking fast transient errors such as impulse noise that are not usually reflected in SNR or CNR values.

A correctable error count of more than 1 percent can be used a warning sign of possible physical plant or cable modem problems that might be developed. An uncorrectable error count of more than 1 percent can indicate an existing problem that is blocking traffic on the upstream. Cable interface line cards that support the intelligent and advanced spectrum management features can use the FEC counters as one of the indicators to be monitored to determine whether an upstream must change frequencies so as to correct noise problems.

- **Microreflections**—Additional copies of a signal that arrive at the receiver, usually at different times and attenuated by different amounts, causing the receiver to misidentify the incoming signal's true phase and amplitude. Microreflections typically are caused by impedance mismatches in the physical cable plant, and can indicate either equipment that has been degraded by weather or other causes, or equipment that has not been installed correctly.

Upstream Signal Channel Overview

The upstream channel is characterized by many cable modems transmitting to the CMTS. These signals operate in a burst mode of transmission. Time in the upstream channel is slotted. The CMTS provides time slots and controls the usage for each upstream interval. The CMTS periodically broadcasts Upstream Channel Descriptor (UCD) messages to all cable modems. The UCD message contains the upstream frequency and transmission parameters associated with an upstream channel. These messages define upstream channel characteristics including the upstream frequencies, symbol rates and modulation schemes, forward error correction (FEC) parameters, and other physical layer values.

Cisco supports all DOCSIS error-correction encoding and modulation types and formats. Upstream signals are demodulated using QPSK or QAM. QPSK carries information in the phase of the signal carrier, whereas QAM uses both phase and amplitude to carry information.

Sending data reliably in the upstream direction is an issue. Because upstream spectrum varies greatly between cable plants, select upstream parameters based on your cable plant's return paths. Select or customize upstream profiles for maximum trade-off between bandwidth efficiency and upstream channel robustness. For example, QAM-16 requires approximately 7 dB higher CNR to achieve the same bit error rate as QPSK, but it transfers information at twice the rate of QPSK.



Note

The above specifications are based on predetermined sets of frequencies that may or may not have an adequate CNR at any given time.

Upstream frequencies can be assigned as follows:

- **Fixed**—Configuring a spectrum group disables the fixed upstream frequency setting.
- **Single subband**—The CMTS administrator can define a center frequency and symbol rate such that the boundaries of the upstream carrier stay within the subband. The frequency and symbol rate can change within the boundary in response to noisy line conditions, based on the defined upstream parameters.
- **Multiple subbands**—The data carrier can remain in a particular subband for a duration of time and then hop to another subband based on the defined upstream parameters.



Tip

Measurement of noise power levels with a spectrum analyzer should be part of the procedure in initially selecting and setting up frequency allocations. Cisco recommends having fixed frequency settings during early deployment, at least until amplifier cascade adjustments or plant repair have become infrequent enough that they no longer significantly affect the nodes connected to the upstream port.

Upstream Frequency Changes

As stated in the DOCSIS radio frequency interface (RFI) specification, RF channel migration or upstream frequency change occurs when a change in the UCD message is broadcast to all cable interfaces.

The speed of channel migration via the UCD message is typically less than 20 milliseconds (ms). During this time, upstream transmission is interrupted until the cable interface transmitter adjusts to its new frequency. Data is stored in the cable interface's buffers during this time and is sent when the frequency hop is complete.

Station maintenance intervals are used to perform per-modem keepalive polling. The CMTS polls each cable modem at least once every 30 seconds, with the default being once every 25 seconds. When ingress noise causes loss of keepalive messages from a configurable percentage of all cable interfaces, resulting in missed polls, a new frequency is selected from the allocation table and a UCD update is performed. The migration time is 2 msec for any upstream UCD update. After the UCD is updated, the hop occurs. The system must wait until a hop-threshold time interval has elapsed before it can change the UCD a second time.

Upstream Segments and Combiner Groups

The Cisco routers divide a cable plant into downstream channels. Downstream channels contain upstream segments. Each upstream segment typically serves more than one fiber node. Upstream segments can be defined as one of the following:

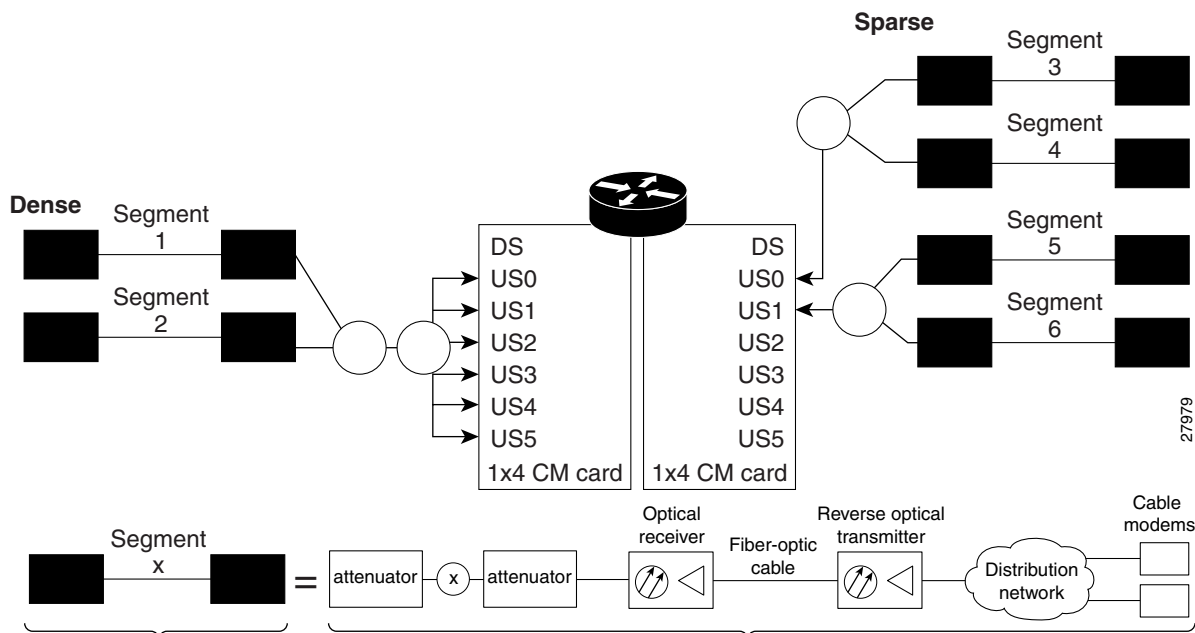
- Sparse segment—Containing one upstream channel per upstream segment.
- Dense segment—Containing multiple upstream channels per upstream segment; frequencies must be different.

**Note**

A cable interface line card can support sparse or dense segments, or both.

Defining sparse segments allows the cable operator to share upstream bandwidth among fiber nodes with fewer subscribers. Defining dense segments allows the cable operator to provide larger upstream bandwidth to fiber nodes with many subscribers.

[Figure 7](#) illustrates sparse versus dense segments.

Figure 7 Sparse Versus Dense Segment Illustrations

As shown in Figure 7, the downstream segment can contain multiple upstream segments. Two fiber nodes can be in one downstream segment but in different upstream segments.

The return path of several fiber nodes can be combined at a single point to form a single RF frequency domain called a combiner group. The CMTS software allows a frequency hop table called a spectrum group to be associated with a combiner group.

**Note**

A combiner group refers to an RF topology point. A spectrum group refers to the frequency hop table associated with a combiner group.

Frequency Management Policy

Spectrum management applies a common frequency-management policy to a set of upstream ports to ensure that data is delivered reliably over the cable plant. Cable plant operators must make noise measurements and determine the cable plant's spectrum management policy. Different modulation schemes, upstream frequency techniques, and symbol rates are used based on the cable plant characteristics and the cable interface line card in the chassis.

See the following sections for more information about these topics:

- [Noise Impairments, page 369](#)
- [Spectrum Groups and Frequency Hopping, page 369](#)
- [Guidelines for Spectrum Management, page 370](#)

Noise Impairments

Upstream noise impairments such as signal degradation on cable networks can negatively affect service to subscribers. Two-way digital data signals are more susceptible than one-way signals to stresses in the condition of the HFC network. Degradation in video signal quality might not be noticeable in one-way cable TV service, but when two-way digital signals share the network with video signals, digital signals can be hampered by:

- **Impulse and electrical signal ingress**—Noise can enter the network from electrical sources within a residence or from high-voltage lines that run near CATV cabling. Two types of ingress noise include broadband and narrowband. Broadband noise is generally of lower frequency (below 10 MHz) and results in harmonic rolloff. Narrowband noise is a more significant interference source. Cable equipment and infrastructure often pick up noise from amateur radio transmissions, citizen band radios, or high-power shortwave broadcast signals. Implement a signal leakage maintenance program to locate and repair areas of signal ingress.
- **Amplifier noise**—Amplifiers add noise to the HFC network that typically goes unnoticed in video signals, but degrades digital data signals if amplifiers are improperly configured. The larger the network, the higher the probability of amplifier noise affecting signals.
- **Noise funneling**—The upstream data path to the headend is susceptible to interference from the entire network. All upstream noise ultimately ends up at the headend because the cumulative nature of noise becomes concentrated at the headend. As a network serviced by a single RF receiver increases in size, the probability of noise funneling also increases.
- **Variable transmit levels**—Temperature affects signal loss over coaxial cable. This can cause variations of 6 to 10 dB per year.
- **Clipping**—The lasers in fiber-optic transmitters can stop transmitting light when input levels are excessive. Excessive input levels introduce bit errors in both the upstream and downstream transmissions. If a laser is overdriven as briefly as a fraction of a second, clipping can occur.

To adjust your return amplifiers and lasers, follow rigorous plant maintenance procedures documented in the *NTSC Supplement on Upstream Transport Issues* or appropriate cable plant standard. Also refer to the hardware installation guide that ships with your CMTS.

Spectrum Groups and Frequency Hopping

We recommend that CMTS administrators configure upstream frequency hopping to counteract long-term, narrowband noise. Cisco CMTS routers support a combination of guided frequency hopping and time-scheduled frequency hopping.

The frequency hop to proactively avoid noise ingress is sometimes called frequency agility. Frequency agility is configured and activated using spectrum groups. Spectrum management supports the creation of a number of cable spectrum groups, allowing multiple upstream ports in a single spectrum group. Each spectrum group defines the table of frequencies to be used in a specific frequency plan. Upstream frequencies can be a fixed single frequency, a single continuous range of frequencies (band), or multiple ranges (or bands) of frequencies.

The cable interface does not operate until you assign a frequency to the upstream, which can be done either by configuring and assigning a spectrum group or assigning a fixed frequency. The spectrum group takes precedence, so if you configure both a spectrum group and a fixed frequency on an upstream, the spectrum group overrides the fixed upstream frequency setting.

From the interface point of view, a spectrum group also represents the set of upstreams connected to the same group of fiber nodes. The spectrum manager software in Cisco routers examines all the RF parameters that have been configured on an upstream to determine whether the upstream frequencies

need to be managed together. For example, if you configure a spectrum group with several fixed frequencies, but those frequencies are all within the configured channel width, the spectrum manager software combines the frequencies into a single band.

The upstream ports use the spectrum group to determine which frequencies are available if frequency hopping is needed to deal with noise or other path impairments. The types of frequency hopping techniques are guided, time-scheduled, and a combined guided and time-scheduled. See the [“Frequency Hopping Capabilities” section on page 372](#) for more information on the types of frequency hopping techniques.

**Note**

When each upstream port has its own RF domain, the group is called a nonshared spectrum group. When multiple upstream ports share the same RF domain, the group is called a shared spectrum group.

Guidelines for Spectrum Management

In general, when defining your spectrum, use the following guidelines:

- Avoid frequencies with known ingress problems, such as amateur radio bands or short-wave bands.
- Avoid hostile spectrum below 20 MHz.
- Allow extra bands for frequency hopping.
- Take the possible channel widths into account when creating frequency bands. The range of frequencies being used must be able to hop between at least two different frequencies when using the channel width that is configured on the upstream.
- Place upstream ports in the same combiner group in a shared spectrum group.
- Use the receive power level setting to perform slight equalization adjustments.
- If you combine multiple upstream ports to provide increased bandwidth, you must avoid overlapping frequency bands. Each port should be using a discrete band of frequencies that does not overlap the bands being used by other ports in the group. We recommend adding at least 20 KHz between the ending frequency of one band and the starting frequency of the next band, to ensure that the bands do not overlap.

Guided and Scheduled Spectrum Management

Guided and Scheduled spectrum management constitutes a set of basic features for all currently supported cable interface line cards. These features are considered basic because they are available for all cable interfaces, and constitute the elementary, cornerstone features upon which the Intelligent and Advanced spectrum management features are built.

See the following sections for more information about each feature:

- [Traffic Shaping, page 371](#)
- [Frequency Hopping Capabilities, page 372](#)
- [Dynamic Upstream Modulation \(SNR-based\), page 374](#)
- [Input Power Levels, page 376](#)

Traffic Shaping

Traffic shaping basically uses queues to limit data surges that can congest a network. The data is buffered and then sent into the network in regulated amounts to ensure that the traffic fits within the expected traffic envelope for the particular connection.

Traffic shaping reduces the chance that information must be retransmitted to hosts on the cable plant. When cable modems (CMs) have rate limits established, the CMTS typically drops data packets to enforce the rate limit. Dropping packets from the requesting CM causes the host sending the information to retransmit its information, which wastes bandwidth on the network. If both hosts sending and requesting information are on the cable plant, the upstream bandwidth is wasted as well.

Traffic shaping allows the CMTS to perform upstream and downstream rate limiting on the DOCSIS upstream and downstream channels. Rate limiting restricts the data rate to and from a CM; the MAC scheduler supports traffic-shaping capabilities for downstream and upstream traffic. Rate limiting ensures that no single CM consumes all of the channel bandwidth and allows a CMTS administrator to configure different maximum data rates for different subscribers. Subscribers requiring higher peak rates and willing to pay for higher rates can be configured with higher peak rate limits in their CM DOCSIS configuration file over regular subscribers, who pay less and get lower rate limits.

Each time a packet belonging to a flow is transmitted on an output channel, the token-bucket policer function checks the rate limit status of the flow, passing the following parameters:

- Token bucket peak rate in bits/msec.
- Token bucket depth (maximum transmit burst) in bits.
- Length of current packet to be sent in bits.
- Pointer to the flow's token bucket.
- Pointer to the flow's token bucket last update time stamp.
- Variable to return the msec buffering delay in case the packet needs to be shaped.
- Maximum buffering delay that the subsequent traffic shaper can handle in msecs.

Every flow has its own shaping buffer where rate-exceeded packets are typically held back in first-in/first-out (FIFO) order for later transmission.

**Tip**

Token bucket policing with shaping is the new per-upstream default rate limiting setting at the CMTS. Shaping can be enabled or disabled for the token-bucket algorithm.

Upstream Traffic Shaping

Upstream traffic shaping allows the CMTS to perform rate limiting on a DOCSIS upstream channel. The upstream traffic shaping feature delays the scheduling of the upstream packet, which in turn, causes the packet to be buffered on the cable modem device, instead of being dropped. This allows the user TCP/IP stack to pace the application traffic appropriately and approach throughput commensurate with the subscriber's defined quality of service (QoS) levels. Upstream traffic shaping enables the CMTS to enforce the peak upstream rate for each CM without degrading overall TCP performance for the subscriber CMs.

When you do not enable the shaping option for upstream rate limiting, the CMTS upstream-rate-policing code drops bandwidth requests from cable modems that are found to have exceeded their configured-peak-upstream rate (using different local drop policies). The effect of bandwidth requests (eventually upstream packets) being dropped causes degraded throughput performance of window-based protocols (like TCP) for these rate-exceeded modems because of the timeouts and retransmits that follow.

Upstream grant shaping is on a per-CM (SID) basis. The grant shaping feature is a configurable option for the current upstream token-bucket rate-limiting algorithm.

A traffic shaping feature is restricted QoS class assignment, which allows a CMTS administrator to override the class of service provisioned for a CM. When this feature is enabled, the user-defined QoS profile is enforced on the CM attempting to register with the CMTS, regardless of the CM's provisioned class of service. Use the **cable qos profile** command to configure a QoS profile.

**Note**

The restricted QoS class assignment feature is added to address instances where a cable operator implemented rate limiting incorrectly. The feature allows an administrator to override the statically provisioned QoS parameters of the CM and force the CM to use a specific QoS profile defined at the CMTS.

For configuration task information on upstream traffic shaping, refer to the [“Enabling Upstream Rate Limiting” section on page 382](#).

Downstream Traffic Shaping

The CMTS supports basic downstream traffic shaping by effecting data rate limiting on a per-modem basis. A downstream traffic shaping feature called downstream rate limiting with type-of-service (ToS) bits extends that capability by allowing the CMTS administrator to configure the ToS byte to calculate the data rate for a specified flow.

Downstream rate limiting with ToS bits enables you to partition downstream traffic for a CM into multiple classes of service and multiple data rates by using the three precedence bits in the ToS byte in the IP header to specify a class of service assignment for each packet. Those packets with the precedence bit set in the ToS field are given higher priority. Using the ToS byte, you can calculate the data rate for a specified flow, in addition to the data rate configured on a per-CM basis. By specifying a maximum data rate for a particular ToS, you can override the common maximum downstream data rate.

The administrator can override the maximum common downstream data rate limits by configuring the ToS byte.

**Note**

Packets that contain ToS bytes that have not been configured for downstream data rates continue to use the common data rate limits.

Frequency Hopping Capabilities

Noise in the upstream transmission line, that is from the consumer to the service provider, can degrade data transmission from the subscriber's home. If the noise impairment is of substantial duration, it may cause the cable modem to temporarily lose communication with the headend facility. As a contingency plan, the multiple service operators (MSOs) can reserve multiple channels or upstream frequencies for their subscribers. If one channel suffers too much interference, the CMTS requests that the cable modems “hop” to another channel.

To provide frequency hopping capability, Cisco CMTS routers contain a spectrum manager that continuously monitors the noise in unused upstream channels. If the CNR reaches an unacceptable level on a particular channel, the spectrum manager automatically assigns a new upstream channel to the cable modem using that channel.

Cisco CMTS routers support the following techniques for upstream frequency hopping when the frequency band in use is not clean:

- Guided frequency hopping—In guided frequency hopping (also known as blind hopping), the spectrum manager automatically assigns a new upstream channel frequency when a configurable threshold of station maintenance (keepalive) messages fails. Failed station maintenance messages represent an impairment of the upstream channel due to noise, plant, or equipment failure. Explicit frequency subbands and associated input power levels are assigned in a spectrum group in guided frequency hopping.
- Time scheduled frequency hopping—Frequency reassignment is scheduled by the time of day or by a specific day of the week.
- Combined guided and time-scheduled frequency hopping.

**Note**

Frequency hopping is not effective against broadband noise phenomena such as impulse noise.

Time-scheduled and guided hopping techniques are independent concepts:

- The spectrum is controlled by a script, not a frequency table.
- The available spectrum is time-scheduled as an option.
- A guided hopping frequency is selected from the available spectrum at the current time.

You can configure and activate frequency hopping by using spectrum groups. You can create up to 32 cable spectrum groups, each containing multiple upstream ports. The configured channel width is used for each upstream frequency.

After you have created one or more spectrum groups for your cable network, you can add characteristics to them, providing you with more definitive control over frequency usage and frequency hopping.

You can configure hopping thresholds. For example, the frequency hop threshold percentage method prevents a single failing cable modem from affecting service to other working cable modems. As long as a high enough threshold is configured, the system does not hop endlessly due to a single cable modem failing to respond to 90 percent of its station maintenance (keepalive) messages.

You can also configure the minimum period between frequency hops, with a default setting of 300 seconds. If the destination channel is expected to be impaired, you can reduce the minimum period between frequency hops to a small value, such as 10 seconds. This allows the frequency hop to continue more rapidly until a clear channel is found. If excessive frequency hop is an issue, you can increase the minimum period between hops.

To configure different techniques of frequency hopping, see the [“Creating and Configuring Spectrum Groups”](#) section on page 385.

**Note**

Spectrum management is not supported for one-way (telco return) cable modems, because spectrum management capabilities focus on the upstream path over an HFC network.

Guided Frequency Hopping

Guided frequency hopping is called “guided” because the frequency hopping uses the frequencies that are specified in the spectrum group, which can be either a set of discrete frequencies or a band. The cable interface cards that support guided frequency hopping do not have a “look-ahead” mechanism that would allow them to determine the quality of the new frequency or band ahead of time, which is why previous

documents referred to this as blind hopping. Because of this, though, the cable interface does not need to perform any search on the new potential frequencies, so the switching time between frequencies is only approximately 20 ms.

You can specify some rules the system uses when hopping to another frequency when the frequency band in use is not clean. You can assign explicit frequency subbands and associated input power levels in a spectrum group. All cable modems then on the upstream port migrate to the next frequency with an assigned input power level. The number of lost station management messages exceeding a configured threshold can initiate an upstream channel frequency reassignment. For example, you can specify a frequency hop based on lost station management messages that exceed a threshold. The default threshold may be 10 to 20 percent depending on the Cisco IOS release. The frequency change occurs rapidly without data loss and with minimal latency.

Take care to reduce the spectrum allocation when it is used with small channel widths. Otherwise, there will be a large number of upstream channel slots. For example, if the allocation is from 20.0-to-28.0 MHz and an upstream port has its channel width set to 0.2 MHz, there are 40 possible slots for that channel width. Guided frequency hopping can require a long time to find the clean slot, because it tries each available slot, one at a time, for several seconds during each try.

Time-Scheduled Frequency Hopping

You can specify upstream channel frequency reassignment based on a configured time of every day or of a specific day of the week. If your cable plant has an upstream noise characteristic on a weekly cycle, use time-scheduled spectrum allocation. With a time-scheduled policy, a single frequency becomes valid at any given time.

Dynamic Upstream Modulation (SNR-based)

The basic Dynamic Upstream Modulation feature is supported on all Cisco cable interface line cards beginning with Cisco IOS Release 12.1(3a)EC1, Cisco IOS Release 12.2(4)BC1b, and later releases. This section describes the operation of this feature, which is based on evaluating the signal-to-noise ratio (SNR) of an upstream.



Note

A more advanced version of Dynamic Upstream Modulation, which uses the carrier-to-noise ratio (CNR), is supported on the cards that support intelligent and advanced spectrum management (such as the Cisco uBR-MC16S/U/X and Cisco uBR-MC28U/X). See the [“Intelligent and Advanced Hardware-Based Spectrum Management”](#) section on page 376 for more information on that version of this feature.

Feature Overview

Cisco cable interface line cards monitor the SNR values and the forward error correction (FEC) counters in the active return path of each upstream port. The Dynamic Upstream Modulation software determines whether upstream channel signal quality can support the modulation scheme configured, and adjusts to the most robust modulation scheme when necessary. When return path conditions improve, this feature returns the upstream channel to the higher modulation scheme that includes the modulation profile.

A modulation profile is a collection of six burst profiles that are sent out in a UCD message to configure modem transmit parameters for the upstream message types: request, request/data, initial maintenance, station maintenance, short grant, and long grant. Dynamic Upstream Modulation adjusts the modulation profiles of an upstream channel based on upstream signal quality.

Dynamic Upstream Modulation can be configured on interfaces with fixed upstream frequencies or on interfaces with assigned spectrum groups. For information on commands to configure Dynamic Upstream Modulation, see [“Configuring Dynamic Upstream Modulation \(SNR-Based\)” section on page 391](#).

On second generation cable interface line cards, such as the Cisco uBR-MC16C, the Dynamic Upstream Modulation feature can also automatically switch the modulation profile between QAM-16 to QPSK to respond to noise on the upstream path. For example, you can configure the Dynamic Upstream Modulation feature on the Cisco CMTS using the following primary and second modulation profiles:

- The primary modulation profile uses QAM-16, which is a more bandwidth-efficient modulation scheme and has a higher throughput than a QPSK profile.
- The secondary modulation profile uses QPSK, which uses a more robust modulation scheme, but at the cost of not being as bandwidth-efficient.

We recommend that the primary profile uses QAM-16 modulation and the secondary uses QPSK, but this is optional. Both modulation profiles can be either QPSK or QAM-16. It is not mandatory that one is QAM-16 and the other QPSK, but modulation profile switchover is tied to the QAM-16 and QPSK thresholds.



Tip

Cisco IOS Release 12.2(15)BC2 introduced a series of robust predefined modulation profiles that can also be used with the Dynamic Upstream Modulation feature. See the description of the **cable modulation-profile** command in the *Cisco CMTS Command Reference Guide* for more information.

Criteria for Switching Modulation Profiles

The Dynamic Upstream Modulation feature uses the following criteria to determine whether it should switch from the primary modulation profile 1 (the more bandwidth-efficient, but less robust profile) to the secondary modulation profile (more robust, but less bandwidth profile):

- The upstream SNR goes below 25dB (SNR < 25dB)
OR
- The number of correctable FEC errors is more than 3 percent of the packets received in a 15-second time period
OR
- The number of uncorrectable FEC errors is more than 1 percent of the packets received in a 15-second time period.

Before switching back to the primary modulation profile, the following criteria must be satisfied:

- The upstream SNR is above 28dB (SNR > 28dB)
AND
- The number of correctable FEC errors is less than 3 percent of the packets received in a 15-second time period
AND
- The number of uncorrectable FEC errors is less than 1 percent of the packets received in a 15-second time period.

It is important to note that the initial switch from the less robust to the more robust profile (from the primary profile to the secondary profile) is based on OR conditions, where only one of the conditions is necessary to perform the switch. The switch back to the primary profile is based on AND conditions, in which all conditions must be satisfied before the cable interface switches back.

If the only problem is that the upstream is experiencing a large number of uncorrectable errors, then a situation could occur where the router continues to switch back and forth between profiles. The uncorrectable errors occur with the primary profile, so the router switches to the secondary profile. The secondary profile does not experience any problems, so the router switches back to the primary profile. But the uncorrectable errors reoccur and the router switches back to the secondary profile, and this cycle continues indefinitely.

To avoid this problem, make sure that the cable plant is capable of supporting the modulation scheme being used in the primary profile (for example, 16-QAM). If you cannot guarantee successful operation on an upstream using this modulation scheme, then you should select a primary profile that uses a more bandwidth-efficient set of burst parameters (such as QPSK). The Cisco IOS software includes predefined modulation profiles that can be used for both the primary and secondary profiles.

Input Power Levels

Upstream input power level modifications were made in Cisco IOS Releases 12.0(6)SC, 12.1(1), 12.1(1)T, 12.1(2)EC1, and 12.2(4)BC1b. The input power level, *power-level-dBmV*, is an option in the **cable spectrum-group** command. The option allows you to specify the expected U.S. input power levels on the upstream receivers on the CMTS when the cable modems are hopping from one fixed frequency to another or from one band to another. Each upstream frequency has an associated upstream input power level in dBmV. The power level is the modem transmit power that each spectrum group can use when an upstream frequency change is necessary. The input power level may be set at the time of the frequency hop.

Specifying an input power level is done so that the cable modems do not have to increase or decrease their transmit power with every hop. The cable operator can perform minor power equalizations as a function of frequency. The valid range is -10 to +10dBmV. The power level value should be changed only if you want to change the power level as part of spectrum management. Some cable plants may want to change only the input power level, and not the frequency, on a daily time schedule.

For information on how to configure input power levels, see the [“Configuring and Assigning Spectrum Groups” section on page 396](#).

Intelligent and Advanced Hardware-Based Spectrum Management

Several cable interface line cards include hardware-based spectrum management features that provide enhancements to the basic features supported by the other Cisco cable interface line cards. (See [Table 6 on page 356](#) for a list of supported cable interface line cards and required Cisco IOS releases.)



Note

The Cisco uBR10012 universal broadband router using Cisco IOS Release 12.2(8)BC2 and the Cisco uBR-LCP2-MC16S cable interface line card supports a subset of these features. See the [“Cisco uBR10012 Router and Cisco IOS Release 12.2\(8\)BC2 Support” section on page 357](#) for more details.

Intelligent Spectrum Management Enhancements

Initial Intelligent spectrum management enhancements were introduced on the Cisco uBR-MC16S line card in Cisco IOS Release 12.1 EC. Initial support for the Cisco uBR-MC16S card also appeared in Cisco IOS Releases 12.0(7)XR3, 12.1(1a)T1, 12.1(2)EC, and 12.2(8)BC2, and included the following features:

- Integrates a DOCSIS cable interface line card with an onboard spectrum analyzer that continuously analyzes the upstream spectrum quality in the DOCSIS frequency range of 5 to 42 MHz.
- Includes hardware-assisted frequency hopping, providing for more intelligent and faster frequency selection than software-only solutions.
- Reduces the response time to ingress noise that could cause modems to drop offline.
- Eliminates blind frequency hopping by initiating frequency hops to known clean channels.
- Improves frequency agility to help eliminate dropped packets and thereby maintain full upstream data rates.
- Supports frequency agility in dense-mode combining environments across a shared spectrum.
- Restricts frequency hopping to a set of discrete fixed frequencies or to a range of frequencies, as desired.
- Allows frequency hop conditions to be customized for specific plant environments and requirements.
- Optionally schedules frequency hops to take advantage of known usage patterns or plant conditions.
- Optionally dynamically reduces channel width to allow cable modems to remain online, even in noisy upstream conditions.

Advanced Spectrum Management Features

The Advanced spectrum management features were introduced on the Cisco uBR-MC16S cable interface line card as a software-only upgrade. These enhancements were supported on additional line cards on the Cisco IOS Releases that are shown in [Table 6 on page 356](#).

The following additional features are part of the Advanced spectrum management feature set:

- Supports proactive channel management, to avoid the impacts of ingress and keep subscribers online and connected.
- Offers flexible configuration choices, allowing users to determine the priority of the actions to be taken when ingress noise on the upstream exceeds the allowable thresholds. The configurable actions are frequency hopping, switching the modulation profile, and reducing the channel width.
- Performs carrier-noise ratio (CNR) calculations using Digital Signal Processor (DSP) algorithms in real-time on a per-interface and a per-modem basis.

**Note**

In Cisco IOS Release 12.2(8)BC2 and later Cisco IOS 12.2 BC releases, the CNR value is typically more accurate than the SNR value because the CNR value is an estimate calculated on a per modem basis, while the SNR value is a general estimate for the entire upstream. For this reason, the CNR and SNR values might not exactly match for any particular period.

- The CNR-based version of the Dynamic Upstream Modulation feature intelligently determines when to modify the frequency, channel width, or modulation profile, based on CNR calculations in the active channel and the number of correctable FEC errors and uncorrectable FEC errors. Frequency hopping, channel width change, or profile change occurs in the following circumstances:
 - The CNR value falls below the user-defined threshold value for the primary modulation profile, AND
 - Either the correctable FEC error value exceeds its user-defined threshold, OR

- The uncorrectable FEC error value exceeds its user-defined threshold.

This logic can be expressed as the following formula:

```
(CNR <= threshold) AND  
( (correctable FEC >= threshold) OR (uncorrectable FEC >= threshold) )
```

This approach helps avoid unneeded channel changes due to transient noise problems that do not actually cause any errors in the data stream. The channel changes only when noise both affects the CNR of the upstream and generates an unacceptable number of FEC errors in the data. If you want channel changes to occur only in response to the CNR, you can set the FEC error threshold values to zero.

Separate CNR threshold values are configured for the primary and secondary modulation profiles. When the upstream has moved to the secondary modulation profile, further frequency hopping or channel width changes occur only when the CNR value falls below the user-defined threshold value for the secondary profile.



Note Previously, channel hopping occurred when the number of missed station maintenance polls exceeded a user-defined threshold or the SNR reported from the Broadcom chip exceeded a certain threshold.

- Enhances the Dynamic Upstream Modulation feature for the Cisco uBR-MC16S line card. This feature supports dynamic modulation using two upstream profiles. The primary profile (typically using QAM-16 “mix” modulation) remains in effect at low noise conditions, but if upstream conditions worsen, the cable modems switch to the secondary profile (typically using QPSK modulation) to avoid going offline. When the noise conditions improve, the modems are moved back to the primary profile.



Note The Dynamic Upstream Modulation feature was introduced in Cisco IOS Release 12.1(3a)EC1. The above enhancements to this feature exist only in Cisco IOS Release 12.2(8)BC2 and later Cisco IOS 12.2 BC releases; they are not supported in any Cisco IOS 12.1 EC release.

- When using a Cisco uBR-MC16S line card on a Cisco CMTS router running Cisco IOS Release 12.2(8)BC2 and later Cisco IOS 12.2 BC releases, the spectrum management hardware uses the real-time CNR readings from the DSPs onboard the Cisco uBR-MC16S line card, instead of the signal-to-noise ratio (SNR) values from the Broadcom 3137 chip, to determine the signal quality of the upstream channel. The CNR value is a more accurate description of noise conditions on the upstream.
- Provides an SNMP interface so that a network management workstation or other graphical tool can obtain spectrum information for either a particular cable modem or for an entire upstream. The frequency resolution can be as fine as 12 KHz.



Note The CISCO-CABLE-SPECTRUM MIB has been enhanced to provide this support.

Benefits

The spectrum management features provided on the Cisco CMTS router platforms provide several key system benefits:

- Improves response time to ingress noise impairments that appear in the upstream return path.
- Boosts the percentage of modems online.
- Mitigates the impact of ingress to subscriber services.
- Saves time and effort by MSO operations staff when troubleshooting minor plant outages.
- Increases cable plant reliability.
- Maximizes spectrum utilization.

Guided and Scheduled Spectrum Management Benefits

The following summarizes the specific benefits of the Guided and Scheduled spectrum management features that are supported for all Cisco CMTS router platforms.

Upstream Traffic Shaping

- The CMTS can buffer the grants for rate-exceeded modems. This grant buffering at the CMTS avoids TCP-related timeouts and retransmits, resulting in an improved TCP throughput performance for the rate-exceeded modems. Thus, traffic shaping enables the CMTS to enforce the peak upstream rate for the modem without degrading overall TCP performance for the modem.

Downstream Traffic Shaping

- Allows users to configure multiple data rates (defined by the value of the IP precedence bits in the ToS byte) for a given modem. By specifying a maximum data rate for a particular ToS, users can override the common maximum downstream data rate.

Input Power Levels

- Allows the cable plant operator to perform minor power level equalization as a function of frequency.

Frequency Hopping Capabilities

- Proactively countermeasures upstream noise impairments by assigning a new upstream channel to the cable modem. MSOs can take advantage of this feature especially when they have less than an optimal carrier-to-noise ratio in the upstream frequencies or when their cable plants exhibit random bursts of ingress noise that affect reliability.

Dynamic Upstream Modulation

- Reduces the risk associated with transitioning to QAM-16 modulation in the return path and provides assurance that subscribers remain online and connected during return path impairments.
- Checks that the active upstream signal quality can support the configured modulation scheme and proactively adjusts to the more robust modulation scheme when necessary.
- Eliminates the necessity to hop channels for cable modems to stay online by automatically switching from the primary modulation profile to the secondary modulation profile.

Intelligent and Advanced Spectrum Management Benefits

The following summarizes the specific benefits of the Advanced spectrum management features that are supported on Cisco CMTS routers using supported cable interface line cards:

Hardware-Assisted Spectrum Management

- Offloads much of the spectrum management processing from the main system processor to the Digital Signal Processing (DSP) hardware onboard the Cisco uBR-MC16S line card, freeing up the main processor for other duties.

Dynamic Channel Width Change

- Improves the DOCSIS upstream channel availability by finding the maximum possible channel width for an upstream when noise conditions make the current channel width unusable.
- Provides the maximum RF spectrum utilization efficiency for current plant conditions.
- Customizable range of channel widths that can be used to respond to noise problems.

Intelligent Frequency Hopping

- Proactively changes upstream frequency for an interface before noise conditions become severe enough to force cable modems offline.
- Dedicated hardware intelligent performs “look-ahead” to choose new upstream frequency to find a stable channel.
- Flexible priority configuration allows hopping decision criteria to be tailored to the individual cable plant environment.
- Improves responsiveness to ingress impairments, by matching the hopping decision criteria to the fluctuating plant conditions.
- Pinpoints CNR variations with per-modem accuracy to isolate problematic cable modems.
- Sustains or even improves subscriber online percentages through user-programmable proactive channel management techniques.

Dynamic Upstream Modulation

- Reduces the risk associated with switching between QPSK and QAM-16 modulation in the upstream to respond to ingress noise, so that subscribers remain online and connected.
- Checks the current upstream signal to ensure that it can support the configured modulation scheme, and proactively adjusts to the secondary, more robust modulation scheme when necessary.
- Improves DOCSIS upstream channel availability and provides maximum RF spectrum utilization efficiency.
- Eliminates unnecessary frequency hopping by switching modulation profiles to one that allows cable modems to remain online while using the currently assigned upstream.
- Provides assurance that subscribers remain online and connected during periods of return path impairments

SNMP Interface

- Provides a way to remotely obtain the current status of noise on an upstream. This information can then be inserted into third-party or custom reporting and graphing applications.
- Provides visibility to ingress and impulse noise under the carrier frequency on a per-port basis.
- Provides an easy-to-use, distributed method to remotely gather real-time display of the DOCSIS upstream spectrum for individual cable modems and set-top boxes (STBs).
- Reduces the reliance on costly spectrum analyzers at every headend or hub.
- Quickly provides spectrum views through an intuitive interface, without the complicated setup time of a spectrum analyzer.

- Allows the technician to troubleshoot the network remotely, as opposed to having to be physically present to connect and use a spectrum analyzer.

How to Configure Spectrum Management

This section describes the configuration tasks that are most commonly performed when using the spectrum management features on the Cisco CMTS platforms. See the following sections for the configuration tasks that are appropriate for your platform and cable interface line cards.

- [Guided and Scheduled Spectrum Management Configuration Tasks, page 382](#)
- [Intelligent and Advanced Spectrum Management Configuration Tasks, page 396](#)

Guided and Scheduled Spectrum Management Configuration Tasks

The following tasks configure the Guided and Scheduled spectrum management features that are supported on all Cisco CMTS platforms:

- [Enabling Upstream Rate Limiting, page 382](#)
- [Enabling Downstream Rate Limiting, page 384](#)
- [Creating and Configuring Spectrum Groups, page 385](#)
- [Assigning a Spectrum Group to One or More Upstream Ports, page 389](#)
- [Configuring Dynamic Upstream Modulation \(SNR-Based\), page 391](#)
- [Verifying Frequency Hopping, page 393](#)

Enabling Upstream Rate Limiting

Upstream rate limiting allows upstream bandwidth requests from rate-exceeding cable modems to be buffered without incurring TCP-related timeouts and retransmits. This enables the CMTS to enforce the peak upstream rate for each cable modem without degrading overall TCP performance for the subscriber customer premises equipment (CPE) devices. Upstream grant shaping is per SID.

By default, all upstreams are configured for rate limiting that uses the token-bucket policing algorithm with traffic shaping, which enforces strict DOCSIS-compliant rate limiting. If you have previously disabled or reconfigured rate limiting on an upstream, use the following procedure to reenables rate limiting on that upstream.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface cable *x/y***
or
interface cable *x/y/z*
4. **cable upstream *usport* rate-limit [token-bucket [shaping]]**
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	interface cable x/y or interface cable x/y/z Example: Router(config)# interface cable 5/1 Router(config-if)#	Enters interface configuration mode for the specified cable interface.
Step 4	[no] cable upstream usport rate-limit [token-bucket [shaping]] Example: Router(config-if)# Router(config-if)#	Enables rate limiting for the specified upstream port. • token-bucket—(Optional, default) Enables rate limiting for the upstream port using the token-bucket policing algorithm, so that the router automatically drops packets in violation of allowable upstream bandwidth. • shaping—(Optional, default) Enables rate limiting for the upstream port employing the token-bucket policing algorithm with traffic shaping to enforce strict DOCSIS-compliant rate limiting. We recommend this configuration, because not specifying the shaping option could result in unacceptable jitter in DOCSIS 1.1 networks. Use the no version of this command to disable rate limiting on an upstream, but we do not recommend doing this.
Note Repeat Step 3 through Step 4 for each upstream port to be configured.		
Step 5	end Example: Router(config-if)# end Router#	Exits interface configuration mode and returns to privileged EXEC mode.

Enabling Downstream Rate Limiting

Downstream rate limiting enables you to use the token-bucket policing algorithm with traffic shaping options or the weighted-discard policing algorithm to buffer, shape, or discard packets that exceed a set bandwidth. Downstream rate limiting is disabled by default.

To enable downstream rate limiting for a downstream port on a Cisco cable interface line card, use the following procedure.

SUMMARY STEPS

- 1. **enable**
- 2. **configure terminal**
- 3. **interface cable *x/y***
or
interface cable *x/y/z*
- 4. **cable downstream rate-limit** [token-bucket [shaping] [granularity *msec* | max-delay *msec* | weighted-discard *exp-weight*]]
- 5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	interface cable <i>x/y</i> or interface cable <i>x/y/z</i> Example: Router(config)# interface cable 5/1 Router(config-if)#	Enters interface configuration mode for the specified cable interface.

	Command or Action	Purpose
Step 4	[no] cable downstream rate-limit [token-bucket [shaping] [granularity msec max-delay msec weighted-discard exp-weight]] Example: Router(config-if)# Router(config-if)#	Enables rate limiting on the downstream. You can also specify the following options: • token-bucket—(Optional) Enables rate limiting on the downstream port using the token-bucket policing algorithm. With this command, the CMTS automatically drops packets that are in violation of the allowable bandwidth. • shaping—(Optional) Enables rate limiting on the downstream port using the token-bucket policing algorithm with traffic shaping. • granularity msec—(Optional) Enables rate limiting on the downstream port using the token-bucket policing algorithm with specific traffic-shaping time granularity. The valid values are 1, 2, 4, 8, or 16 milliseconds. • max-delay msec—(Optional) Enables rate limiting on the downstream port using the token-bucket policing algorithm with specific maximum traffic-shaping buffering delay. The valid values are 128, 256, 512, or 1028 milliseconds. • weighted-discard exp-weight—(Optional) Enables rate limiting on the downstream port using the weighted-packet discard policing algorithm and the specified weight for the exponential moving average of loss rate. The valid values are 1 to 4.
	Note Repeat Step 3 through Step 4 to configure each downstream interface.	
Step 5	end Example: Router(config-if)# end Router#	Exits interface configuration mode and returns to privileged EXEC mode.

Creating and Configuring Spectrum Groups

A spectrum group defines the frequencies that an upstream is allowed to use when frequency hopping is done, as well as other parameters that control the frequency hops. When creating and configuring spectrum groups, you can specify the following parameters:

- Frequencies that are assigned to the group. The cable interface uses these frequencies to determine what frequencies are available to use when frequency hopping is needed. You can specify either a list of fixed frequencies or a band of frequencies, or both. The Cisco CMTS uses the following rules when adding frequencies to a spectrum group:
 - When specifying a fixed frequency, the Cisco CMTS assumes it is a center frequency with a 6.4 MHz channel width, to allow that frequency to operate at all possible channel widths. For example, specifying a frequency of 17,700,000 Hz is equivalent to specifying a frequency band from 14,500,000 Hz to 20,900,000 Hz (a band that is 6.4 MHz wide).

- If you configure multiple fixed frequencies or bands of frequencies that overlap, the spectrum group combines them into one band. For example, if you specify a fixed frequency of 17,700,000 Hz and a band from 15,800,000 Hz to 25,200,000 Hz, the spectrum group is configured with one band from 14,500,000 Hz to 25,200,00 Hz.

If you want more control over a spectrum group's frequencies, configure bands of frequencies with the same width as the desired channel width. For example, if you want to use a center frequency of 17,700,000 Hz with a 3.2 MHz channel width, specify a band that ranges from 16,100,000 Hz to 19,300,000 Hz. To ensure you configure non-overlapping bands, separate the bands by a minimum of 20 KHz.

- Upstream input power level—(Optional) Power level, in dBmV, that the upstream should use when hopping to a new frequency. (Some cable plants might want to change only the input power level, and not the frequency, on a daily time schedule.)
- Hop threshold—(Optional) Percentage of cable modems that must be offline (that is, missing 16 consecutive station maintenance messages) before a frequency hop can occur. Configure the hop threshold percentage as needed to prevent a single failing cable interface from affecting service to other good cable interfaces. This ensures that the system does not hop endlessly because one cable modem is generating 90% of the errors and 90% of the traffic.
- Hop period—(Optional) Minimum time period that must elapse between frequency hops. This allows you to specify a time period long enough to allow an upstream to stabilize before another frequency hop can be performed.
- Scheduled hop time—(Optional) Time of day at which a frequency hop should be scheduled.
- Shared—(Optional) Specifies that all the upstream ports using a spectrum group use the same frequency.

To create and configure a spectrum group, use the the following procedure.


Tip

Before adding a list of upstream frequencies (or frequency hop tables), start by determining which upstream ports are assigned to a combiner group. Refer to the [“Determining the Upstream Ports Assigned to a Combiner Group Example”](#) section on page 415 for an example.

Restrictions

- The Cisco uBR10012 router does not support spectrum groups with fixed frequencies.
- The Cisco uBR10012 router does not support shared spectrum groups.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cable spectrum-group** *group-number* [**time** *day hh:mm:ss*] **frequency** *up-freq-Hz* [*power-level-dBmV*]
4. **cable spectrum-group** *group-number* [**time** *day hh:mm:ss*] **band** *up-freq-Hz up-freq2-hz* [*power-level-dBmV*]
5. **cable spectrum-group** *group-number* **hop period** *seconds*
6. **cable spectrum-group** *group-number* **hop threshold** [*percent*]

7. **cable spectrum-group** *group-number* *shared*
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable Router#	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal Router(config)#	Enters global configuration mode.
Step 3	cable spectrum-group <i>group-number</i> [time <i>day hh:mm:ss</i>] frequency <i>up-freq-Hz</i> [<i>power-level-dBmV</i>] Example: Router(config)# cable spectrum-group 4 frequency 6500000 Router(config)# cable spectrum-group 4 time Monday 12:00:00 frequency 40000000 Router(config)#	Creates the spectrum group (if it does not already exist), and adds the specified fixed frequency to the group. • <i>Group-number</i>—Number of the spectrum group to be created or configured. The valid range is from 1 to 32, or from 1 to 40, depending on the Cisco IOS software release. • time day hh:mm:ss—(Optional) for scheduled spectrum groups, enter the day of the week (Sun—Sat) and the time of day that the frequency and input power level should change. • frequency up-freq-Hz—Upstream center frequency, in Hertz. The valid range is 5,000,000 Hz to 42,000,000 Hz (DOCSIS), 55,000,000 Hz (Japan), or 65,000,000 (EuroDOCSIS). • <i>power-level-dBmV</i>—(Optional) Default input power level, in dBmV, that should be used for the upstream when hopping to one of the frequencies in this group. The valid range is –10 to +25 dBmV, with a default of 0 dBmV.

	Command or Action	Purpose
Step 4	command <code>cable spectrum-group group-number [time day hh:mm:ss] band up-freq-Hz up-freq2-hz [power-level-dBmV]</code> Example: <pre>Router(config)# cable spectrum-group 4 band 12000000 18000000 Router(config)# cable spectrum-group 4 band 20000000 24000000 13 Router(config)#</pre>	Creates the spectrum group (if it does not already exist), and adds the specified band of frequencies to the group. <i>Group-number</i>—Number of the spectrum group to be created or configured. The valid range is from 1 to 32, or from 1 to 40, depending on the Cisco IOS software release. <i>time day hh:mm:ss</i>—(Optional) for scheduled spectrum groups, enter the day of the week (Sun—Sat) and the time of day that the frequency and input power level should change. <i>band up-freq1-hz up-freq2-hz</i>—Specifies a range of center frequencies the Cisco CMTS can scan to find an acceptable channel to which the spectrum group may hop. The valid range for <i>up-freq1-hz</i> is 5,000,000 Hz to 42,000,000 Hz (DOCSIS), 55,000,000 Hz (Japan), or 65,000,000 (EuroDOCSIS). The valid range for <i>up-freq2-hz</i> is the same, but <i>up-freq2-hz</i> must be greater than <i>up-freq1-hz</i>. <i>power-level-dBmV</i>—(Optional) Input power level, in dBmV, that should be used for the upstream when hopping to one of the frequencies in this group. The default value is 0 dBmV.
	Note Repeat Step 3 and Step 4 as needed for each fixed frequency and frequency band that should be a member of this spectrum group. You must assign at least two fixed frequencies, or a frequency band that contains at least two center frequencies, to a spectrum group before frequency hopping can occur.	
Step 5	command <code>cable spectrum-group group-number hop period seconds</code> Example: <pre>Router(config)# cable spectrum-group 4 hop period 60 Router(config)#</pre>	Specifies the minimum time, in seconds, between frequency hops. <i>seconds</i>—Specifies the frequency-hop time period in seconds. Valid values are from 1 to 3600 seconds (before Cisco IOS Release 12.2(8)BC1), or from 1 to 300 seconds (Cisco IOS Release 12.2(8)BC1 or later). Note We recommend a configuration of 30 seconds when using a Cisco uBR-LCP2-MC16 cable interface line card on a Cisco uBR10012 router.
Step 6	command <code>cable spectrum-group group-number hop threshold [percent]</code> Example: <pre>Router(config)# cable spectrum-group 4 hop threshold 25 Router(config)#</pre>	Specifies the frequency hop threshold for a spectrum group: <i>percent</i>—(Optional) Specifies the frequency hop threshold as a percentage of station maintenance messages that are lost. Valid range is from 1 to 100 percent, with a default of 20 percent.

	Command or Action	Purpose
Step 7	cable spectrum-group <i>group-number</i> shared Example: Router(config)# cable spectrum-group 4 shared Router(config)#	(Optional) Specifies that the upstream ports in a spectrum group share the same upstream frequency.
Step 8	end Example: Router(config)# end Router#	Exits global configuration mode and returns to privileged EXEC mode.

Assigning a Spectrum Group to One or More Upstream Ports

After a spectrum group has been created and configured, you must assign it to one or more upstream ports before the group's frequency spectrum is used for frequency hopping. You can assign a spectrum group to an upstream in the following ways:

- Use the **cable spectrum-group** interface configuration command to assign a spectrum group to all of the upstreams on a cable interface.
- Use the **cable upstream spectrum-group** interface configuration command to assign a spectrum group to one individual upstream. This command overrides a group that might have been assigned to all of the upstreams on the interface by the **cable spectrum-group** command.

To assign a spectrum group to one or all upstream ports on an interface, use the following procedure.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface cable** *x/y*
or
interface cable *x/y/z*
4. **cable spectrum-group** *group-number*
5. **cable upstream** *n* **spectrum-group** *group-number*
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	interface cable <i>x/y</i> or interface cable <i>x/y/z</i> Example: Router(config)# interface cable 5/1 Router(config-if)#	Enters interface configuration mode for the specified cable interface.
Step 4	cable spectrum-group <i>group-number</i> Example: Router(config-if)# cable spectrum-group 4 Router(config-if)#	Assigns the specified spectrum group as the default group for all upstreams on this cable interface. The valid range for <i>group-number</i> is from 1 to 32, or from 1 to 40, depending on the Cisco IOS software release.
Step 5	cable upstream <i>n</i> spectrum-group <i>group-number</i> Example: Router(config-if)# cable upstream 0 spectrum-group 5 Router(config-if)# cable upstream 1 spectrum-group 5 Router(config-if)#	Assigns the specified spectrum group to this individual upstream, overriding any previous assignment that was done for all upstreams on the interface using the cable spectrum-group command. <i>n</i>—Upstream port number. Valid values start with 0 for the first upstream port on the cable interface line card. <i>group-number</i>—Specifies the spectrum group to be assigned to this particular upstream. The valid range is from 1 to 32, or from 1 to 40, depending on the Cisco IOS software release. Note Repeat this step for each upstream to be configured.
Note Repeat Step 3 through Step 5 for each cable interface to be configured.		
Step 6	end Example: Router(config-if)# end Router#	Exits interface configuration mode and returns to privileged EXEC mode.

**Note**

For help in determining which upstream ports to assign in a combiner group, refer to the example, [Determining the Upstream Ports Assigned to a Combiner Group Example, page 415](#).

**Tip**

To verify the spectrum-group configuration, use the **show cable spectrum-group** command in privileged EXEC mode.

Configuring Dynamic Upstream Modulation (SNR-Based)

To use the Dynamic Upstream Modulation feature on cable interface line cards that support only the SNR version of this feature, you must do the following:

1. Create a primary modulation profile. This typically is a more bandwidth-efficient but a less robust profile.
2. Optionally create a secondary modulation profile. This typically is a less bandwidth-efficient but a more robust profile.
3. Assign the profiles to the desired cable interfaces and upstreams.

To create and assign the primary and secondary profiles to an upstream, use the following procedures.

**Tip**

When creating the modulation profiles, we recommend that you use the predefined modulation profiles, as opposed to manually specifying each burst parameter for each modulation profile.

Restrictions

- The Dynamic Upstream Modulation feature is supported only for DOCSIS 1.0/DOCSIS 1.1 TDMA-only modulation profiles. It is not supported for DOCSIS 2.0 mixed-mode or A-TDMA-only mode modulation profiles.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cable modulation-profile** *profile* {**mix** | **qam-16** | **qpsk** | **robust-mix**}
4. **cable modulation-profile** *profile* {**mix** | **qam-16** | **qpsk** | **robust-mix**}
5. **interface cable** *x/y*
or
interface cable *x/y/z*
6. **cable upstream** *n* **modulation-profile** *primary-profile-number* [*secondary-profile-number*]
7. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable Router#	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal Router(config)#	Enters global configuration mode.
Step 3	cable modulation-profile <i>profile</i> { mix qam-16 qpsk robust-mix } Example: Router(config)# cable modulation-profile 3 mix Router(config)#	Creates the primary modulation profile for use on a DOCSIS 1.0/DOCSIS 1.1 TDMA upstream. <i>profile</i> = Specifies the modulation profile number. For the DOCSIS 1.0/DOCSIS 1.1 TDMA mode, the valid range is 1 to 10, 21 to 30, or 41 to 50, depending on the cable interface being used. The system creates profile 1, 21, or 41 as a default TDMA-only modulation profile. - The following preconfigured profiles are available: mix = Default QPSK/16-QAM profile. qam-16 = Default 16-QAM profile. qpsk = Default QPSK profile. robust-mix = Default QPSK/16-QAM profile that is more robust and more able to deal with noise than the mix profile. Typically, the primary profile is either qam-16 or mix.
Step 4	cable modulation-profile <i>profile</i> { mix qam-16 qpsk robust-mix } Example: Router(config)# cable modulation-profile 4 robust-mix Router(config)#	(Optional) Repeat this command to create the secondary profile for use on a DOCSIS 1.0/DOCSIS 1.1 TDMA upstream. Typically, the secondary profile is either robust-mix or qpsk.
	Note You can also create custom modulation profiles with the cable modulation-profile command by configuring the values for the individual burst parameters. These parameters, however, should not be modified unless you are thoroughly familiar with how changing each parameter affects the DOCSIS MAC layer. We recommend using the preconfigured default modulation profiles for most cable plants.	
Step 5	interface cable <i>x/y</i> or interface cable <i>x/y/z</i> Example: Router(config)# interface cable 5/1 Router(config-if)#	Enters interface configuration mode for the specified cable interface.

	Command or Action	Purpose
Step 6	cable upstream <i>n</i> modulation-profile <i>primary-profile-number</i> [<i>secondary-profile-number</i>] Example: Router(config-if)# cable upstream 0 modulation-profile 3 4 Router(config-if)#	Assigns a primary modulation profile, and an optional secondary modulation profile, to the specified upstream port. <i>n</i>—Upstream port number. Valid values start with 0 for the first upstream port on the cable interface line card. <i>primary-profile-number</i>—Specify the primary modulation profile created in Step 3. <i>secondary-profile-number</i>—(Optional) Specify the secondary modulation profile created in Step 4.
Step 7	end Example: Router(config-if)# end Router#	Exits interface configuration mode and returns to privileged EXEC mode.

**Tip**

See the [“Dynamic Upstream Modulation \(SNR-based\)” section on page 374](#) for a complete description of this feature.

Verifying Frequency Hopping

You can verify frequency hopping on the CMTS either by using command-line interface (CLI) or by using an RF tone generator.

Verifying Frequency Hopping Using CLI Commands

To verify frequency hopping using CLI commands, use the following procedure:

Step 1	Verify that the interface being tested is up, using the show interface cable command in privileged EXEC mode. The first line of the output shows whether both the interface and line protocol are up. For example: Router# show interface c6/0 Cable6/0 is up, line protocol is up Hardware is BCM3210 ASIC, address is 000a.13e8.1ca8 (bia 000a.13e8.1ca8) Internet address is 10.20.114.33/27 MTU 1500 bytes, BW 27000 Kbit, DLY 1000 usec, ... Router#
Step 2	Verify that the upstream being tested is up, using the show interface cable upstream command. The first line shows whether the upstream is up. For example: Router# show interface c6/0 upstream 5 Cable6/0: Upstream 5 is up Received 8 broadcasts, 0 multicasts, 6388105 unicasts 0 discards, 0 errors, 0 unknown protocol 6388113 packets input, 0 uncorrectable 0 noise, 0 microreflections Total Modems On This Upstream Channel : 23 (22 active)

Router#

- Step 3** Use the **show cable hop upstream** command to display the frequency that the upstream is currently using:

Router# **show cable hop c6/0 upstream 5**

Upstream Port	Port Status	Poll Rate (ms)	Missed Poll Count	Min Poll Sample	Missed Poll Pcnt	Hop Thres Pcnt	Hop Period (sec)	Corr FEC Errors	Uncorr FEC Errors
Cable6/0/U5	16.816 Mhz	1000	0	10	0%	20%	25	0	0

Router#

- Step 4** Use the **test cable hop** command to force the desired upstream to perform a frequency hop. A few seconds after giving the command, a console message should appear informing you of the hop. Repeat the command as needed to verify that the upstream hops through all the frequencies that have been assigned to the upstream's spectrum group. For example:

Router# **test cable hop c6/0 upstream 5**

2w0d: %UBR7200-5-USFREQCHG: Interface Cable6/0 Port U5, frequency changed to 15.760 MHz

Router# **test cable hop c6/0 upstream 5**

2w0d: %UBR7200-5-USFREQCHG: Interface Cable6/0 Port U5, frequency changed to 26.832 MHz

Router#

Verifying Frequency Hopping Using an RF Tone Generator

To verify frequency hopping using an RF tone generator, first verify that the upstream is performing properly. Then inject a tone to the upstream port at the current upstream frequency and cable modem power level.

For example, if the upstream frequency is 22.4-MHz, inject a 22.4 MHz tone at approximately the same power level as the modem. If the power level at the modem is 40 dBmV, set the tone power to 40 dBmV. The interfering carrier should shut down the channel and cause the frequency to change to the next configured value (such as 24.0 MHz).

If you do not have an RF tone generator, use another line card and modem that carries traffic. Connect the upstream to the same combiner group, and use the data carrier as an interfering signal by setting it to the same frequency. For example, to test frequency hopping on c3/0, install c4/0 and connect both upstreams together using a combiner. If the upstream frequency of c3/0 is 22.4 MHz, set c4/0 to 22.4 MHz while c4/0 is carrying traffic. This should force c3/0 to change the frequency to the next configured value.

The comparison of the number of errors versus the number of error-free packets is a measure of the link quality. The percentage of errors should be less than 1 percent.

Troubleshooting Spectrum Group Characteristics

To troubleshoot the configuration, make sure that you entered a valid spectrum group number, time, frequency, and input power level. Also, when defining your spectrum, use the following guidelines:

- Avoid frequencies with known ingress problems, such as amateur radio bands or short-wave bands.
- Avoid hostile spectrum below 20 MHz.

- Allow extra bands for frequency hopping.
- Place upstream ports in the same combiner group in a shared spectrum group.
- Use the receive power level setting to perform slight equalization adjustments.

Intelligent and Advanced Spectrum Management Configuration Tasks

The following sections describe the configuration tasks that are needed to configure a Cisco uBR7200 series router or Cisco uBR10012 router for the Intelligent and Advanced spectrum management features that are available when using the Cisco uBR-MC16S/U/X and Cisco uBR-MC28U/X cable interface line cards.

- [Configuring and Assigning Spectrum Groups, page 396](#)
- [Configuring Dynamic Upstream Modulation \(CNR-Based\), page 396](#)
- [Configuring Proactive Channel Management, page 399](#)
- [Verifying the Spectrum Management Configuration, page 402](#)

Configuring and Assigning Spectrum Groups

You must create and configure a spectrum group before you can use the intelligent and advanced spectrum management features. These procedures are the same as those used for guided and scheduled spectrum management, which are given in the following sections:

- [Creating and Configuring Spectrum Groups, page 385](#)
- [Assigning a Spectrum Group to One or More Upstream Ports, page 389](#)

After the spectrum groups have been configured and assigned to upstreams, the Cisco IOS software automatically uses the advanced frequency hopping algorithms on the cable interface line cards that support it. See the [“Advanced Spectrum Management Features” section on page 377](#) for more information.

**Note**

For efficient use of the intelligent and advanced spectrum management features, we recommend configuring only frequency bands, and not fixed frequencies, when creating spectrum groups. A spectrum group must contain a frequency band that is wide enough for the cable interface to find at least two center frequencies at the configured channel width, before frequency hopping can occur.

Configuring Dynamic Upstream Modulation (CNR-Based)

Configuring the CNR-based version of the Dynamic Upstream Modulation feature is similar to configuring the SNR-version of this feature:

1. Create a primary modulation profile. This typically is a more bandwidth-efficient but a less robust profile.
2. Create a secondary modulation profile. This typically is a less bandwidth-efficient but a more robust profile.

**Tip**

When creating the modulation profiles, we recommend that you use the predefined modulation profiles, as opposed to manually specifying each burst parameter for each modulation profile.

3. Assign the profiles to the desired cable interfaces and upstreams.

After the modulation profiles have been created and assigned to upstreams, the Cisco IOS software automatically uses the advanced CNR-based version of the Dynamic Upstream Modulation feature on the cable interface line cards that support it. See the [“Advanced Spectrum Management Features” section on page 377](#) for more information.

Restrictions

- The Dynamic Upstream Modulation feature is supported only for DOCSIS 1.0/DOCSIS 1.1 TDMA-only modulation profiles. It is not supported for DOCSIS 2.0 mixed-mode or A-TDMA-only mode modulation profiles.
- If you are using a software release between Cisco IOS Release 12.2(8)BC2 and Cisco IOS Release 12.2(11)BC2 inclusive, you must perform an additional configuration when using the **mix** and **qam-16** predefined modulation profiles. This is because the short and long grant bursts of the **mix** and **qam-16** profiles default to a unique word offset of 8 (uw8). These values should be changed to **uw16** for optimal performance. To do this, first create the modulation profiles using the procedure given in this section, and then issue the following commands for each modulation profile that uses the **mix** or **qam-16** predefined modulation profiles:

```
cable modulation-profile n short 6 75 6 8 16qam scrambler 152 no-diff 144
fixed uw16
cable modulation-profile n long 8 220 0 8 16qam scrambler 152 no-diff 160
fixed uw16
```

The defaults for these predefined profiles were corrected in Cisco IOS Release 12.2(11)BC3 and later releases, and this step is no longer needed.

To assign the primary and secondary profiles to an upstream, use the following procedure.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cable modulation-profile profile {mix | qam-16 | qpsk | robust-mix}**
4. **cable modulation-profile profile {mix | qam-16 | qpsk | robust-mix}**
5. **interface cable x/y**
or
interface cable x/y/z
6. **cable upstream n modulation-profile primary-profile-number secondary-profile-number**
7. **exit**

DETAILED STEPS

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

	Command or Action	Purpose
Step 3	cable modulation-profile <i>profile</i> {mix qam-16 qpsk robust-mix} Example: Router(config)# cable modulation-profile 3 mix Router(config)#	Creates the primary modulation profile for use on a DOCSIS 1.0/DOCSIS 1.1 TDMA upstream. <i>profile</i> = Specifies the modulation profile number. For the DOCSIS 1.0/DOCSIS 1.1 TDMA mode, the valid range is 1 to 10, 21 to 30, or 41 to 50, depending on the cable interface being used. The system creates profile 1, 21, or 41 as a default TDMA-only modulation profile. - The following preconfigured profiles are available: mix = Default QPSK/16-QAM profile. qam-16 = Default 16-QAM profile. qpsk = Default QPSK profile. robust-mix = Default QPSK/16-QAM profile that is more robust and more able to deal with noise than the mix profile. Typically, the primary profile is either qam-16 or mix.
Step 4	cable modulation-profile <i>profile</i> {mix qam-16 qpsk robust-mix} Example: Router(config)# cable modulation-profile 4 robust-mix Router(config)#	Repeat this command to create the secondary profile for use on a DOCSIS 1.0/DOCSIS 1.1 TDMA upstream. Typically, the secondary profile is either robust-mix or qpsk.
	Note You can also create custom modulation profiles with the cable modulation-profile command by configuring the values for the individual burst parameters. These parameters, however, should not be modified unless you are thoroughly familiar with how changing each parameter affects the DOCSIS MAC layer. We recommend using the preconfigured default modulation profiles for most cable plants.	
Step 5	interface cable <i>x/y</i> or interface cable <i>x/y/z</i> Example: Router(config)# interface cable 5/1 Router(config-if)#	Enters interface configuration mode for the specified cable interface.

	Command or Action	Purpose
Step 6	cable upstream <i>n</i> modulation-profile <i>primary-profile-number</i> <i>secondary-profile-number</i> Example: <pre>Router(config-if)# cable upstream 0 modulation-profile 3 4 Router(config-if)#</pre>	Assigns a primary modulation profile, and an optional secondary modulation profile, to the specified upstream port. <i>n</i>—Upstream port number. Valid values start with 0 for the first upstream port on the cable interface line card. <i>primary-profile-number</i>—Specify the primary modulation profile created in Step 3. <i>secondary-profile-number</i>—Specify the secondary modulation profile created in Step 4.
Step 7	end Example: <pre>Router(config-if)# end Router#</pre>	Exits interface configuration mode and returns to privileged EXEC mode.

**Tip**

See the [“Advanced Spectrum Management Features” section on page 377](#) for a complete description of the CNR-based Dynamic Upstream Modulation feature.

Configuring Proactive Channel Management

The cable interface line cards that support the advanced spectrum management features can be configured with following parameters so as to fine tune the operation of proactive channel management on the cards' upstreams:

- Priority of the corrective actions to be taken when noise on an upstream exceeds the threshold for its modulation profile.
- CNR threshold and FEC values for the upstream and its two modulation profiles.
- Allowable range of channel widths that can be used if frequency hopping or modulation switching cannot avoid the upstream problems.
- Polling interval that determines how often the cable interface line card examines each upstream to determine its CNR value.

To configure these parameters, use the following procedure. These parameters all have default settings, so you do not need to perform this procedure unless you want to change these parameters to better match the characteristics of your physical plant.

A major exception to this is if you are using only one modulation profile and are using a software release prior to Cisco IOS Release 12.2(8)BC2. In these releases, a frequency hop would occur if just one of the measured values (CNR value, correctable FEC counter, or uncorrectable FEC counter) crosses the configured threshold value. Because of this, if you are using only one modulation profile (QPSK) with one of these software releases, you might need to reduce the CNR threshold value and increase the correctable FEC error value to prevent undesired frequency hopping.

This situation no longer occurs in Cisco IOS Release 12.2(8)BC2 and later releases, because a frequency hop can occur only when both the CNR value and one of the FEC counters falls below its threshold value. See the [“Advanced Spectrum Management Features” section on page 377](#) for more information.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface cable** *x/y*
or
interface cable *x/y/z*
4. **cable upstream** *n* **hop-priority** **frequency modulation channel-width**
or
cable upstream *n* **hop-priority modulation frequency channel-width**
or
cable upstream *n* **hop-priority frequency channel-width modulation**
5. **cable upstream** *n* **threshold** **cnr-profile1** *threshold1-in-dB* **cnr-profile2** *threshold2-in-dB*
corr-fec *fec-corrected* **uncorr-fec** *fec-uncorrected*
6. **cable upstream** *n* **channel-width** *first-choice-width* [*last-choice-width*]
7. **cable upstream** *n* **snr-polling** *interval-in-ms*
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	interface cable <i>x/y</i> or interface cable <i>x/y/z</i> Example: Router(config)# interface cable 5/1 Router(config-if)#	Enters interface configuration mode for the specified cable interface.

	Command or Action	Purpose
Step 4	cable upstream <i>n</i> hop-priority frequency modulation channel-width or cable upstream <i>n</i> hop-priority modulation frequency channel-width or cable upstream <i>n</i> hop-priority frequency channel-width modulation Example: Router(config-if)# cable upstream 0 hop-priority frequency channel-width modulation Router(config-if)#	(Optional) Specifies the priority of the three types of corrective actions (modulation, frequency, and channel-width) to be taken when the noise for the upstream exceeds the threshold specified for the current modulation profile. The default priority is frequency, modulation, and channel-width. <i>n</i>—Upstream port number. Valid values start with 0 for the first upstream port on the cable interface line card. Note The channel-width option must always appear after the frequency option.
Step 5	cable upstream <i>n</i> threshold cnr-profile1 threshold1-in-dB cnr-profile2 threshold2-in-dB corr-fec fec-corrected uncorr-fec fec-uncorrected Example: Router(config-if)# cable upstream 5 threshold cnr-profile1 20 cnr-profile2 10 corr-fec 5 uncorr-fec 1 Router(config-if)#	(Optional) Specifies the CNR threshold and FEC values for the upstream and its two modulation profiles. <i>n</i>—Upstream port number. Valid values start with 0 for the first upstream port on the cable interface line card. cnr-profile1 threshold1-in-dB—CNR threshold for the primary modulation profile (5 to 35 dB, with a default of 25) cnr-profile2 threshold1-in-dB—CNR threshold for the secondary modulation profile (5 to 35 dB, must be less than that for the primary modulation profile, with a default of 15) corr-fec fec-corrected—Allowable number of correctable FEC errors for the upstream, as given as a percentage of total packets received on the upstream during the polling period. The valid range is 0 to 30 percent of total packets, and a default of 3 percent. uncorr-fec fec-uncorrected—Allowable number of uncorrectable FEC errors for the upstream, as given as a percentage of total packets received on the upstream during the polling period. The valid range is 0 to 30 percent of total packets, with a default of 1 percent. Note For normal plant use, we recommend that the uncorrectable FEC threshold remain at its default of 1 percent to avoid an unacceptable number of errors on the channel.

	Command or Action	Purpose
Step 6	command <code>cable upstream n channel-width first-choice-width [last-choice-width]</code> Example: <pre>Router(config-if)# cable upstream 0 channel-width 3200000 Router(config-if)# cable upstream 0 channel-width 800000 800000 Router(config-if)#</pre>	(Optional) Specifies the range of allowable channel widths that can be used when ingress noise conditions require changing the channel width. The upstream begins with the first-choice channel width and decreases in half until it hits the secondary channel width. <i>first-choice-width</i>—Specifies upstream channel width in hertz (Hz). The valid values are: 200,000 (160,000 symbols/sec) 400,000 (320,000 symbols/sec) 800,000 (640,000 symbols/sec) 1,600,000 (1,280,000 symbols/sec) (default) 3,200,000 (2,560,000 symbols/sec) 6,400,000 Hz (5,120,000 symbols/sec) (DOCSIS 2.0 ATDMA-only upstreams only) <i>last-choice-width</i>—(Optional) Upstream channel width in hertz. Supports the same values as <i>first-choice-width</i>, but must be less than or equal to <i>first-choice-width</i>.
Step 7	command <code>cable upstream n snr-polling interval-in-ms</code> Example: <pre>Router(config-if)# cable upstream 5 snr-polling 10000 Router(config-if)#</pre>	(Optional) Configures how often the cable interface card should poll an upstream to determine its CNR value. <i>n</i>—Upstream port number. Valid values start with 0 for the first upstream port on the cable interface line card. <i>interval-in-ms</i>—The valid range is 1000 to 25000 milliseconds, with a default of 15000 milliseconds.
Note Repeat Step 4 through Step 7 for each upstream to be configured.		
Step 8	command <code>end</code> Example: <pre>Router(config-if)# end Router#</pre>	Exits interface configuration mode and returns to privileged EXEC mode.

Verifying the Spectrum Management Configuration

- Step 1** To check the value of the settings you have entered, use the **show running-config** command in privileged EXEC mode:
- ```
Router# show running-config
```
- Step 2** To display the configuration for each modulation profile, use the **show cable modulation-profile** command in privileged EXEC mode:
- ```
Router# show cable modulation-profile
```
- To display the configuration for a specific modulation profile, add the profile number to the **show cable modulation-profile** command in privileged EXEC mode:
- ```
Router# show cable modulation-profile n
```

**Step 3** To display the status and configuration of each upstream, use the **show controllers cable upstream** command in privileged EXEC mode. The following example shows the display for the first two upstreams on a Cisco uBR-MC16S line card:

Router# **show controllers c6/0 upstream**

```
Cable6/0 Upstream 0 is administratively down
 Frequency not set, Channel Width 1.600 MHz, QPSK Symbol Rate 1.280 Msps
 Spectrum Group is unassigned
 CNR - Unknown - no modems online.
 Nominal Input Power Level 0 dBmV, Tx Timing Offset 0
 Ranging Backoff automatic (Start 0, End 3)
 Ranging Insertion Interval automatic (60 ms)
 Tx Backoff Start 0, Tx Backoff End 4
 Modulation Profile Group 1
 Concatenation is enabled
 Fragmentation is enabled
 part_id=0x3137, rev_id=0x03, rev2_id=0xFF
 nb_agc_thr=0x0000, nb_agc_nom=0x0000
 Range Load Reg Size=0x58
 Request Load Reg Size=0x0E
 Minislot Size in number of Timebase Ticks is = 8
 Minislot Size in Symbols = 64
 Bandwidth Requests = 0x0
 Piggyback Requests = 0x0
 Invalid BW Requests= 0x0
 Minislots Requested= 0x0
 Minislots Granted = 0x0
 Minislot Size in Bytes = 16
 Map Advance (Dynamic) : 2180 usecs
 UCD Count = 0
 DES Ctrl Reg#0 = C000C043, Reg#1 = 0
Cable6/0 Upstream 1 is up
 Frequency 25.008 MHz, Channel Width 1.600 MHz, 16-QAM Symbol Rate 1.280 Msps
 Spectrum Group 1, Last Frequency Hop Data Error: NO(0)
 MC16S CNR measurement - 45 dB
 Nominal Input Power Level 0 dBmV, Tx Timing Offset 2811
 Ranging Backoff automatic (Start 0, End 3)
 Ranging Insertion Interval automatic (60 ms)
 Tx Backoff Start 0, Tx Backoff End 4
 Modulation Profile Group 1
 Concatenation is enabled
 Fragmentation is enabled
 part_id=0x3137, rev_id=0x03, rev2_id=0xFF
 nb_agc_thr=0x0000, nb_agc_nom=0x0000
 Range Load Reg Size=0x58
 Request Load Reg Size=0x0E
 Minislot Size in number of Timebase Ticks is = 8
 Minislot Size in Symbols = 64
 Bandwidth Requests = 0x12
 Piggyback Requests = 0x5
 Invalid BW Requests= 0x0
 Minislots Requested= 0xFA
 Minislots Granted = 0xFA
 Minislot Size in Bytes = 32
 Map Advance (Dynamic) : 2454 usecs
 UCD Count = 230
 DES Ctrl Reg#0 = C000C043, Reg#1 = 0
 Dynamic Services Stats:
 DSA: 0 REQs 0 RSPs 0 ACKs
 0 Successful DSAs 0 DSA Failures
 DSC: 0 REQs 0 RSPs 0 ACKs
 0 Successful DSCs 0 DSC Failures
 DSD: 0 REQs 0 RSPs
```

```
0 Successful DSDs 0 DSD Failures
```

```
DCC: 0 REQs 0 RSPs 0 ACKs
0 Successful DCCs 0 DCC Failures
```

```
Router#
```

**Note**

In the above example, upstream 0 displays “CNR - Unknown - no modems online” to indicate that the CNR value has not yet been calculated because no cable modems have come online for that particular upstream yet.

- Step 4** To display the hop period and hop threshold values for each upstream, use the **show cable hop** in privileged EXEC mode command:

```
Router# show cable hop
```

| Upstream<br>Port | Port<br>Status | Poll<br>Rate | Missed<br>Poll<br>Count | Min<br>Poll<br>Sample | Missed<br>Poll<br>Pcnt | Hop<br>Thres<br>Pcnt | Hop<br>Period<br>(sec) | Corr<br>FEC<br>Errors | Uncorr<br>FEC<br>Errors |
|------------------|----------------|--------------|-------------------------|-----------------------|------------------------|----------------------|------------------------|-----------------------|-------------------------|
| Cable3/0/U0      | 20.800 Mhz     | 105          | 0                       | 20                    | 0%                     | 25%                  | 45                     | 1                     | 4                       |
| Cable3/0/U1      | 20.800 Mhz     | 105          | 0                       | 48                    | 0%                     | 25%                  | 45                     | 2                     | 19                      |
| Cable3/0/U2      | 23.120 Mhz     | 105          | 0                       | 45                    | 0%                     | 25%                  | 45                     | 0                     | 5                       |
| Cable3/0/U3      | 22.832 Mhz     | 105          | 0                       | 26                    | 0%                     | 25%                  | 45                     | 0                     | 6                       |
| Cable3/0/U4      | 22.896 Mhz     | 105          | 0                       | 43                    | 0%                     | 25%                  | 45                     | 0                     | 7                       |
| Cable3/0/U5      | 23.040 Mhz     | 105          | 0                       | 54                    | 0%                     | 25%                  | 45                     | 1                     | 3                       |
| Cable4/0/U0      | 22.896 Mhz     | 117          | 0                       | 26                    | 0%                     | 25%                  | 45                     | 0                     | 2                       |
| Cable4/0/U1      | 23.168 Mhz     | 117          | 0                       | 87                    | 0%                     | 25%                  | 45                     | 4                     | 2                       |
| Cable4/0/U2      | 22.896 Mhz     | 117          | 0                       | 23                    | 0%                     | 25%                  | 45                     | 1                     | 0                       |
| Cable4/0/U3      | 20.800 Mhz     | 117          | 0                       | 54                    | 0%                     | 25%                  | 45                     | 0                     | 0                       |
| Cable4/0/U4      | 22.928 Mhz     | 117          | 0                       | 22                    | 0%                     | 25%                  | 45                     | 0                     | 1                       |
| Cable4/0/U5      | 22.960 Mhz     | 117          | 0                       | 0                     | -----                  | 25%                  | 45                     | 0                     | 0                       |

```
Router#
```

- Step 5** To display the assignment of each spectrum group, use the **show cable spectrum-group** command in privileged EXEC mode:

```
Router# show cable spectrum-group
```

| Group<br>No. | Frequency<br>Band<br>(Mhz) | Upstream<br>Port | Weekly Scheduled<br>Availability<br>From Time: | To Time: | Power<br>Level<br>(dBmV) | Shared<br>Spectrum |
|--------------|----------------------------|------------------|------------------------------------------------|----------|--------------------------|--------------------|
| 1            | 20.000-21.600              |                  |                                                |          | 0                        | No                 |
| 1            | 22.000-24.000              |                  |                                                |          | 0                        | No                 |
| 1            | 20.784 [1.60]              | Cable3/0 U0      |                                                |          | 0                        |                    |
| 1            | 20.784 [1.60]              | Cable3/0 U1      |                                                |          | 0                        |                    |
| 1            | 23.120 [1.60]              | Cable3/0 U2      |                                                |          | 0                        |                    |
| 1            | 22.832 [1.60]              | Cable3/0 U3      |                                                |          | 0                        |                    |
| 1            | 22.896 [1.60]              | Cable3/0 U4      |                                                |          | 0                        |                    |
| 1            | 23.024 [1.60]              | Cable3/0 U5      |                                                |          | 0                        |                    |
| 1            | 23.152 [1.60]              | Cable4/0 U1      |                                                |          | 0                        |                    |
| 1            | 22.896 [1.60]              | Cable4/0 U0      |                                                |          | 0                        |                    |
| 1            | 22.896 [1.60]              | Cable4/0 U2      |                                                |          | 0                        |                    |
| 1            | 20.784 [1.60]              | Cable4/0 U3      |                                                |          | 0                        |                    |
| 1            | 22.928 [1.60]              | Cable4/0 U4      |                                                |          | 0                        |                    |
| 1            | 22.960 [1.60]              | Cable4/0 U5      |                                                |          | 0                        |                    |

```
Router#
```

- Step 6** To display the current CNR value for a particular cable modem, use the **show cable modem cnr** command in privileged EXEC mode:

```
Router# show cable modem 10.240.179.234 cnr
```

| MAC Address    | IP Address     | I/F     | MAC State | Prim Sid | CNR (db) |
|----------------|----------------|---------|-----------|----------|----------|
| 0020.40bc.3588 | 10.240.179.234 | C3/0/U2 | online    | 2        | 38.0     |

```
Router# show cable modem 10.240.179.51 cnr
```

| MAC Address    | IP Address    | I/F     | MAC State | Prim Sid | CNR (db) |
|----------------|---------------|---------|-----------|----------|----------|
| 0020.40ef.4be0 | 10.240.179.51 | C3/0/U5 | online    | 11       | 39.5     |

```
Router#
```

---

# Monitoring Spectrum Management

You can use Cisco IOS CLI commands to monitor spectrum management activity on the Cisco CMTS. If you are using Cisco IOS Release 12.2(8)BC2 or later 12.2 BC releases, you can also use SNMP to monitor the spectrum management activity. See the following sections for more information:

- [Using CLI Commands, page 406](#)
- [Using SNMP, page 407](#)

## Using CLI Commands

The following commands provide information on the spectrum condition of an upstream:

| Command                                                                                                                                                                      | Purpose                                                                                                                                                                                                                                                                                                                                        |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Router# <b>show cable hop</b> [ <i>cx/y</i> ]<br>[ <i>upstream usport</i> ]                                                                                                  | Displays the hop period and hop threshold values, as well as the FEC error counters, for all upstreams in the router, all upstreams on one cable interface line card, or a single upstream.                                                                                                                                                    |
| Router# <b>show cable modem</b> [ <i>ip-address</i>   <i>interface</i>   <i>mac-address</i> ] [ <i>options</i> ]                                                             | Displays information, including SNR values, for the registered and unregistered cable modems.<br><br><b>Note</b> Cisco IOS Release 12.2(8)BC2 and later 12.2 BC releases also support a <b>cnr</b> option that displays the CNR value for a specific cable modem, if it is using an upstream on the Cisco uBR-MC16S cable interface line card. |
| Router# <b>show cable modulation-profile</b> [ <i>num</i> ] [ <i>initial</i>   <i>long</i>   <i>reqdata</i>   <i>request</i>   <i>short</i>   <i>station</i> ]               | Displays the configuration for all modulation profiles, for a particular modulation profile, or for a specific burst type for a particular modulation profile.                                                                                                                                                                                 |
| Router# <b>show cable spectrum-group</b> [ <i>groupnum</i> ] [ <i>detail</i> ]                                                                                               | Displays information about the spectrum groups that have been configured.<br><br><b>Note</b> The <b>detail</b> keyword is supported only in Cisco IOS Release 12.2(8)BC2 and later 12.2 BC releases.                                                                                                                                           |
| Router# <b>show controllers cable</b> <i>x/y</i> <b>upstream n</b> [ <i>ip-address</i>   <i>mac-address</i> ] [ <i>start-freq</i> <i>end-freq</i> <i>res-freq</i> ]          | Displays the upstream's status, including the current frequency, channel width, modulation rate, and spectrum groups.                                                                                                                                                                                                                          |
| Router# <b>show controllers cable</b> <i>x/y</i> <b>upstream n spectrum</b> [ <i>ip-address</i>   <i>mac-address</i> ] [ <i>start-freq</i> <i>end-freq</i> <i>res-freq</i> ] | Displays the noise levels for a particular cable modem or displays the background noise for an entire upstream.                                                                                                                                                                                                                                |



### Note

The **show cable flap-list** command displays the CMTS router's flap list, which can provide additional information about whether cable modems on an upstream are experiencing problems, and if so, what type of problems are occurring. For more information, see the chapter "[Flap List Troubleshooting for the Cisco CMTS](#)" in this guide.

## Using SNMP

When you are using Cisco IOS Release 12.2(8)BC2 and later 12.2 BC releases and the Cisco uBR-MC16S cable interface line card, you can use SNMP to monitor the spectrum management activity. The SNMP manager can be a graphically based SNMP manager such as CiscoView or the Cable Broadband Troubleshooter (release 3.0 or greater).

The CISCO-CABLE-SPECTRUM-MIB has been enhanced to provide this SNMP support using the following MIB attributes:

- [ccsSNRRequestTable](#), page 407
- [ccsSpectrumRequestTable](#), page 408
- [ccsSpectrumDataTable](#), page 408
- [ccsUpSpecMgmtTable](#), page 409
- [ccsHoppingNotification](#), page 410

### ccsSNRRequestTable

**Table 10** lists the attributes in the `ccsSNRRequestTable`, which contains the CNR measurements that are made for individual cable modems on an upstream:

**Table 10** *ccsSNRRequestTable Attributes*

| Attribute                             | Type                | Description                                                                                                                                   |
|---------------------------------------|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| <code>ccsSNRRequestIndex</code>       | Integer32           | Arbitrary index to uniquely identify each table entry.                                                                                        |
| <code>ccsSNRRequestMacAddr</code>     | MacAddress          | MAC address of the remote online cable modem being reported on.                                                                               |
| <code>ccsSNRRequestSNR</code>         | Integer32           | SNR value, in dB, that has been measured. This value is 0 when the Operation State is “running.”                                              |
| <code>ccsSNRRequestOperation</code>   | CCSRequestOperation | Sets the current operation: start, pending, running, or abort.                                                                                |
| <code>ccsSNRRequestOperState</code>   | CCSRequestOperState | Reports on the current operation state: idle, pending, running, noError, aborted, notOnLine, invalidMac, timeOut, fftBusy, fftFailed, others. |
| <code>ccsSNRRequestStartTime</code>   | TimeStamp           | Contains the time when the SNR measurement operation starts.                                                                                  |
| <code>ccsSNRRequestStoppedTime</code> | TimeStamp           | Contains the time when the SNR measurement stops.                                                                                             |
| <code>ccsSNRRequestStatus</code>      | RowStatus           | Controls the modification, creation, and deletion of table entries.                                                                           |

## ccsSpectrumRequestTable

Table 11 lists the attributes for each entry in the ccsSpectrumRequestTable table, which is used to obtain the spectrum profile for a particular cable modem or to obtain the background SNR for an entire upstream:

**Table 11** ccsSpectrumRequestTable Attributes

| Attribute                     | Type                  | Description                                                                                                                               |
|-------------------------------|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| ccsSpectrumRequestIndex       | Integer32             | Arbitrary index to uniquely identify each table entry.                                                                                    |
| ccsSpectrumRequestIfIndex     | InterfaceIndex OrZero | Interface identifying the upstream.                                                                                                       |
| ccsSpectrumRequestMacAddr     | MacAddress            | MAC address to specify an SNR value for a particular cable modem, or 0000.0000.0000 to indicate background noise for the entire spectrum. |
| ccsSpectrumRequestUpperFreq   | CCSFrequency          | Upper frequency for the frequency range to be monitored (5000 to 42000 KHz, with a default of 42000 KHz).                                 |
| ccsSpectrumRequestLowFreq     | CCSFrequency          | Lower frequency (in KHz) for the frequency range to be monitored (5000 to 42000 KHz, with a default of 5000 KHz).                         |
| ccsSpectrumRequestResolution  | Integer32             | Requested resolution to determine how the frequency range should be sampled (12 to 37000 KHz, with a default of 60 KHz).                  |
| ccsSpectrumRequestStartTime   | TimeStamp             | Time when the spectrum measurement began.                                                                                                 |
| ccsSpectrumRequestStoppedTime | TimeStamp             | Time when the spectrum measurement finished.                                                                                              |
| ccsSpectrumRequestOperation   | CCSRequestOperation   | Starts a new spectrum management request or aborts the current one.                                                                       |
| ccsSpectrumRequestOperState   | CCSRequestOperState   | Provides the operational state of the current spectrum management request.                                                                |
| ccsSpectrumRequestStatus      | RowStatus             | Controls the modification, creation, and deletion of table entries.                                                                       |

## ccsSpectrumDataTable

Table 12 lists the attributes in each entry of the ccsSpectrumDataTable table, which contains the results for a spectrum request:

**Table 12** ccsSpectrumDataTable Attributes

| Attribute            | Type                 | Description                                                      |
|----------------------|----------------------|------------------------------------------------------------------|
| ccsSpectrumDataFreq  | CCSMeasuredFrequency | Frequency in KHz for which this power measurement was made       |
| ccsSpectrumDataPower | INTEGER              | Measured received power for the given frequency (-50 to 50 dBmV) |



**Note**

The `ccsSpectrumRequestTable` and `ccsSpectrumDataTable` tables provide the same information as that provided by the **show controllers cable upstream spectrum** command.

## ccsUpSpecMgmtTable

[Table 13](#) lists the attributes in the `ccsUpSpecMgmtTable` table, which provides an entry describing each frequency hop:

**Table 13** *ccsUpSpecMgmtEntry Attributes*

| Attribute                                    | Type         | Description                                                                                                                                                                                                   |
|----------------------------------------------|--------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>ccsUpSpecMgmtHopPriority</code>        | INTEGER      | Specifies the priority of frequency, modulation profile, and channel width in determining corrective action for excessive noise on the upstream (default is frequency, modulation profile, and channel width) |
| <code>ccsUpSpecMgmtSnrThres1</code>          | Integer32    | Specifies the upper SNR threshold for modulation profile 1 (5–35 dB, default of 25)                                                                                                                           |
| <code>ccsUpSpecMgmtSnrThres2</code>          | Integer32    | Specifies the upper SNR threshold for modulation profile 2 (5–35 dB, default of 15, and must be lower than that specified for <code>ccsUpSpecMgmtSnrThres1</code> )                                           |
| <code>ccsUpSpecMgmtFecCorrectThres1</code>   | Integer32    | Specifies the FEC correctable error threshold for modulation profile 1 (1–20%)                                                                                                                                |
| <code>ccsUpSpecMgmtFecCorrectThres2</code>   | Integer32    | Deprecated and no longer used                                                                                                                                                                                 |
| <code>ccsUpSpecMgmtFecUnCorrectThres1</code> | Integer32    | Specifies the FEC uncorrectable error threshold for modulation profile 1 (1–20%)                                                                                                                              |
| <code>ccsUpSpecMgmtFecUnCorrectThres2</code> | Integer32    | Deprecated and no longer used                                                                                                                                                                                 |
| <code>ccsUpSpecMgmtSnrPollPeriod</code>      | Integer32    | Deprecated and no longer used                                                                                                                                                                                 |
| <code>ccsUpSpecMgmtHopCondition</code>       | INTEGER      | Reports the condition that triggers a frequency hop (SNR value or percentage of modems going offline)                                                                                                         |
| <code>ccsUpSpecMgmtFromCenterFreq</code>     | CCSFrequency | Provides the center frequency (in KHz) before the latest frequency hop                                                                                                                                        |
| <code>ccsUpSpecMgmtToCenterFreq</code>       | CCSFrequency | Provides the current center frequency (in KHz) after the latest frequency hop                                                                                                                                 |
| <code>ccsUpSpecMgmtFromBandWidth</code>      | CCSFrequency | Provides the channel width (in KHz) before the latest frequency hop                                                                                                                                           |
| <code>ccsUpSpecMgmtToBandWidth</code>        | CCSFrequency | Provides the current channel width (in KHz) after the latest frequency hop                                                                                                                                    |
| <code>ccsUpSpecMgmtFromModProfile</code>     | Integer32    | Provides the modulation profile number before the latest frequency hop                                                                                                                                        |

**Table 13** *ccsUpSpecMgmtEntry Attributes (continued)*

| Attribute                 | Type      | Description                                                                   |
|---------------------------|-----------|-------------------------------------------------------------------------------|
| ccsUpSpecMgmtToModProfile | Integer32 | Provides the current modulation profile number after the latest frequency hop |
| ccsUpSpecMgmtSNR          | Integer32 | Provides the current SNR value (in dB) for the upstream                       |

## ccsHoppingNotification

Table 14 describes the attributes contained in the notification that is sent after each frequency hop:

**Table 14** *ccsHoppingNotification Attributes*

| Attribute                   | Type         | Description                                                                                           |
|-----------------------------|--------------|-------------------------------------------------------------------------------------------------------|
| ccsUpSpecMgmtHopCondition   | INTEGER      | Reports the condition that triggers a frequency hop (SNR value or percentage of modems going offline) |
| ccsUpSpecMgmtFromCenterFreq | CCSFrequency | Provides the center frequency (in KHz) before the latest frequency hop                                |
| ccsUpSpecMgmtToCenterFreq   | CCSFrequency | Provides the current center frequency (in KHz) after the latest frequency hop                         |
| ccsUpSpecMgmtFromBandWidth  | CCSFrequency | Provides the channel width (in KHz) before the latest frequency hop                                   |
| ccsUpSpecMgmtToBandWidth    | CCSFrequency | Provides the current channel width (in KHz) after the latest frequency hop                            |
| ccsUpSpecMgmtFromModProfile | Integer32    | Provides the modulation profile number before the latest frequency hop                                |
| ccsUpSpecMgmtToModProfile   | Integer32    | Provides the current modulation profile number after the latest frequency hop                         |

# Configuration Examples

- [Upstream Traffic Shaping and Rate Limiting Examples, page 411](#)
- [Downstream Traffic Shaping and Rate Limiting Examples, page 414](#)
- [Spectrum Group and Combiner Group Examples, page 415](#)
- [Other Spectrum Management Configuration Examples, page 417](#)
- [Dynamic Upstream Modulation Examples, page 419](#)
- [Input Power Level Example, page 420](#)
- [Advanced Spectrum Management Configuration Examples, page 421](#)

## Upstream Traffic Shaping and Rate Limiting Examples

Upstream rate limiting is enabled by default in the Cisco CMTS router, so the **cable upstream rate-limit** command does not appear in the router's configuration file. To determine if upstream rate limiting is configured and activated, enter the **show running-config** command and look for the cable interface configuration information.

If upstream rate limiting is disabled, no **cable upstream rate-limit** appears in the output. You can also perform the following tasks to verify that rate limiting is enabled on the upstream channel:

- 
- Step 1** Configure a low-peak upstream rate limit for the cable modem in its QoS profile. Either use the command-line interface (CLI) to modify the modem's QoS profile, or edit the modem's TFTP configuration file.
- Use a regular rate-limiting algorithm on the upstream without rate shaping and note the drops of the excess bandwidth requests from this cable modem when it exceeds its peak upstream rate.
- Use the **show interface cx/y sid counters** command to see the bandwidth request drops. Verify that the upstream rate received by that modem is less than its configured peak rate due to the timeouts and backoffs produced by the drop in bandwidth requests. Enter the **show interface cx/y sid** command to see the input rate at CMTS in bps.
- Step 2** Enable grant shaping on the upstream channel by using the new **shaping** keyword extension to the token-bucket algorithm CLI command.
- Step 3** Make the cable modem exceed its peak upstream rate by generating upstream traffic, and note the effect of grant buffering (shaping) at the CMTS. If you use cable modem-to-CMTS pings, you see a perceivable slowing down of the pings.
- Let the pings run for a period to let averages at the CMTS settle; then view the upstream rate received by this single modem. Use the **show interface cx/y** command and see the input rate in bps. This value should be close to the modem's peak upstream rate. Also note the drop counts for the modem's SID by using the **show interface sid counters** command, and verify that the CMTS no longer drops the bandwidth requests from the cable modem.
- The bandwidth request drop count (from previous nonshaping test) remains unchanged when upstream rate shaping is used, indicating that the CMTS is actually shaping (buffering) the grants for the modem. Verify that the input rate at the CMTS (from the single rate-exceeded CM) stabilizes close to the configured peak rate of 128 Kbps.
-

- Ensure that the cable connections are not loose or disconnected.
- Ensure that the cable interface line card is firmly seated in its chassis slot.
- Ensure that the captive installation screws are tight.
- Verify that you have entered the correct slot and port numbers.
- Verify that you selected a valid frequency for your router.

## Enabling Shaping Example

## Forcing the Cable Modem to Exceed the Peak Rate Example

Cisco IOS Release 12.2 BC

```

Received 92 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
4004 packets output, 5868720 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 output buffer failures, 0 output buffers swapped out

```

```
Router# show int c3/0 sid counters
```

| Sid | Inpackets | Inoctets | Outpackets | Outoctets | Ratelimit<br>BWReqDrop | Ratelimit<br>DSPktDrop |
|-----|-----------|----------|------------|-----------|------------------------|------------------------|
| 1   | 4780      | 6996880  | 4774       | 6987772   | 6244                   | 0                      |

```
Router# show int c3/0 sid counters
```

| Sid | Inpackets | Inoctets | Outpackets | Outoctets | Ratelimit<br>BWReqDrop | Ratelimit<br>DSPktDrop |
|-----|-----------|----------|------------|-----------|------------------------|------------------------|
| 1   | 4866      | 7122488  | 4865       | 7120970   | 6244                   | 0                      |

## Downstream Traffic Shaping and Rate Limiting Examples

### Downstream Rate Limiting Example

The following example shows how to apply the token-bucket filter algorithm:

```
router(config-if)# cable downstream rate-limit token-bucket shaping
```

### Verifying Downstream Rate Limiting Example

To determine if downstream rate limiting is configured and activated, enter the **show running-config** command and look for the cable interface configuration information. If downstream rate limiting is configured and enabled, a rate limiting entry appears in the output. If downstream rate limiting is disabled, no rate limiting entry appears.

```
CMTS01# show running-config
```

```

Building configuration...
Current configuration:
!
interface cable5/0/0
ip address 10.254.254.254 255.0.0.0
no ip directed-broadcast
cable helper-address 192.168.1.1
no keepalive
cable downstream rate-limit token-bucket shaping
cable downstream annex B
cable downstream modulation 64qam

```

Perform these steps if you are having difficulty with verification:

- Ensure that the cable connections are not loose or disconnected.
- Ensure that the cable interface line card is firmly seated in its chassis slot.
- Ensure that the captive installation screws are tight.
- Verify that you have entered the correct slot and port numbers
- Verify that you selected the default if you are not certain about the modulation rate needed.
- Verify the downstream carrier is active using the **cable downstream if-output** command.

## Spectrum Group and Combiner Group Examples

### Verifying Spectrum Group Creation Example

To verify that a spectrum group has been created, enter the **show cable spectrum-group** command:

```
CMTS01# show cable spectrum-group

spectrum-group 1
spectrum-group 2
spectrum-group 3
```

### Time-Scheduled Spectrum Group Example

If your cable plant has an upstream noise characteristic on a weekly cycle, use time-scheduled spectrum allocation. An example follows:

```
CMTS01(config)# cable spectrum-group 1 time Mon 08:00:00 frequency 21600000
```

Deletion is performed using the **delete** keyword:

```
CMTS01(config)# cable spectrum-group 1 time Mon 18:00:00 delete frequency 21600000
```

### Verifying Spectrum Group Configuration Example

To verify if spectrum groups have been configured and activated, enter the **show cable spectrum-group** command. This command displays each spectrum group, the frequencies assigned to it, the upstream port to which it has been assigned, whether a schedule exists for it, the currently measured power level, and whether it is a shared spectrum group.

```
CMTS01# show cable spectrum-group

22:07:46: %SYS-5-CONFIG_I: Configured from console by console
Group Frequency Upstream Weekly Scheduled Power Shared
No. Band Port Availability Level Spectrum
 (Mhz)
1 5.000-15.000
1 12.000
1 22.000 Cable6/0 U5 From Time: To Time: 7 Yes
2 29.000 Cable6/0 U4 6 No
2 26.000 0 No
3 35.000-41.000
3 16.000-19.000 Cable6/0 U3 5 No
5* 5.000-10.000 Thu 21:50:00 Thu 21:45:00 0 Yes
```

```
CMTS01#
```

### Determining the Upstream Ports Assigned to a Combiner Group Example

Following is a sample topology for a CMTS with combiner groups designated A through J. Combiner groups C and E have multiple upstream ports that should be configured in a shared spectrum group. The other upstreams should be configured in a nonshared spectrum group.

In this example, ten combiner groups are served with frequency hop tables from three spectrum groups:

```
Cable3/0
DS +-----+ Upconverter +----- laser group 1
U0 +----- combiner group A
```

```

U1 +----- combiner group B
U2 +-----combiner group C
U3 +-----combiner group C
U4 +----- combiner group D
U5 +-----combiner group E

Cable4/0
DS +-----+ Upconverter +----- laser group 2
U0 +-----combiner group E
U1 +----- combiner group F
U2 +----- combiner group G
U3 +----- combiner group H
U4 +----- combiner group I
U5 +----- combiner group J

```

The laser group term refers to the set of fiber nodes that share the same downstream signal. An optical splitter is often used to create individual feeds per node.

In the downstream direction, two 6-MHz channel slots are assigned. All fiber nodes in combiner groups A through E should have a channel slot containing the downstream signal from Cable3/0. Combiner groups A through E are said to belong to laser group 1.

All fiber nodes in combiner groups E through J should have a channel slot containing the downstream signal from Cable4/0. Combiner groups E through J are said to belong to laser group 2.

Because combiner group E belongs to two laser groups, there should be two different downstream channel slots for Cable3/0 and Cable4/0.

## Combiner Group Example

The following example enables spectrum management for all upstream ports, where all combiner groups use the frequency band from 20 to 26 MHz:

```

CMTS01(config)# cable spectrum-group 1 band 20000000 26000000
CMTS01(config)# cable spectrum-group 2 shared
CMTS01(config)# cable spectrum-group 2 band 20000000 26000000
CMTS01(config)# cable spectrum-group 3 shared
CMTS01(config)# cable spectrum-group 3 band 20000000 26000000
CMTS01(config)# interface Cable3/0
CMTS01(config-if)# cable spectrum-group 1
CMTS01(config-if)# cable upstream 2 spectrum-group 2
CMTS01(config-if)# cable upstream 3 spectrum-group 2
CMTS01(config-if)# cable upstream 5 spectrum-group 3
CMTS01(config-if)# exit
CMTS01(config)# interface Cable4/0
CMTS01(config-if)# cable spectrum-group 1
CMTS01(config-if)# cable upstream 0 spectrum-group 3

```

A description of the spectrum groups 1 through 3 follows:

- Spectrum group 1—This group is nonshared. Upstream RF domains exist for each member upstream port.

| Upstream Port | RF Domain        |
|---------------|------------------|
| Cable3/0 U0   | combiner group A |
| Cable3/0 U1   | combiner group B |
| Cable3/0 U4   | combiner group D |
| Cable4/0 U1   | combiner group F |
| Cable4/0 U2   | combiner group G |
| Cable4/0 U3   | combiner group H |
| Cable4/0 U4   | combiner group I |
| Cable4/0 U5   | combiner group J |



- Spectrum group 2—This group is shared. A single upstream RF domain exists.

|               |                  |
|---------------|------------------|
| Upstream Port | RF Domain        |
| Cable3/0 U2   | combiner group C |
| Cable3/0 U3   | combiner group C |

- Spectrum group 3—This group is shared. A single upstream RF domain exists.

|               |                  |
|---------------|------------------|
| Upstream Port | RF Domain        |
| Cable3/0 U5   | combiner group E |
| Cable4/0 U0   | combiner group E |

For the 20- to 26-MHz band of each RF domain, the spectrum is channelized according to the channel width settings of each member port. For example, if the ports U2 and U3 of Cable3/0 are set to 3.2 MHz and 1.6 MHz channel widths, respectively, then spectrum group 2 uses the following channelization:

```
> Channel Width Start Stop Center
> (Mhz) (Mhz) (Mhz) (Mhz)
> 1 3.2 20.0 23.2 21.6
> 2* 1.6 20.0 21.6 20.8
> 3* 1.6 21.6 23.2 22.4
> 4 1.6 23.2 24.8 24.0
```

**Note**

Channels 2 and 3 are not available when channel 1 is in use.

Because the group is shared, ports U2 and U3 will be assigned channels 1 and 4, respectively, to prevent overlap.

**Note**

There are no alternate frequency assignments for either port, and bandwidth is wasted from 24.8 to 26.0 MHz. To create alternate channels, increase the upper boundary from 26.0 to 28.0 MHz.

```
> Channel Width Start Stop Center
> (Mhz) (Mhz) (Mhz) (Mhz)
> 1 3.2 20.0 23.2 21.6
> 2 3.2 23.2 26.4 24.8
> 3 1.6 20.0 21.6 20.8
> 4 1.6 21.6 23.2 22.4
> 5 1.6 23.2 24.8 24.0
> 6 1.6 24.8 26.4 25.6
> 7 1.6 26.4 28.0 27.4
```

Try to reduce the spectrum allocation when it is used with small channel widths. Otherwise, there will be a large number of upstream channel slots, and the frequency hopping may require several minutes to find a clean slot.

## Other Spectrum Management Configuration Examples

To configure differing spectrum groups, refer to the following examples:

- Use the following example to add time-scheduled spectrum. You can add spectrum on a weekly schedule by including an optional weekday and time:

```
Router(config)# cable spectrum-group 1 time Mon 08:00:00 frequency 21600000
```

Use the **delete** keyword to delete the frequency:

```
Router(config)# cable spectrum-group 1 time Mon 18:00:00 delete frequency 21600000
```

- Use the following example to configure spectrum group 1 with an upstream frequency of 6,500,000 Hz and a default power level of 0 dBmV:

```
Router(config)# cable spectrum-group 1 frequency 6500000
```

- Use the following example to add the upstream frequency 7,000,000 Hz to the list of valid frequencies with a default power level of 0 dBmV for spectrum group 1:

```
Router(config)# cable spectrum-group 1 frequency 7000000
```

- Use the following example to configure spectrum group 2 with an upstream frequency 7,500,000 Hz and change the power level to 5 dBmV:

```
Router(config)# cable spectrum-group 2 frequency 7500000 5
```

- Use the following example to configure spectrum group 3 with an upstream band of 12,000,000 to 18,000,000 Hz and default power level of 0 dBmV:

```
Router(config)# cable spectrum-group 3 band 12000000 18000000
```

- Use the following example to add the upstream band 20,000,000 to 24,000,000 Hz to the list of valid bands with a change in the power level of 13 dBmV for spectrum group 3:

```
Router(config)# cable spectrum-group 3 band 20000000 24000000 13
```

- Use the following example to configure a continuous band between 5,000,004 and 40,000,000 Hz for scheduled spectrum group 4 with a default power level of 0 dBmV. The band is available to the spectrum group starting at 12:00 p.m. local time each Monday:

```
Router(config)# cable spectrum-group 4 time Monday 12:00:00 band 5000004 40000000
```

- Use the following example to add the upstream frequency 9,500,000 Hz to the list of valid frequencies and change the nominal power level to 5 dBmV. The spectrum manager adjusts frequencies and power levels on this group at 2:00 a.m. local time each day:

```
Router(config)# cable spectrum-group 3 time 02:00:00 frequency 9500000 5
```

- Use the following example to configure the minimum period before which a frequency hop can occur in seconds:

```
Router(config)# cable spectrum-group 3 hop period 800
```

- Use the following example to configure the threshold value (expressed as a percentage) of the number of “offline” modems identified before the router initiates an automatic frequency hop:

```
Router(config)# cable spectrum-group 3 hop threshold 40
```

- Use the following example to configure a particular spectrum group as a shared RF spectrum group. Specifying a given spectrum group as “shared” tells the router that you want to be sure that upstream frequencies assigned to upstream ports are not assigned to additional upstream ports:

```
Router(config)# cable spectrum-group 3 shared
```

- Use the following example to remove a specified spectrum group from your configuration:

```
Router(config)# no cable spectrum-group 3
```

- The following is an example of a spectrum group configuration that is designed to perform minor equalization as a function of frequency.

```
CMTS01(config)# cable spectrum-group 1 frequency 21600000
CMTS01(config)# cable spectrum-group 1 frequency 24800000 1
CMTS01(config)# cable spectrum-group 1 frequency 28000000 2
```

In this example, the upstream port receives power at 21.6 MHz with a default power level of 0 dBmV, at 24.8 MHz with a power level of 1 dBmV, and at 28.0 MHz with a power level of 2 dBmV. At any time, the power level set in the interface configuration overrides the spectrum group power level.

## Dynamic Upstream Modulation Examples

The following examples describe how to display modulation profile information with the **show cable modulation-profile** command and to define a modulation profile with the **cable modulation-profile** command.

### Verifying Your Settings

- Step 1** To check the value of the settings you have entered, enter the **show running-config** command in privileged EXEC mode at the `Router#` prompt:

```
Router# show running-config
```

To review changes you make to the configuration, use the **show startup-config** command in privileged EXEC mode to display the information stored in NVRAM.

- Step 2** To display modulation profile group information, use the **show cable modulation-profile** command in privileged EXEC mode:

```
Router# show cable modulation-profile [profile] [iuc-code]
```

*profile*—(Optional) Profile number. Valid values are from 1 to 8.

*iuc-code*—(Optional) Internal usage code.

Valid options are:

- **initial**—Initial ranging burst
- **long**—Long grant burst
- **request**—Request burst
- **short**—Short grant burst
- **station**—Station ranging burst

### Modulation Profiles Example

In Cisco IOS Release 12.1(3a)EC1 and later, the Cisco CMTS has one preconfigured modulation profile resident in memory, which defines a typical profile for QPSK modulation. To use the Dynamic Upstream Modulation feature, a second profile must be created that is unique from the first profile, and typically provides a higher, more robust modulation scheme.

The following example is a modulation profile for QAM-16, in which the initial, request, and station maintenance messages are sent as QPSK, and the short and long data packets are sent as QAM-16. The QAM-16 modulation is more bandwidth-efficient than QPSK, but QPSK is more robust than QAM-16.

**Note**

The upstream request and station maintenance messages use less time on the cable network when configured in QPSK for symbol rates of 640, 1280, and 2560K symbols/sec. Thus, these messages are actually more efficient when used in QPSK mode and they ensure a more reliable modem connection. The upstream initial maintenance message takes exactly the same amount of time on the cable network, no matter how it is configured. Modems connect more quickly and experience fewer cycles of power adjustment during initial maintenance if the system is set for QPSK.

```
Router# configure terminal
Router(config)# cable modulation-profile 2 request 0 16 1 8 qpsk scrambler
152 no-diff 64 fixed uw16
Router(config)# cable modulation-profile 2 initial 5 34 0 48 qpsk scrambler
152 no-diff 128 fixed uw16
Router(config)# cable modulation-profile 2 station 5 34 0 48 qpsk scrambler
152 no-diff 128 fixed uw16
Router(config)# cable modulation-profile 2 short 6 75 6 8 16qam scrambler 152
no-diff 72 fixed uw16
Router(config)# cable modulation-profile 2 long 8 220 0 8 16qam scrambler 152
no-diff 160 fixed uw16
```

In the following example, all message types are carried with QAM-16 modulation. Although QAM-16 modulation offers a consistent modulation scheme for all five types of messages, the added length of the QAM-16 preamble offsets the increased bandwidth efficiency of the MAC data message for the station maintenance messages and bandwidth request messages.

```
Router# configure terminal
Router(config)# cable modulation-profile 2 request 0 16 1 8 16qam scrambler
152 no-diff 128 fixed uw16
Router(config)# cable modulation-profile 2 initial 5 34 0 48 16qam
scrambler 152 no-diff 256 fixed uw16
Router(config)# cable modulation-profile 2 station 5 34 0 48 16qam
scrambler 152 no-diff 256 fixed uw16
Router(config)# cable modulation-profile 2 short 5 75 6 8 16qam scrambler
152 no-diff 144 fixed uw16
Router(config)# cable modulation-profile 2 long 8 220 0 8 16qam scrambler
152 no-diff 160 fixed uw16
```

**Note**

When using DOCSIS concatenation with a 16-QAM or mixed symbol rate, configure the CMTS for Unique Word 16 ("uw16") in the preamble for both short and long data burst profiles.

Add the **cable upstream port-number modulation-profile primary profile-number secondary profile-number** command to the appropriate interfaces. In this example, modulation-profile 2 is for QAM-16 modulation and profile 1 is for QPSK modulation.

```
Router# configure terminal
Router(config)# interface Cable6/0
Router(config-if)# cable upstream 0 modulation-profile 2 1
```

## Input Power Level Example

In the following example, the modem transmit power at 24.8 MHz is adjusted upstream by 1 dBmV and the modem transmit power at 28.0 MHz is adjusted upstream by 2 dBmV.

```
CMTS01(config)# cable spectrum-group 1 frequency 21600000
CMTS01(config)# cable spectrum-group 1 frequency 24800000 1
CMTS01(config)# cable spectrum-group 1 frequency 28000000 2
```

## Advanced Spectrum Management Configuration Examples

This section provides the following typical configurations:

- [Advanced Spectrum Management for the Cisco uBR7200 Series Router Example, page 421](#)
- [Advanced Spectrum Management for the Cisco uBR10012 Router Example, page 424](#)

### Advanced Spectrum Management for the Cisco uBR7200 Series Router Example

This section provides a typical configuration example for a Cisco uBR7200 series router using the Cisco uBR-MC16S cable interface line card. This configuration does the following:

- Creates three spectrum groups with different frequency bands, hop periods, and hop thresholds.
- Creates two upstream modulation profiles, one for QPSK operation and one for QAM-16 operation, by specifying the parameters for each burst type.
- Creates two upstream modulation profiles, one for QPSK operation and one for mixed QPSK/QAM-16 operation, using the default profile options (**qpsk** and **mix**).
- Configures one upstream (port 5) on cable interface 3/0 to use spectrum group 3.
- Configures the upstreams with the primary modulation profile set to mixed QPSK/QAM-16 operation and the secondary modulation profile set for QPSK operation.
- Configures the upstream so that when its noise threshold is reached, it first attempts to change the frequency, then the channel-width, and finally to switch the modulation profile (using the Dynamic Upstream Modulation feature).

```
!
version 12.1
no service pad
no service password-encryption
service udp-small-servers
service tcp-small-servers
!
hostname ubr7200
!
!
! Define a frequency band for a 1.6 MHz channel around center frequency of 20.800 MHz
cable spectrum-group 1 band 19750000 21850000 0
! Define a frequency band for a 1.6 MHz channel around center frequency of 23.200 MHz
cable spectrum-group 1 band 22150000 24250000 0
! Hop period set to 30 sec to avoid modems going offline before initiating a hop priority
cable spectrum-group 1 hop period 30
! Percentage of missed station maintenance from modems
cable spectrum-group 1 hop threshold 20
!
cable modulation-profile 1 initial 5 34 0 48 qpsk scrambler 152 no-diff 128 fixed uw16
cable modulation-profile 1 station 5 34 0 48 qpsk scrambler 152 no-diff 128 fixed uw16

! Create second modulation profile numbered 4
cable modulation-profile 4 request 0 16 0 8 qpsk scrambler 152 no-diff 64 fixed uw16
cable modulation-profile 4 initial 5 34 0 48 qpsk scrambler 152 no-diff 128 fixed uw16
cable modulation-profile 4 station 5 34 0 48 qpsk scrambler 152 no-diff 128 fixed uw16
cable modulation-profile 4 short 6 75 6 8 16qam scrambler 152 no-diff 144 shortened uw16
cable modulation-profile 4 long 8 220 0 8 16qam scrambler 152 no-diff 160 shortened uw16

! Create two modulation profiles using the default QPSK and QPSK/16-QAM profiles
cable modulation-profile 3 qpsk
cable modulation-profile 5 mix
!
```

```

no cable qos permission create
no cable qos permission update
cable qos permission modems
cable time-server
clock calendar-valid
no ip subnet-zero
no ip domain-lookup
!
!
!
interface FastEthernet0/0
 no ip address
 no ip mroute-cache
 shutdown
 media-type MII
 full-duplex
!
interface Ethernet1/0
 ip address 10.11.10.1 255.0.0.0
 no ip mroute-cache
 half-duplex
!

interface Cable3/0
 ip address 255.255.255.0 secondary
 ip address 255.255.255.0
 no keepalive
 cable map-advance static
 cable bundle 1 master
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream frequency 687000000
! Assign upstream to spectrum group
 cable upstream 0 spectrum-group 1
! Set channel-width to be fixed at 1.6 MHz
 cable upstream 0 channel-width 1600000 1600000
! Set priority of corrective actions
 cable upstream 0 hop-priority frequency channel-width modulation
! Set the thresholds for corrective action
 cable upstream 0 threshold cnr-profile1 23 cnr-profile2 15 Corr-Fec 5 Uncorr-Fec 1
! Assign modulation profiles to upstream port in order of preference
 cable upstream 0 modulation-profile 5 1
 no cable upstream 0 concatenation
 no cable upstream 0 shutdown
 cable upstream 1 spectrum-group 1
 cable upstream 1 channel-width 1600000 1600000
 cable upstream 1 hop-priority frequency channel-width modulation
 cable upstream 1 threshold cnr-profile1 23 cnr-profile2 15 Corr-Fec 5 Uncorr-Fec 1
 cable upstream 1 modulation-profile 5 1
 no cable upstream 1 concatenation
 no cable upstream 1 shutdown
 cable upstream 2 spectrum-group 1
 cable upstream 2 channel-width 1600000 1600000
 cable upstream 2 hop-priority frequency channel-width modulation
 cable upstream 2 threshold cnr-profile1 23 cnr-profile2 15 Corr-Fec 5 Uncorr-Fec 1
 cable upstream 2 modulation-profile 5 1
 no cable upstream 2 concatenation
 no cable upstream 2 shutdown
 cable upstream 3 spectrum-group 1
 cable upstream 3 channel-width 1600000 1600000
 cable upstream 3 hop-priority frequency channel-width modulation
 cable upstream 3 threshold cnr-profile1 23 cnr-profile2 15 Corr-Fec 5 Uncorr-Fec 1
 cable upstream 3 modulation-profile 5 1

```

```
no cable upstream 3 concatenation
no cable upstream 3 shutdown
cable upstream 4 spectrum-group 1
cable upstream 4 channel-width 1600000 1600000
cable upstream 4 hop-priority frequency channel-width modulation
cable upstream 4 threshold cnr-profile1 23 cnr-profile2 15 Corr-Fec 5 Uncorr-Fec 1
cable upstream 4 modulation-profile 5 1
no cable upstream 4 concatenation
no cable upstream 4 shutdown
cable upstream 5 spectrum-group 1
cable upstream 5 channel-width 1600000 1600000
cable upstream 5 hop-priority frequency channel-width modulation
cable upstream 5 threshold cnr-profile1 23 cnr-profile2 15 Corr-Fec 5 Uncorr-Fec 1
cable upstream 5 modulation-profile 5 1
no cable upstream 5 concatenation
no cable upstream 5 shutdown
no cable dci-response
cable dhcp-giaddr policy
!
interface Cable4/0
no ip address
no keepalive
cable map-advance static
cable bundle 1
cable downstream annex B
cable downstream modulation 64qam
cable downstream interleave-depth 32
cable downstream frequency 687000000
cable upstream 0 spectrum-group 1
cable upstream 0 channel-width 1600000 1600000
cable upstream 0 hop-priority frequency channel-width modulation
cable upstream 0 threshold cnr-profile1 23 cnr-profile2 15 Corr-Fec 5 Uncorr-Fec 1
cable upstream 0 modulation-profile 5 1
no cable upstream 0 concatenation
no cable upstream 0 shutdown
cable upstream 1 spectrum-group 1
cable upstream 1 channel-width 1600000 1600000
cable upstream 1 hop-priority frequency channel-width modulation
cable upstream 1 threshold cnr-profile1 23 cnr-profile2 15 Corr-Fec 5 Uncorr-Fec 1
cable upstream 1 modulation-profile 5 1
no cable upstream 1 concatenation
no cable upstream 1 shutdown
cable upstream 2 spectrum-group 1
cable upstream 2 channel-width 1600000 1600000
cable upstream 2 hop-priority frequency channel-width modulation
cable upstream 2 threshold cnr-profile1 23 cnr-profile2 15 Corr-Fec 5 Uncorr-Fec 1
cable upstream 2 modulation-profile 5 1
no cable upstream 2 concatenation
no cable upstream 2 shutdown
cable upstream 3 spectrum-group 1
cable upstream 3 channel-width 1600000 1600000
cable upstream 3 hop-priority frequency channel-width modulation
cable upstream 3 threshold cnr-profile1 23 cnr-profile2 15 Corr-Fec 5 Uncorr-Fec 1
cable upstream 3 modulation-profile 5 1
no cable upstream 3 concatenation
no cable upstream 3 shutdown
cable upstream 4 spectrum-group 1
cable upstream 4 channel-width 1600000 1600000
cable upstream 4 hop-priority frequency channel-width modulation
cable upstream 4 threshold cnr-profile1 23 cnr-profile2 15 Corr-Fec 5 Uncorr-Fec 1
cable upstream 4 modulation-profile 5 1
no cable upstream 4 concatenation
no cable upstream 4 shutdown
cable upstream 5 spectrum-group 1
```

```

cable upstream 5 channel-width 1600000 1600000
cable upstream 5 hop-priority frequency channel-width modulation
cable upstream 5 threshold cnr-profile1 23 cnr-profile2 15 Corr-Fec 5 Uncorr-Fec 1
cable upstream 5 modulation-profile 5 1
no cable upstream 5 concatenation
no cable upstream 5 shutdown
no cable dci-response
cable dhcp-giaddr primary
!
ip default-gateway 10.11.0.1
ip classless
ip route 10.11.254.254 255.255.255.255 10.11.0.1
no ip http server
!
!
snmp-server engineID local 00000009020000D0CAA7BB00
snmp-server community private RW
snmp-server trap-source FastEthernet0/0
snmp-server packetize 2048
snmp-server system-shutdown
snmp-server enable traps cable hopping
snmp-server manager
!
!
line con 0
 exec-timeout 0 0
 transport input none
line aux 0
line vty 0 4
 no login
!
end

```

## Advanced Spectrum Management for the Cisco uBR10012 Router Example

This section provides an excerpt from a typical configuration example for a Cisco uBR10012 router using the Cisco uBR-LCP2-MC16S cable interface line card. This configuration does the following:

- Configures four spectrum groups with a hop period of 30 seconds.
- Creates a QPSK modulation profile and assigns it to four upstreams on the Cisco uBR-LCP2-MC16S cable interface line card in slot 6/1/0.
- Assigns a spectrum group to each of the four upstreams.
- Configures each upstream for the default CNR and FEC thresholds.

```

Current configuration : 4899 bytes
!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service internal
!
hostname UBR10012
!
no logging rate-limit
!
redundancy
 main-cpu

```



```
 auto-sync standard
card 1/0 1gigetheretnet-1
card 1/1 2cable-tccplus
card 4/0 1oc12pos-1
card 6/1 1cable-mc16s
card 7/0 1cable-mc16s
card 8/0 1cable-mc16s
card 8/1 1cable-mc16s
cable spectrum-group 1 hop period 30
cable spectrum-group 1 band 6000000 11000000
cable spectrum-group 2 hop period 30
cable spectrum-group 2 band 12000000 17000000
cable spectrum-group 3 hop period 30
cable spectrum-group 3 band 18000000 23000000
cable spectrum-group 4 hop period 30
cable spectrum-group 4 band 24000000 31000000
cable modulation-profile 2 qpsk
interface Cable6/1/0
 ip address 10.55.0.1 255.255.0.0
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
! upstream 0
 cable upstream 0 spectrum-group 1
 cable upstream 0 modulation-profile 2
 cable upstream 0 threshold cnr-profile1 16 cnr-profile2 5 Corr-Fec 1 Uncorr-Fec 1
 no cable upstream 0 shutdown
! upstream 1
 cable upstream 1 spectrum-group 2
 cable upstream 1 modulation-profile 2
 cable upstream 1 threshold cnr-profile1 16 cnr-profile2 5 Corr-Fec 1 Uncorr-Fec 1
 no cable upstream 1 shutdown
! upstream 2
 cable upstream 2 spectrum-group 3
 cable upstream 2 modulation-profile 2
 cable upstream 2 threshold cnr-profile1 16 cnr-profile2 5 Corr-Fec 1 Uncorr-Fec 1
 no cable upstream 2 shutdown
! upstream 3
 cable upstream 3 spectrum-group 4
 cable upstream 3 modulation-profile 2
 cable upstream 3 threshold cnr-profile1 16 cnr-profile2 5 Corr-Fec 1 Uncorr-Fec 1
 no cable upstream 3 shutdown
```

# Additional References

The following sections provide references related to Spectrum Management for the Cisco CMTS routers.

## Related Documents

| Related Topic                            | Document Title                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CMTS Command Reference                   | <p><i>Cisco Broadband Cable Command Reference Guide</i>, at the following URL:</p> <p><a href="http://www.cisco.com/univercd/cc/td/doc/product/cable/bbcmref/index.htm">http://www.cisco.com/univercd/cc/td/doc/product/cable/bbcmref/index.htm</a></p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Cisco IOS Release 12.2 Command Reference | <p>Cisco IOS Release 12.2 Configuration Guides and Command References, at the following URL:</p> <p><a href="http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/index.htm">http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/index.htm</a></p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Cable Features Configuration Guide       | <p><i>Cisco CMTS Feature Guide</i>, at the following URL:</p> <p><a href="http://www.cisco.com/univercd/cc/td/doc/product/cable/cab_rout/cmtsfg/index.htm">http://www.cisco.com/univercd/cc/td/doc/product/cable/cab_rout/cmtsfg/index.htm</a></p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Installing Cisco uBR7100 series routers  | <i>Cisco uBR7100 Series Universal Broadband Router Hardware Installation Guide</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Configuring Cisco uBR7100 series routers | <i>Cisco uBR7100 Series Universal Broadband Router Software Configuration Guide</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Installing Cisco uBR7200 Series Routers  | <p><i>Cisco uBR7200 Series Universal Broadband Router Hardware Installation Guide</i></p> <p><i>Cisco uBR7200 Series Universal Broadband Router Cable Modem Card Installation and Configuration publication</i></p> <p><i>Cisco uBR7200 Series Universal Broadband Router Port Adapter Installation and Configuration publication</i></p> <p><i>Cisco uBR7200 Series Universal Broadband Router 550-Watt DC-Input Power Supply Replacement Instructions</i></p> <p><i>Cisco uBR7200 Series Universal Broadband Router Subchassis and Midplane Replacement Instructions</i></p> <p><i>Cisco uBR7200 Series Rack-Mount and Cable-Management Kit Installation Instructions</i></p> <p><i>Cisco uBR7200 Series Universal Broadband Router Fan Tray Replacement Instructions</i></p> |
| Configuring Cisco uBR7200 Series Routers | <p><i>Cisco uBR7200 Series Universal Broadband Router Software Configuration Guide</i></p> <p><i>Cisco uBR7200 Series Universal Broadband Router Feature Enhancements publication</i></p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

| Related Topic                         | Document Title                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Installing Cisco uBR10012 Router      | <a href="#">Cisco uBR10012 Series Universal Broadband Router Hardware Installation Guide</a><br><a href="#">2400W AC-Input Power Shelf for the Cisco uBR10000 Series Universal Broadband Router</a><br><a href="#">Cable Interface Line Card Processor Hardware Installation for the Cisco uBR10000 Series Universal Broadband Router</a><br><a href="#">Fan Assembly Module for the Cisco uBR10000 Series Universal Broadband Router</a><br><a href="#">DC Power Entry Module for the Cisco uBR10000 Series Universal Broadband Router</a><br><a href="#">Performance Routing Engine Card Hardware Installation for the Cisco uBR10000 Series Universal Broadband Router</a><br><a href="#">TCC+ Card for the Cisco uBR10000 Series Universal Broadband Router</a> |
| Configuring the Cisco uBR10012 Router | <a href="#">Cisco uBR10012 Universal Broadband Router Software Configuration Guide</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

## Standards

| Standards                              | Title                                                                                                           |
|----------------------------------------|-----------------------------------------------------------------------------------------------------------------|
| <a href="#">SP-RFIV1.1-I09-020830</a>  | Data-over-Cable Service Interface Specifications Radio Frequency Interface Specification, version 1.1           |
| <a href="#">SP-RFIV2.0-I03-021218</a>  | Data-over-Cable Service Interface Specifications Radio Frequency Interface Specification, version 2.0           |
| <a href="#">SP-OSSIV2.0-I03-021218</a> | Data-over-Cable Service Interface Specifications Operations Support System Interface Specification, version 2.0 |
| <a href="#">SP-BPI+-I09-020830</a>     | Data-over-Cable Service Interface Specifications Baseline Privacy Plus Interface Specification, version 2.0     |

## MIBs

| MIBs                                                                                       | MIBs Link                                                                                                                                                                                                                         |
|--------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li><a href="#">CISCO-CABLE-SPECTRUM-MIB</a></li> </ul> | <p>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:</p> <p><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></p> |

## RFCs

No new or modified RFCs are supported by this feature.

## Technical Assistance

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



## Telco Return for the Cisco CMTS

---

The Telco Return feature allows service providers to offer Data-over-Cable Service Interface Specification (DOCSIS) 1.0 internet access over a one-way cable network. Downstream data is sent to the telco return cable modems over the cable network, while upstream data is sent from the cable modem to the headend over a separate dial-up connection.

### Feature Specifications for Telco Return

| Feature History                                                         |                                                                       |
|-------------------------------------------------------------------------|-----------------------------------------------------------------------|
| Release                                                                 | Modification                                                          |
| 12.0(4)XI                                                               | This feature was introduced for Cisco uBR7200 series routers.         |
| 12.1(2)EC                                                               | The <b>cable telco-return registration-ip</b> command was introduced. |
| 12.1(5)EC                                                               | Support was added for the Cisco uBR7111 and Cisco uBR7114 routers.    |
| Supported Platforms                                                     |                                                                       |
| Cisco uBR7100 series, Cisco uBR7200 series universal broadband routers. |                                                                       |

### Finding Support Information for Platforms and Cisco IOS Software Images

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

## Contents

- [Prerequisites for Telco Return, page 430](#)
- [Restrictions for Telco Return, page 430](#)
- [Information about Telco Return, page 431](#)
- [How to Configure the Telco Return Feature, page 434](#)
- [Monitoring Telco Return Operations, page 439](#)
- [Configuration Examples, page 440](#)
- [Additional References, page 441](#)



---

#### Corporate Headquarters:

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

Copyright © 2003 Cisco Systems, Inc. All rights reserved.

## Prerequisites for Telco Return

The Telco Return feature has the following prerequisites and requirements:

- The Cisco CMTS router must be running a Cisco IOS Release 12.1 EC software image that contains a “t” in the filename.
- The Cisco CMTS must be using a DOCSIS-compliant cable interface line card. The Cisco uBR-MC11C cable interface line card (which has only one upstream port) is sufficient for cable plants that will never be upgraded from one-way-only operation. If, however, you plan to upgrade your plant to two-way operation, consider installing other cable interface cards, such as the Cisco uBR-MC16C or Cisco uBR-MC28C card, so as to simplify the conversion process when two-way operation is implemented.
- The downstream cable plant must meet DOCSIS specifications.
- The headend is wired for narrowcast downstream data transmission.
- You have assigned downstream frequencies.
- All equipment needed to support upstream traffic over the PSTN, as well as to monitor telco return service features, is installed. Key components include:
  - Dial-up access server (for example, the Cisco AS5300 or Cisco AS5800)
  - RADIUS dial security server
- Upstream data from a PC through the CM to the Internet is carried over a dial-up connection. This dial-up connection can include a log or security server.
- All third-party, telco return cable modems are DOCSIS-compliant and configured for telco return.
- Dynamic Host Configuration Protocol (DHCP) and DOCSIS configuration files have been created and pushed to appropriate servers so that each cable modem, when initialized, can transmit a DHCP request, receive an IP address, obtain TCP/IP and Time-of-Day (ToD) server addresses, and download a DOCSIS configuration file.
- The DOCSIS configuration files being used for telco return cable modems should include the relevant telco return Type/Length/Value (TLV) fields.
- The customer premises equipment (CPE) (telco return cable modem or PCs) should meet the requirements for your network and server offerings.

## Restrictions for Telco Return

- DOCSIS Baseline Privacy Interface (BPI) encryption is not supported over the telco return path.
- EuroDOCSIS cable interfaces (Cisco uBR-MC16E cable interface line card and Cisco uBR7111E/Cisco uBR7114E routers) do not support Telco Return operations.
- Cisco IOS Release 12.2 BC does not support Telco Return operations.
- Some vendors’ telco return cable modems cannot receive traffic over the same downstream channel as cable modems operating on a two-way data system. In these instances, segment your cable plant to allow more than one downstream channel.
- A DOCSIS ping (which is sent using the **ping docsis** command) cannot be used with telco return modems. An IP ping, however, can still be used.
- The **show cable flap-list** command does not display telco return cable modems.
- The **clear cable modem reset** command has no affect on telco return cable modems.

# Information about Telco Return

This section contains the following information that describes the Telco Return feature:

- [Feature Overview, page 431](#)
- [DOCSIS Cable Plants, page 431](#)
- [Telco Return Operation, page 432](#)
- [Benefits, page 434](#)

## Feature Overview

The DOCSIS specifications included optional support for Telco Return operations, which allows service providers to offer Internet data connectivity to cable customers who are still on cable plants that do not yet support two-way operations. Service providers can immediately provide data connectivity to their customers as they incrementally upgrade their cable plants to support two-way connections.

In a Telco Return configuration, the subscriber uses a telco return cable modem that receives downstream traffic over the cable network, but transmits the upstream traffic over a dial-up connection that is made using the local Public Switched Telephone Network (PSTN). The telco return cable modem makes the dial-up connection using a standard telephone modem, which can be either internal or external, depending on the type and model of the cable modem being used.

Telco Return operations is made possible by the fact that most Internet sessions are asymmetrical, with approximately 80 to 90% of the total traffic being transmitted in the downstream direction from the headend to the cable modem. The upstream transmits a much smaller volume of traffic, so Telco Return customers can still have broadband-quality Internet access.

**Note**

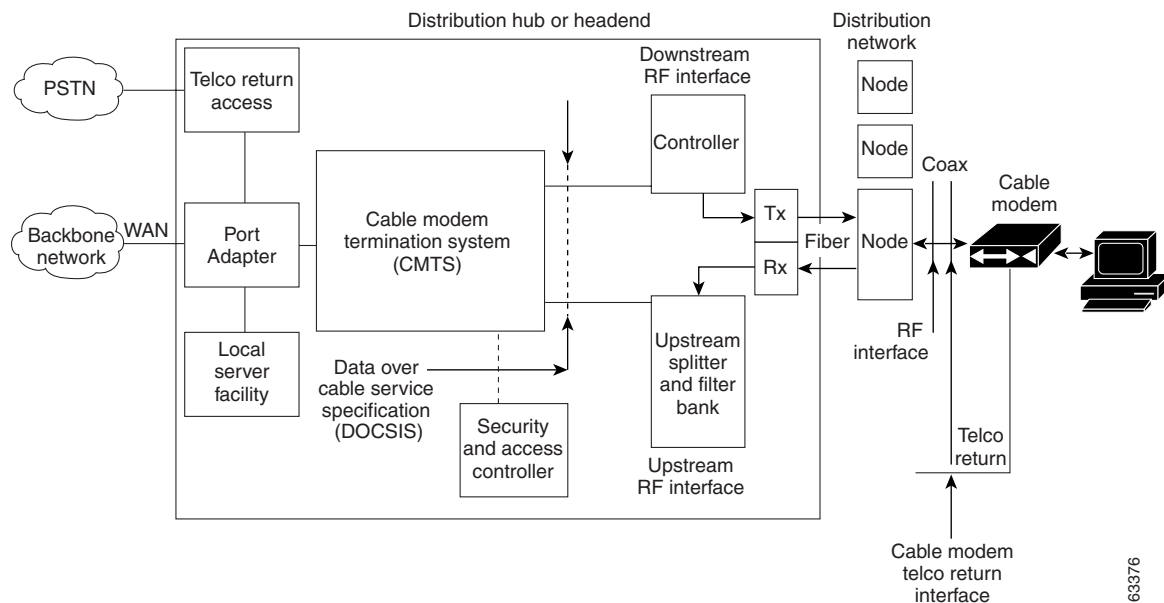
---

To support telco return operations, the subscriber must be using a DOCSIS-compliant telco return cable modem

---

## DOCSIS Cable Plants

DOCSIS-compliant cable plants can support both two-way and telco return connections over the same cable network. [Figure 8](#) illustrates a typical DOCSIS cable network that supports both two-way and telco return cable modems.

**Figure 8** DOCSIS Two-Way and Telco Return Architecture

Typically, the headend uses high-speed WAN links, such as a fiber backbone, to connect to the Internet backbone network. The Cable Modem Termination System (CMTS) at the headend is responsible for routing traffic between the backbone network and cable network.

Two-way and telco return operations on the downstream use the same facilities and servers at the headend. In both cases, the CMTS routes traffic over the cable interface to the appropriate cable modems.

For upstream traffic, the two-way cable modems transmit over the same coaxial cable network that is used for the downstream (although using different frequencies). Telco Return cable modems, however, use a dial-up modem connection to connect to the PSTN, which routes the upstream traffic to a Remote Authentication Dial In User Service (RADIUS) server at the headend. This server in turn forwards the traffic to the appropriate destination, either on the Internet or cable network.

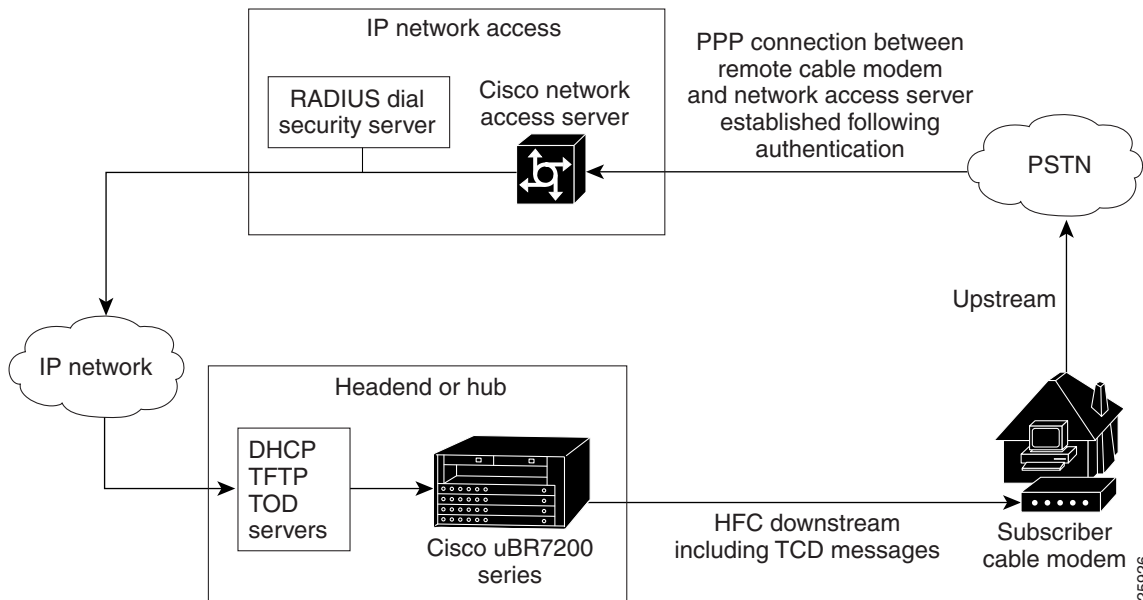
**Note**

Some brands of telco return cable modems cannot receive traffic over the same downstream channel as cable modems operating on a two-way data system. To accommodate both two-way and telco return operation, segment your cable plant so that it uses multiple downstream channels, with at least one downstream channel dedicated for telco return cable modems.

## Telco Return Operation

To support Telco Return operations, the Cisco CMTS must interoperate with both the cable network, and a RADIUS authentication system that is connected to the local PSTN. [Figure 9](#) illustrates a typical telco return configuration.



**Figure 9** Typical Telco Return Network

To coordinate the telco return traffic between the cable and PSTN/RADIUS networks, the Cisco CMTS transmits Telephony Channel Descriptor (TCD) messages along with the other downstream traffic. The TCD messages contain the routing and other information that the telco return cable modem needs to access the headend through the PSTN.

In particular, the TCD messages contain at least one (and up to five) Service Provider Descriptors (SPD). Each SPD contains dialing and authentication information that the telco return cable modem should use when it creates a dial-up Point-to-Point Protocol (PPP) connection with the network access server (NAS) that provides the upstream access to the Internet and headend networks.

At minimum, the SPD contains the following three elements that are critical in creating the dial-up upstream connection:

- At least one, and up to three, dial-up telephone numbers for the telco return cable modem to use when using the PSTN to connect to the headend's network access server.
- Username to be used for the PPP authentication procedure.
- Password to be used for the PPP authentication procedure.

When the telco return cable modem establishes the dial-up connection, it sends the username and password to the RADIUS server for network authentication. If access is granted, the network server creates the PPP session that will be used for upstream traffic.

The telco return cable modem maintains the dial-up connection as long as necessary. If the connection times out because of inactivity or because of noise problems on the PSTN, the telco return cable modem uses the information from the SPD to automatically redial the appropriate number and reestablish the dial-up connection.

**Note**

Some telco return cable modems require that the user manually dial the telephone number to establish the dial-up connection.

## Benefits

- Allows cable companies to offer Internet access services to their subscribers without first upgrading their plant to support two-way operations.
- Allows service providers to support their cable subscribers without replacing existing hardware.
- Service providers can begin providing cable access using low-density cable interface cards because upstream ports are not required. As the cable plant is upgraded to two-way operations, the cable interface line cards can be upgraded as needed.

## How to Configure the Telco Return Feature

To enable and configure Telco Return operations on a cable interface, use the following procedures:

- [Enabling Telco Return, page 434](#)
- [Configuring the Service Provider Descriptor Attributes, page 435](#)
- [Configuring the Registration IP Address \(optional\), page 438](#)

## Enabling Telco Return

To enable telco return on the Cisco CMTS, perform the following steps beginning in EXEC mode:

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface cable *x/y***
4. **cable telco-return enable**
5. **cable telco-return interval *seconds***
6. **exit**
7. **exit**

### DETAILED STEPS

|        | Command or Action                                                                                 | Purpose                                                        |
|--------|---------------------------------------------------------------------------------------------------|----------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable<br>Router#                                 | Enables privileged EXEC mode. Enter your password if prompted. |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal<br>Router(config)# | Enters global configuration mode.                              |

|        | Command or Action                                                                                                                                   | Purpose                                                                                                                                                                                                                                                |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 3 | <b>interface cable <i>x/y</i></b><br><br><b>Example:</b><br>Router(config)# interface cable 4/0<br>Router(config-if)#                               | Enters cable interface configuration mode for the specified cable interface.                                                                                                                                                                           |
| Step 4 | <b>cable telco-return enable</b><br><br><b>Example:</b><br>Router(config-if)# cable telco-return enable<br>Router(config-if)#                       | Enables telco return operations on this cable interface.                                                                                                                                                                                               |
| Step 5 | <b>cable telco-return interval <i>seconds</i></b><br><br><b>Example:</b><br>Router(config-if)# cable telco-return interval 10<br>Router(config-if)# | (Optional) Sets the interval, in seconds, for sending Telephony Channel Descriptor (TCD) and Termination System Information (TSI) messages to the downstream cable modems. The valid range for <i>seconds</i> is 2 to 60 seconds, with a default of 2. |
| Step 6 | <b>exit</b><br><br><b>Example:</b><br>Router(config-if)# exit<br>Router(config)#                                                                    | Exits interface configuration mode.                                                                                                                                                                                                                    |
| Step 7 | <b>exit</b><br><br><b>Example:</b><br>Router(config)# exit<br>Router#                                                                               | Exits global configuration mode.                                                                                                                                                                                                                       |

## Configuring the Service Provider Descriptor Attributes

To configure the telephony attributes for a Service Provider Descriptor (SPD), perform the following steps, beginning in EXEC mode. Up to five SPDs can be defined on each cable interface (but only one SPD per cable interface is active at any one time).

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface cable *x/y***
4. **cable telco-return spd *spd-number* phonenum *dial-string***
5. **cable telco-return spd *spd-number* username *login-string***
6. **cable telco-return spd *spd-number* password *password-string***
7. **cable telco-return spd *spd-number* radius realm *string***
8. **cable telco-return spd *spd-number* ppp-authenticate [both | chap | pap]**
9. **cable telco-return spd *spd-number* dhcp-authenticate**

10. **cable telco-return spd** *spd-number* **dhcp-server** *ip-address*
11. **cable telco-return spd** *spd-number* **dial-timer** *seconds*
12. **cable telco-return spd** *spd-number* **threshold** *threshold*
13. **cable telco-return spd** *spd-number* **service-provider** *string*
14. **cable telco-return spd** *spd-number* **factory-default**
15. **cable telco-return spd** *spd-number* **manual-dial**
16. **exit**
17. **exit**

## DETAILED STEPS

|                                                                                                       | Command or Action                                                                                                                                                                                      | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1                                                                                                | <b>enable</b><br><br><b>Example:</b><br>Router> enable<br>Router#                                                                                                                                      | Enables privileged EXEC mode. Enter your password if prompted.                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Step 2                                                                                                | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal<br>Router(config)#                                                                                                      | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Step 3                                                                                                | <b>interface cable</b> <i>x/y</i><br><br><b>Example:</b><br>Router(config)# interface cable 4/0<br>Router(config-if)#                                                                                  | Enters cable interface configuration mode for the specified cable interface.                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Step 4                                                                                                | <b>cable telco-return spd</b> <i>spd-number</i> <b>phonenum</b> <i>dial-string</i><br><br><b>Example:</b><br>Router(config-if)# cable telco-return spd 2<br>phonenum 15105551212<br>Router(config-if)# | Specifies the telephone number that the telco return CM uses when connecting to the headend's network access server. <ul style="list-style-type: none"> <li><i>spd-number</i> = ID for this SPD. The valid range is 1 to 5, with no default.</li> <li><i>dial-string</i> = Actual telephone number to be dialed. Enter only digits, without any spaces, hyphens, or other special characters.</li> </ul> <b>Note</b> Optionally repeat this command to specify a maximum of three phone numbers. |
| <b>Note</b> Use the same <i>spd-number</i> value for all of the following commands in this procedure. |                                                                                                                                                                                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Step 5                                                                                                | <b>cable telco-return spd</b> <i>spd-number</i> <b>username</b> <i>login-string</i><br><br><b>Example:</b><br>Router(config-if)# cable telco-return spd 2<br>username joeuser123<br>Router(config-if)# | Specifies the user name that the cable modem uses during initialization to establish the Point-to-Point Protocol (PPP) connection.                                                                                                                                                                                                                                                                                                                                                               |

|         | Command or Action                                                                                                                                                                                                              | Purpose                                                                                                                                                                                                                                                                                                                                                   |
|---------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 6  | <b>cable telco-return spd <i>spd-number</i> password <i>password-string</i></b><br><br><b>Example:</b><br>Router(config-if)# cable telco-return spd 2<br>password 9JwoKd7<br>Router(config-if)#                                | Specifies the password that the cable modem uses during initialization to establish the PPP connection.                                                                                                                                                                                                                                                   |
| Step 7  | <b>cable telco-return spd <i>spd-number</i> ppp-authenticate [<i>chap</i>   <i>pap</i>   <i>both</i>]</b><br><br><b>Example:</b><br>Router(config-if)# cable telco-return spd 2<br>ppp-authenticate chap<br>Router(config-if)# | (Optional) Selects the authentication procedure that the cable modem should use to establish the PPP connection: <ul style="list-style-type: none"> <li>• <b>chap</b> = Challenge Handshake Authentication Protocol (CHAP)</li> <li>• <b>pap</b> = Password Authentication Protocol (PAP)</li> <li>• <b>both</b> = (default) Both CHAP and PAP</li> </ul> |
| Step 8  | <b>cable telco-return spd <i>spd-number</i> radius realm <i>string</i></b><br><br><b>Example:</b><br>Router(config-if)# cable telco-return spd 2<br>radius-realm cisco<br>Router(config-if)#                                   | Specifies the RADIUS Realm string that the cable modem should use to construct a domain name to be used with the login name during the PPP authentication procedure.                                                                                                                                                                                      |
| Step 9  | <b>cable telco-return spd <i>spd-number</i> dhcp-authenticate</b><br><br><b>Example:</b><br>Router(config-if)# cable telco-return spd 2<br>dhcp-authenticate<br>Router(config-if)#                                             | (Optional) Requires that the cable modem use the Dynamic Host Configuration Protocol (DHCP) server that is specified with the <b>cable telco-return spd dhcp-server</b> command. The default is for the cable modem to use any available DHCP server.                                                                                                     |
| Step 10 | <b>cable telco-return spd <i>spd-number</i> dhcp-server <i>ip-address</i></b><br><br><b>Example:</b><br>Router(config-if)# cable telco-return spd 2<br>dhcp-server 192.168.100.213<br>Router(config-if)#                       | (Optional) Specifies the IP address of the DHCP server that the cable modem should use during its authentication and initialization process. The default is for the cable modem to use any available DHCP server.                                                                                                                                         |
| Step 11 | <b>cable telco-return spd <i>spd-number</i> dial-timer <i>seconds</i></b><br><br><b>Example:</b><br>Router(config-if)# cable telco-return spd 2<br>dial-timer 86400<br>Router(config-if)#                                      | (Optional) Sets the number of seconds that the telephone connection is idle before the cable modem disconnects the call. The valid range is 0 through 4,294,967,295 seconds. The default is 0, which indicates that the dial-timer is not used and that inactive calls are not disconnected.                                                              |
| Step 12 | <b>cable telco-return spd <i>spd-number</i> threshold <i>threshold</i></b><br><br><b>Example:</b><br>Router(config-if)# cable telco-return spd 2<br>threshold 3<br>Router(config-if)#                                          | (Optional) Specifies the number of times that the cable modem attempts to dial the numbers specified by the <b>cable telco-return spd phonenum</b> command before declaring a connection failure. (The cable modem allows the remote end of the connection to ring 10 times before handing up.) The valid range is 1 through 255, with a default of 1.    |

|         | Command or Action                                                                                                                                                                                                          | Purpose                                                                                                                                                                                                                                                                                   |
|---------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 13 | <b>cable telco-return spd</b> <i>spd-number</i><br><b>service-provider</b> <i>string</i><br><br><b>Example:</b><br>Router(config-if)# cable telco-return spd 2<br>service-provider CableProviderName<br>Router(config-if)# | (Optional) Specifies that the cable modem should include the specified <i>string</i> in the Telephony Channel Descriptor (TCD) messages as the service provider's name.                                                                                                                   |
| Step 14 | <b>cable telco-return spd</b> <i>spd-number</i><br><b>factory-default</b><br><br><b>Example:</b><br>Router(config-if)# cable telco-return spd 2<br>factory-default<br>Router(config-if)#                                   | (Optional) Indicates that the cable modem should use this SPD during the initialization process. The default is for the SPD not to be used during initialization.<br><br><b>Note</b> At least one and only one SPD must be defined as the <b>factory-default</b> on each cable interface. |
| Step 15 | <b>cable telco-return spd</b> <i>spd-number</i> <b>manual-dial</b><br><br><b>Example:</b><br>Router(config-if)# cable telco-return spd 2<br>manual-dial<br>Router(config-if)#                                              | (Optional) Allows the cable modem to operate in manual dial mode.                                                                                                                                                                                                                         |
|         | <b>Note</b> Repeat <a href="#">Step 4</a> through <a href="#">Step 15</a> for each SPD to be configured (up to a maximum of 5 per cable interface).                                                                        |                                                                                                                                                                                                                                                                                           |
| Step 16 | <b>exit</b><br><br><b>Example:</b><br>Router(config-if)# exit<br>Router(config)#                                                                                                                                           | Exits interface configuration mode.                                                                                                                                                                                                                                                       |
| Step 17 | <b>exit</b><br><br><b>Example:</b><br>Router(config)# exit<br>Router#                                                                                                                                                      | Exits global configuration mode.                                                                                                                                                                                                                                                          |

## Configuring the Registration IP Address (optional)

To specify an alternate registration IP address to be sent in Termination System Information (TSI) message, use the following procedure, beginning in EXEC mode. By default, the Cisco CMTS uses the IP address for the downstream cable interface as the registration address. Use this procedure to specify a different registration address.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface cable** *x/y*
4. **cable telco-return registration-ip** *ip-address*
5. **exit**

## 6. exit

## DETAILED STEPS

|        | Command or Action                                                                                                                                                          | Purpose                                                                                                                                                                                                                                    |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable<br>Router#                                                                                                          | Enables privileged EXEC mode. Enter your password if prompted.                                                                                                                                                                             |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal<br>Router(config)#                                                                          | Enters global configuration mode.                                                                                                                                                                                                          |
| Step 3 | <b>interface cable x/y</b><br><br><b>Example:</b><br>Router(config)# interface cable 4/0<br>Router(config-if)#                                                             | Enters cable interface configuration mode for the specified cable interface.                                                                                                                                                               |
| Step 4 | <b>cable telco-return registration-ip ip-address</b><br><br><b>Example:</b><br>Router(config-if)# cable telco-return<br>registration-ip 10.10.10.119<br>Router(config-if)# | Specifies an alternate registration IP address that the cable modem should use in its Termination System Information (TSI) messages. By default, the cable modem uses the IP address for the downstream cable interface on the Cisco CMTS. |
| Step 5 | <b>exit</b><br><br><b>Example:</b><br>Router(config-if)# exit<br>Router(config)#                                                                                           | Exits interface configuration mode.                                                                                                                                                                                                        |
| Step 6 | <b>exit</b><br><br><b>Example:</b><br>Router(config)# exit<br>Router#                                                                                                      | Exits global configuration mode.                                                                                                                                                                                                           |

## Monitoring Telco Return Operations

To display the telco return cable modems that are currently online, use the **show cable modem** command. For example:

Router# **show cable modem**

| Interface   | Prim<br>Sid | Online<br>State | Timing<br>Offset | Rec<br>Power | QoS | CPE | IP address | MAC address    |
|-------------|-------------|-----------------|------------------|--------------|-----|-----|------------|----------------|
| Cable4/0/U0 | 2           | online          | 2848             | -0.50        | 5   | 1   | 10.2.0.3   | 0010.7b6b.53d5 |
| Cable4/0/T  | 3           | online          | 2853             | 0.25         | 2   | 1   | 10.2.0.101 | 0020.4001.4af6 |
| Cable4/0/U0 | 4           | online          | 2852             | -0.75        | 5   | 1   | 10.2.0.6   | 0010.7b6b.7255 |

```

Cable4/0/U0 5 online 2850 0.25 5 1 10.2.0.7 0010.7b6b.5669
Cable4/0/U0 6 online 2851 0.00 2 1 10.2.0.4 0010.7b6b.53c9
Cable4/0/T 7 online 2849 0.50 2 0 10.2.0.102 0020.4001.4b32

```

Router#

The **show cable modem** command identifies telco return cable modems by displaying a “T” instead of an upstream port.

## Configuration Examples

- [Typical Telco Return Example, page 440](#)
- [Minimal Telco Return Example, page 441](#)
- [Minimal RADIUS Configuration, page 441](#)

### Typical Telco Return Example

The following excerpt from a configuration file shows a typical sample configuration that enables Telco Return operations on a cable interface:

```

!
interface cable 6/0
 ip address 172.16.1.1 secondary
 ip address 10.1.1.1
 no ip directed-broadcast
 ip helper-address 192.168.1.1
 no keepalive
 cable insertion-interval 500
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream frequency 687000000
 cable upstream 0 frequency 13008000
 no cable upstream 0 shutdown
 cable telco-return enable
 cable telco-return spd 1 factory-default
 cable telco-return spd 1 phonenum 8005551212
 cable telco-return spd 1 phonenum 4085551212
 cable telco-return spd 1 phonenum 6505551212
 cable telco-return spd 1 service-provider norcal
 cable telco-return spd 1 dhcp-server 172.31.172.172
 cable telco-return spd 1 username joe
 cable telco-return spd 1 password testing
 cable telco-return spd 1 dhcp-authenticate
 cable telco-return spd 1 threshold 5
 cable telco-return spd 1 ppp-authenticate both
 cable telco-return spd 1 manual-dial
 cable telco-return spd 1 dial-timer 7200
 cable telco-return registration-ip 172.16.1.1

```



## Minimal Telco Return Example

The following excerpt from a configuration file shows the minimal configuration that is needed to enable Telco Return operations on a cable interface:

```
cable telco-return enable
cable telco-return spd 1 factory-default
cable telco-return spd 1 dhcp-authenticate
cable telco-return spd 1 dhcp-server 24.1.1.84
cable telco-return spd 1 ppp-authenticate chap
cable telco-return spd 1 phonenum 918005555555
cable telco-return spd 1 phonenum 18005555555
cable telco-return spd 1 username test
cable telco-return spd 1 password test
```

## Minimal RADIUS Configuration

The following excerpt from a configuration file shows the minimal configuration that is needed to enable RADIUS support on the Cisco CMTS to allow the required authentication, authorization, and accounting (AAA) support:

```
aaa new-model
aaa authentication login default radius enable
aaa authentication login vty line
aaa accounting update newinfo
aaa accounting exec default start-stop radius
aaa accounting commands 15 default start-stop radius
aaa accounting network default start-stop radius
aaa accounting system default start-stop radius
```

## Additional References

For additional information related to the Telco Return feature, refer to the following references:

### Related Documents

| Related Topic                            | Document Title                                                                                                                                                                                                                                                                     |
|------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CMTS Command Reference                   | <i>Cisco Broadband Cable Command Reference Guide</i> , at the following URL:<br><br><a href="http://www.cisco.com/univercd/cc/td/doc/product/cable/bbccmref/index.htm">http://www.cisco.com/univercd/cc/td/doc/product/cable/bbccmref/index.htm</a>                                |
| Cisco IOS Release 12.2 Command Reference | Cisco IOS Release 12.2 Configuration Guides and Command References, at the following URL:<br><br><a href="http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/index.htm">http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/index.htm</a> |

| Related Topic                                                 | Document Title                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cisco IOS Release 12.1 Multiservice Applications Information  | <p><i>Cisco IOS Multiservice Applications Configuration Guide</i>, Release 12.1, at the following URL:</p> <p><a href="http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/multi_c/index.htm">http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/multi_c/index.htm</a></p> <p><i>Cisco IOS Multiservice Applications Command Reference</i>, Release 12.1, at the following URL:</p> <p><a href="http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/multi_r/index.htm">http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/multi_r/index.htm</a></p> |
| AAA and RADIUS Configuration                                  | <p>For information on configuring the AAA and RADIUS servers, see the <i>Authentication, Authorization, and Accounting (AAA)</i> chapter in the Cisco IOS Security Configuration Guide, Release 12.2 at the following URL:</p> <p><a href="http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/index.htm">http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/index.htm</a></p>                                                                                                                                                                                             |
| Cisco uBR7100 Series Universal Broadband Router Documentation | <p><i>Cisco uBR7100 Series Universal Broadband Router Hardware Installation Guide</i>, at the following URL:</p> <p><a href="http://www.cisco.com/univercd/cc/td/doc/product/cable/ubr7100/hig7100/index.htm">http://www.cisco.com/univercd/cc/td/doc/product/cable/ubr7100/hig7100/index.htm</a></p> <p><i>Cisco uBR7100 Series Universal Broadband Router Software Configuration Guide</i>, at the following URL:</p> <p><a href="http://www.cisco.com/univercd/cc/td/doc/product/cable/ubr7100/scg7100/index.htm">http://www.cisco.com/univercd/cc/td/doc/product/cable/ubr7100/scg7100/index.htm</a></p>                          |
| Cisco uBR7200 Series Universal Broadband Router Documentation | <p><i>Cisco uBR7200 Series Universal Broadband Router Hardware Installation Guide</i>, at the following URL:</p> <p><a href="http://www.cisco.com/univercd/cc/td/doc/product/cable/cab_rout/cr72hig/index.htm">http://www.cisco.com/univercd/cc/td/doc/product/cable/cab_rout/cr72hig/index.htm</a></p> <p><i>Cisco uBR7200 Series Universal Broadband Router Software Configuration Guide</i>, at the following URL:</p> <p><a href="http://www.cisco.com/univercd/cc/td/doc/product/cable/cab_rout/cr72scg/index.htm">http://www.cisco.com/univercd/cc/td/doc/product/cable/cab_rout/cr72scg/index.htm</a></p>                      |

## Standards

| Standards <sup>1</sup>                                           | Title                                                                                                                                                                                   |
|------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">ANSI/SCTE 22-1 2002</a> (formerly SP-RFI-C01-011119) | Data-Over-Cable Service Interface Specification DOCSIS 1.0 Radio Frequency Interface (RFI) ( <a href="http://www.cablemodem.com">http://www.cablemodem.com</a> )                        |
| <a href="#">SP-CMTRI-I01-970804</a>                              | Data-Over-Cable Service Interface Specification Cable Modem Telephony Return Interface Specification, version 1.0 ( <a href="http://www.cablemodem.com">http://www.cablemodem.com</a> ) |

1. Not all supported standards are listed.

## MIBs

| MIBs <sup>1</sup>                                      | MIBs Link                                                                                                                                                                                                              |
|--------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No new or modified MIBs are supported by this feature. | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

1. Not all supported MIBs are listed.

## RFCs

| Description | Link                                                |
|-------------|-----------------------------------------------------|
| RFC 2865    | Remote Authentication Dial In User Service (RADIUS) |
| RFC 2866    | RADIUS Accounting                                   |

## Technical Assistance

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

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, TeleRouter, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0502R)

Copyright © 2003 Cisco Systems, Inc. All rights reserved.





## Time-of-Day Server for the Cisco CMTS

The Time-of-Day Server feature enables the Cisco Cable Modem Termination System (CMTS) to provide a time-of-day (ToD) server to the cable modems and other customer premises equipment (CPE) devices connected to its cable interfaces. The cable modem uses the ToD server to get the current date and time to accurately time-stamp its Simple Network Management Protocol (SNMP) messages and error log entries.

### Feature Specifications for the Time-of-Day Server

#### Feature History

| Release            | Modification                                                                          |
|--------------------|---------------------------------------------------------------------------------------|
| Release 12.0(4)XI  | This feature was introduced for the Cisco uBR7200 series routers.                     |
| Release 12.1(5)EC  | This feature was supported on the Cisco uBR7100 series routers.                       |
| Release 12.2(4)BC1 | This feature was supported on the Release 12.2 BC train for all Cisco CMTS platforms. |

#### Supported Platforms

Cisco uBR7100 series, Cisco uBR7200 series, Cisco uBR10012 universal broadband routers.

### Finding Support Information for Platforms and Cisco IOS Software Images

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



#### Note

This document describes only the ToD server on the Cisco CMTS. For information about using the ToD server along with the Dynamic Host Configuration Protocol (DHCP) and Trivial File Transfer Protocol (TFTP) services that are also available on the Cisco CMTS, see the *DHCP, ToD, and TFTP Services for the Cisco CMTS* chapter in the Cisco CMTS Feature Guide, at the following URL:

[http://www.cisco.com/univercd/cc/td/doc/product/cable/cab\\_rout/cmtsfg/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/cable/cab_rout/cmtsfg/index.htm)

# Contents

- [Prerequisites for the Time-of-Day Server, page 446](#)
- [Restrictions for the Time-of-Day Server, page 446](#)
- [Information About the Time-of-Day Server, page 446](#)
- [How to Configure the Time-of-Day Server on the Cisco CMTS, page 447](#)
- [Configuration Examples for the Time-of-Day Server, page 449](#)
- [Additional References, page 450](#)

## Prerequisites for the Time-of-Day Server

- The Cisco CMTS must be running Cisco IOS Release 12.0(4)XI or later release. Cisco recommends using the latest Cisco IOS Release 12.2 BC software release.
- To supply an accurate clock, the system clock on the Cisco CMTS should be configured for the correct time, either by using the **set clock** command or by configuring the Cisco CMTS to act as a Network Time Protocol (NTP) or Simple Network Time Protocol (SNTP) client.
- To be able to use the Cisco CMTS as the ToD server, either alone or along with other, external ToD servers, you must configure the DHCP server to provide the IP address Cisco CMTS as one of the valid ToD servers (DHCP option 4) for cable modems.

## Restrictions for the Time-of-Day Server

- To conform to the Data-over-Cable Service Interface Specifications (DOCSIS) specifications, the time-of-day server is restricted to using User Datagram Protocol (UDP) packets.

## Information About the Time-of-Day Server

The DOCSIS 1.0 and 1.1 specifications require that a DOCSIS cable modem or other CPE device must specify the following time-related fields in the Dynamic Host Configuration Protocol (DHCP) request it sends during its initial power-on provisioning:

- Time Offset (option 2)—Specifies the time zone for the cable modem or CPE device, as the number of seconds that the device's time stamp is offset from Greenwich Mean Time (GMT).
- Time Server Option (option 4)—Specifies one or more IP addresses for a time-of-day server.

During initial provisioning, a DOCSIS cable modem or CPE device attempts to contact the time-of-day server. If successful, the cable device updates its onboard clock with the time offset and timestamp received from the time-of-day server. If a time-of-day server cannot be reached or if it does not respond, the cable device eventually times out and continues on with the initialization process.

**Note**

Initial versions of the DOCSIS 1.0 specification specified that the cable device must obtain a valid response from a ToD server before continuing with the initialization process. This requirement was removed in later versions of the DOCSIS 1.0 specification and in the DOCSIS 1.1 specification. Older cable devices that are compliant with the initial DOCSIS 1.0 specification, however, might require a time-of-day server before being able to come online.

By providing a time-of-day server, the Cisco CMTS eliminates the requirement for a separate, external time-of-day server. Using the time-of-day server also ensures that all devices connected to the cable interfaces are using the same time-stamp references, making it easier to troubleshoot system problems when analyzing the debugging output and error logs generated by the cable modems, CPE devices, CMTS, and other servers.

**Note**

To be able to use the Cisco CMTS as the ToD server, either alone or with other, external servers, you must configure the DHCP server to provide the IP address Cisco CMTS as one of the valid ToD servers (DHCP option 4) for cable modems.

Although a DOCSIS cable modem or cable CPE device does not have to contact a time-of-day server to complete its provisioning sequence, the DOCSIS specification requires that the device attempt to contact the time-of-day server at least once, and no more than three times, before timing out. When the Cisco CMTS provides a time-of-day server, it enables cable devices to register more quickly because they do not have to wait for the time-of-day timeout period before continuing.

In addition, although the DOCSIS specifications do not require that a cable modem successfully obtain a response from a ToD server before coming online, not obtaining a timestamp could prevent the cable modem from coming online in the following situations:

- If DOCSIS configuration files are being timestamped, to prevent cable modems from caching the files and replaying them, the clocks on the cable modem and CMTS must be synchronized. Otherwise, the cable modem cannot determine whether a DOCSIS configuration file has the proper timestamp.
- If cable modems register using Baseline Privacy Interface Plus (BPI+) authentication and encryption, the clocks on the cable modem and CMTS must be synchronized. This is because BPI+ authorization requires that the CMTS and cable modem verify the timestamps on the digital certificates being used for authentication. If the timestamps on the CMTS and cable modem are not synchronized, the cable modem cannot come online using BPI+ encryption.

## How to Configure the Time-of-Day Server on the Cisco CMTS

See the following sections for information on enabling and disabling the time-of-day server on the Cisco CMTS server.

- [Enabling the Time-of-Day Server, page 447](#)
- [Disabling the Time-of-Day Server, page 448](#)

### Enabling the Time-of-Day Server

To enable the time-of-day server on the Cisco CMTS, use the following procedure beginning in user EXEC mode:

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **service udp-small-servers max-servers no-limit**
4. **cable time-server**
5. **exit**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                    | Purpose                                                                                                                                                                                                                                                                                                                                                                       |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable<br>Router#                                                                                                    | Enables privileged EXEC mode. Enter your password if prompted.                                                                                                                                                                                                                                                                                                                |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal<br>Router(config)#                                                                    | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                             |
| Step 3 | <b>service udp-small-servers max-servers no-limit</b><br><br><b>Example:</b><br>Router(config)# service udp-small-servers<br>max-servers no-limit<br>Router(config)# | Enables use of minor servers that use the UDP protocol (such as ToD, echo, chargen, and discard). The <b>max-servers no-limit</b> option allows a large number of cable modems to obtain the ToD server at one time, in the event that a cable or power failure forces many cable modems offline. When the problem has been resolved, the cable modems can quickly reconnect. |
| Step 4 | <b>cable time-server</b><br><br><b>Example:</b><br>Router(config)# cable time-server<br>Router(config)#                                                              | Enables the time-of-day server on the Cisco CMTS.                                                                                                                                                                                                                                                                                                                             |
| Step 5 | <b>exit</b><br><br><b>Example:</b><br>Router(config)# exit<br>Router#                                                                                                | Exits global configuration mode.                                                                                                                                                                                                                                                                                                                                              |

## Disabling the Time-of-Day Server

To disable the time-of-day server on the Cisco CMTS, use the following procedure beginning in user EXEC mode:

## SUMMARY STEPS

1. **enable**



2. **configure terminal**
3. **no cable time-server**
4. **no service udp-small-servers**
5. **exit**

## DETAILED STEPS

|        | Command or Action                                                                                                             | Purpose                                                        |
|--------|-------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable<br>Router#                                                             | Enables privileged EXEC mode. Enter your password if prompted. |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal<br>Router(config)#                             | Enters global configuration mode.                              |
| Step 3 | <b>no cable time-server</b><br><br><b>Example:</b><br>Router(config)# no cable time-server<br>Router(config)#                 | Disables the time-of-day server on the Cisco CMTS.             |
| Step 4 | <b>no service udp-small-servers</b><br><br><b>Example:</b><br>Router(config)# no service udp-small-servers<br>Router(config)# | (Optional) Disables the use of all minor UDP servers.          |
| Step 5 | <b>exit</b><br><br><b>Example:</b><br>Router(config)# exit<br>Router#                                                         | Exits global configuration mode.                               |

## Configuration Examples for the Time-of-Day Server

The following excerpt from a configuration file shows a typical configuration that enables the time-of-day server on the Cisco CMTS:

- [Time-of-Day Server Configuration, page 449](#)

## Time-of-Day Server Configuration

```
!
service udp small-servers max-servers no-limit
!
```

```
cable time-server
```

## Additional References

For additional information related to the Time-of-Day Server on the Cisco CMTS, refer to the following references:

## Related Documents

| Related Topic                                   | Document Title                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DHCP, ToD, and TFTP Services for the Cisco CMTS | For information about using the ToD server along with the Dynamic Host Configuration Protocol (DHCP) and Trivial File Transfer Protocol (TFTP) services that are also available on the Cisco CMTS, see the <i>DHCP, ToD, and TFTP Services for the Cisco CMTS</i> chapter in the Cisco CMTS Feature Guide, at the following URL:<br><br><a href="http://www.cisco.com/univercd/cc/td/doc/product/cable/cab_rout/cmtsfg/index.htm">http://www.cisco.com/univercd/cc/td/doc/product/cable/cab_rout/cmtsfg/index.htm</a>                                      |
| NTP or SNTP Configuration                       | To configure the Cisco CMTS to use Network Time Protocol (NTP) or Simple Network Time Protocol (SNTP) to set its system clock, see the “Performing Basic System Management” chapter in the “System Management” section of the <i>Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2</i> , at the following URL:<br><br><a href="http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/ffun_c/fcftp3/fcf012.htm">http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/ffun_c/fcftp3/fcf012.htm</a> |
| Cable Command Reference Guide                   | For syntax and usage information on the cable-specific commands used in this chapter, see the “Cisco Cable Modem Termination System Commands” chapter of the <i>Cisco Broadband Cable Command Reference Guide</i> at the following URL:<br><br><a href="http://www.cisco.com/univercd/cc/td/doc/product/cable/bbcmref/bcmmts.htm">http://www.cisco.com/univercd/cc/td/doc/product/cable/bbcmref/bbcmmts.htm</a>                                                                                                                                            |
| Cisco IOS Release 12.2 Command Reference        | Cisco IOS Release 12.2 Configuration Guides and Command References, at the following URL:<br><br><a href="http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/index.htm">http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/index.htm</a>                                                                                                                                                                                                                                                                         |

## Standards

| Standards <sup>1</sup> | Title                                                                                                 |
|------------------------|-------------------------------------------------------------------------------------------------------|
| SP-RFIV1.1-I09-020830  | Data-Over-Cable Service Interface Specifications Radio Frequency Interface Specification, version 1.1 |

1. Not all supported standards are listed.

## MIBs

| MIBs <sup>1</sup>                                      | MIBs Link                                                                                                                                                                                                              |
|--------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No new or modified MIBs are supported by this feature. | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

1. Not all supported MIBs are listed.

## RFCs

| RFCs <sup>1</sup> | Title                                    |
|-------------------|------------------------------------------|
| RFC 868           | Time Protocol                            |
| RFC 2131          | Dynamic Host Configuration Protocol      |
| RFC 2132          | DCHP Options and BOOTP Vendor Extensions |

1. Not all supported RFCs are listed.

## Technical Assistance

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

---

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, TeleRouter, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0502R)

Copyright © 2003 Cisco Systems, Inc. All rights reserved.



## A

- acronyms, list of [xix](#)
- Acterna [358, 380](#)
- Advanced spectrum management [376, 377](#)
  - CNR [378](#)
  - configuration examples [421](#)
  - configuring Dynamic Upstream Modulation [396](#)
  - configuring proactive channel management [399](#)
  - configuring spectrum groups [396](#)
  - frequency hopping [377](#)
  - hardware-based [376](#)
  - monitoring spectrum management [406](#)
  - proactive channel management [377](#)
  - SNMP [378](#)
  - verifying spectrum management configuration [402](#)

## B

- benefits
  - Advanced spectrum management [379](#)
  - cable monitor command [17](#)
  - flap-list troubleshooting [155](#)
  - Internal DOCSIS Configurator File Generator [179](#)
  - maximum CPE or host parameters [208](#)
  - spectrum management [378](#)
  - telco return [434](#)
- blind frequency hopping [373](#)

## C

- cable commands
  - cable dhcp-giaddr command [33](#)

- cable interface line card [376](#)
- Cable Manager 2.0 [154](#)
- cable monitor command
  - overview [14](#)
  - timestamping [22](#)
- cable plant [362, 430](#)
- cable relay agent [50, 52](#)
- cable time-server, no command [448](#)
- carrier-noise ratio. See CNR.
- ccsHoppingNotification attributes [410](#)
- ccsSNRRequestTable [407](#)
- ccsSpectrumDataTable [408](#)
- ccsSpectrumRequestTable [408](#)
- ccsUpSpecMgmtTable [409](#)
- channel-group [144](#)
- channel management, proactive [377](#)
- Cisco Broadband Troubleshooter [358](#)
- Cisco IOS commands
  - cable downstream annex [242, 243](#)
  - cable downstream interleave-depth [242, 243](#)
  - cable downstream modulation [242, 243](#)
  - hccp group channel-switch member-id [246](#)
  - hccp group lockout member-id [249](#)
  - hccp group protect member-id [246](#)
  - hccp group switch member [257](#)
  - hccp group unlockout member [250](#)
  - hccp group working member-id [246](#)
  - no hccp group {working | protect} member-id [250](#)
  - no shutdown [247](#)
  - ping [258](#)
  - show cable modem ip-address [258](#)
  - show config [260](#)
  - show hccp {group-member} channel-switch [252](#)

- show hccp brief [253](#)
- show hccp channel-switch [273](#)
- show ip interface brief [252](#)
- show module [254, 260](#)
- shutdown [249](#)
- switch group-name 0 [256](#)
- telnet [256](#)
- test module [256](#)
- Cisco RF Switch
  - configuring N+1 [235](#)
  - creating module bitmaps [238](#)
  - displaying module status [254](#)
  - in N+1 Redundancy [229](#)
  - modules [231](#)
  - testing with manual switchover [255](#)
- Cisco uBR10012 router [232, 238, 248, 256, 269, 273, 274, 279, 293](#)
  - and Cisco RF Switch [229](#)
  - chassis slot numeration [227](#)
  - configuring with HCCP [245](#)
  - N+1 Redundancy configurations [225, 226, 259](#)
  - N+1 Redundancy restrictions [223](#)
  - switchover testing tasks [251](#)
- Cisco uBR7246VXR router [229, 248, 285, 293](#)
  - N+1 Redundancy configurations [225, 228](#)
  - N+1 Redundancy restrictions [222](#)
  - switchover testing tasks [251](#)
- CLI commands [406](#)
- CNR [362, 377, 378, 379](#)
- combiner [355](#)
- combiner groups [367](#)
- commands
  - channel-group [144](#)
  - interface port-channel [145, 146](#)
- commands, configuration
  - Advanced spectrum management [396](#)
  - assigning spectrum group [389](#)
  - assigning upstream ports [389](#)
  - cable max-hosts command [211](#)
  - cable modem max-cpe command [209](#)
  - cable monitor command [17](#)
  - CMTS onboard TFTP server [194](#)
  - creating DOCSIS configuration file [180](#)
  - Dynamic Upstream Modulation, SNR-based [391](#)
  - Guided and Scheduled spectrum management [382](#)
  - spectrum management [382](#)
  - telco return [434](#)
  - time-of-day server [447](#)
  - verifying Advanced spectrum management configuration [402](#)
  - verifying frequency hopping [393](#)
- configuration examples
  - Advanced spectrum management [421](#)
  - cable max-hosts command [213](#)
  - cable modem max-cpe [213](#)
  - cable modem max-hosts [213](#)
  - cable monitor command [23](#)
  - combiner group [415, 416](#)
  - DOCSIS configuration file [196](#)
  - downstream traffic shaping [414](#)
  - Dynamic Upstream Modulation [419](#)
  - flap-list troubleshooting [171](#)
  - input power level [420](#)
  - max CPE or host parameters [213](#)
  - modulation profiles [419](#)
  - rate limiting [411, 414](#)
  - spectrum management [411, 417](#)
  - spectrum managment [415](#)
  - telco return [440](#)
  - time-of-day server [449](#)
  - time-scheduled spectrum group [415](#)
  - upstream ports assigned to combiner group [415](#)
  - upstream traffic shaping [411](#)
  - verify Dynamic Upstream Modulation settings [419](#)
  - verifying frequency hopping [393](#)
  - verifying spectrum group configuration [415](#)
  - verifying spectrum group creation [415](#)
- configuration file editor

create file, standalone editor [177](#)

configuration tasks

- Advanced spectrum management [396](#)
- assigning spectrum group, Guided and Scheduled [389](#)
- assigning upstream ports, Guided and Scheduled [389](#)
- cable config-file command [180](#)
- cable max-hosts command [211](#)
- cable modem max-cpe command [209](#)
- cable modem max-hosts command [212](#)
- cable monitor command [17](#)
- CMTS onboard TFTP server [194](#)
- creating DOCSIS configuration file [180](#)
- creating spectrum groups, Guided and Scheduled [385](#)
- Dynamic Upstream Modulation, SNR-based [391](#)
- flap-list troubleshooting [155](#)
- Guided and Scheduled spectrum management [382](#)
- Internal DOCSIS Configurator File Generator [179](#)
- maximum CPE or host parameters [209](#)
- reset max permitted CPE devices [209](#)
- setting downstream rate limiting [384](#)
- setting upstream rate limiting [382](#)
- specifying SNMP MIB objects, option 11 [184](#)
- specifying vendor-specific info, option 43 [191](#)
- spectrum management [382](#)
- telco return [434](#)
- time-of-day server [447](#)
- verifying Advanced spectrum management configuration [402](#)
- verifying frequency hopping [393](#)

CPE

- limit max permitted number [177](#)
- maximum number [202](#)
- set max number

customer premises equipment. See CPE.

customer premises equipment devices [202](#)

## D

DCMTA [358](#)

dense segment [367](#)

DHCP [355](#)

DHCP giaddr [33](#)

DOCSIS configuration file

- set max permitted CPE devices on CMTS [202](#)

downstream rate limiting [372](#)

downstream traffic shaping [372](#)

DSP [377, 380](#)

Dynamic Host Configuration Protocol. See DHCP.

Dynamic Upstream Modulation [358, 374, 379, 380](#)

Dynamic Upstream Modulation (CNR-based) [378](#)

Dynamic Upstream Modulation (SNR-based) [374](#)

## E

EtherChannel

- command reference [143](#)
- configuration examples [136](#)
- configuring [133](#)
- FastEtherChannel [132](#)
- GigabitEtherChannel [132](#)
- information about [131](#)
- restrictions [131](#)
- verifying [136](#)

EtherChannel for the Cisco CMTS [129](#)

examples, configuration

- Advanced spectrum management [421](#)
- cable max-hosts command [213](#)
- cable modem max-cpe [213](#)
- cable modem max-hosts [213](#)
- cable monitor command [23](#)
- combiner group [415, 416](#)
- DOCSIS configuration file [196](#)
- downstream traffic shaping [414](#)
- Dynamic Upstream Modulation [419](#)
- flap-list troubleshooting [171](#)

input power level [420](#)  
 maximum CPE or host parameters [213](#)  
 modulation profiles [419](#)  
 rate limiting [411, 414](#)  
 spectrum management [411, 415, 417](#)  
 telco return [440](#)  
 time-of-day server [449](#)  
 time-scheduled spectrum group [415](#)  
 upstream ports assigned to combiner group [415](#)  
 upstream traffic shaping [411](#)  
 verifying Dynamic Upstream Modulation settings [419](#)  
 verifying frequency hopping [393](#)  
 verifying spectrum group configuration [415](#)  
 verifying spectrum group creation [415](#)

## F

FEC [366, 374](#)  
 fiber nodes [368, 369](#)  
 figures  
     LAN Packet Analyzer in a DOCSIS Two-Way Configuration [16](#)  
     Telco Return Network Example [433](#)  
 fixed upstream frequency [366](#)  
 flap-list detection [362](#)  
 flap-list troubleshooting [153](#)  
     Cable Manager 2.0 [154](#)  
     monitoring and troubleshooting [162](#)  
     performing amplitude averaging [169](#)  
     power adjustment [158](#)  
     troubleshooting suggestions [166, 169](#)  
     using CLI [162, 166](#)  
     using SNMP [166](#)  
     using SNMP API [161](#)  
 forward error correction. See FEC.  
 frequency agility [369, 377](#)  
 frequency hopping  
     blind frequency hops [377](#)  
     capabilities [372](#)

guided [373](#)  
 hardware-based [377](#)  
 intelligent [380](#)  
 RF tone generator [394](#)  
 spectrum groups [369](#)  
 time-scheduled [374](#)  
 frequency management policy [368](#)

## G

grant buffering [379](#)  
 grant shaping [372](#)  
 Guided and Scheduled spectrum management [370](#)  
 guided frequency hopping [373](#)

## H

hardware-based spectrum management [376, 377](#)  
 HCCP  
     configuring HCCP groups for N+1 Redundancy [245](#)  
     disabling HCCP Revertive on HCCP Protect interfaces [224](#)  
     displaying HCCP group status [251](#)  
     displaying HCCP interface status [253](#)  
     enabling HCCP Protect interfaces for N+1 Redundancy [247](#)  
     locking out HCCP interface switchover [249](#)  
     preconfiguring HCCP Protect interfaces for N+1 Redundancy [242](#)  
     removing configuration from HCCP Working interfaces [248](#)  
     removing configuration from HCCP Working or Protect interfaces [250](#)  
     shutting down HCCP Protect interfaces [248](#)  
     testing HCCP groups with manual switchover [257](#)  
 HCCP 1+1 [359](#)



**I**

## IF Muting

- in N+1 Redundancy [232](#)
- prerequisites [234](#)
- restrictions [233](#)

ingress noise [377, 379](#)

input power levels [376](#)

intelligent frequency hopping [380](#)

Intelligent spectrum management [376](#)

interface port-channel command [145](#)

**L**

line card [376](#)

**M**

max-servers no-limit option [447](#)

MC16S cable interface line card [376](#)

## MIBs

- Advanced spectrum management [378](#)
- Internal DOCSIS Configurator File Generator [198](#)
- SNMP support [407](#)
- spectrum management [426](#)

modulation profile [380](#)

modulation profiles [375](#)

## monitoring spectrum management

- using CLI commands [406](#)
- using SNMP [407](#)

**N**

## N+1 Redundancy

- additional references [293](#)
- Cisco RF Switch [229](#)
- configuration examples (table summary) [259](#)
- configuring the Cisco CMTS [241](#)

configuring the Cisco RF Switch [235](#)

feature history [220](#)

glossary [295](#)

IF Muting [232](#)

prerequisites for the Cisco CMTS [221](#)

pre-testing the CMTS [251](#)

restrictions/limitations on Cisco CMTS [222](#)

restrictions/limitations on Cisco uBR10012 router [223](#)

restrictions/limitations on Cisco uBR7246VXR  
router [222](#)

switchover testing procedures [255](#)

terminology [225](#)

testing HCCP groups with manual switchover [257](#)

with Cisco CMTS [219](#)

with Cisco RF Switch [229](#)

with Cisco uBR10012 router [226](#)

with Cisco uBR7246VXR router [222, 228](#)

noise impairments [362, 369, 379](#)

NTP [68, 126, 319, 450](#)

**O**

## overview

- cable max-hosts command [204](#)
- cable modem max-cpe command [204](#)
- cable modem max-hosts command [204](#)
- cable monitor command [14](#)
- flap-list troubleshooting [153](#)
- Internal DOCSIS Configurator File Generator [177](#)
- maximum CPE or host parameters [202](#)
- telco return [431](#)
- time-of-day server [446](#)

**P**

ports [373](#)

power levels [376](#)

## prerequisites

- spectrum management [354](#)

telco return [430](#)  
 proactive channel management [380](#)  
 proactive frequency hopping [356](#)  
 protocols  
     TFTP (Trivial File Transfer Protocol) [45](#)

## Q

QAM [379, 380](#)  
 QPSK [380](#)

## R

rate limiting [371](#)  
 rate limiting, downstream [372](#)  
 rate limiting, upstream [371](#)  
 redundancy support [359](#)  
 relay agent, activating cable [50, 52](#)  
 restrictions and limitations  
     cable monitor command [14](#)  
     DCMTA [358](#)  
     Dynamic Upstream Modulation [356](#)  
     fixed frequency spectrum groups [358](#)  
     flap-list troubleshooting [152](#)  
     HCCP 1+1 redundancy support [359](#)  
     Internal DOCSIS Configurator File Generator [176](#)  
     spectrum management [356](#)  
     telco return [430](#)  
     time-of-day server [446](#)  
     uBR-MC16S line card [356](#)  
 RFCs  
     Internal DOCSIS Configurator File Generator [198](#)  
     spectrum management [426](#)  
 RF tone generator [394](#)

## S

segment, upstream [367](#)

service udp-small-servers command [447](#)  
 set clock command [68, 126, 319, 450](#)  
 show cable modulation-profile command [402, 419](#)  
 show cable spectrum-group command [415](#)  
 show interface port-channel command [146](#)  
 simple network management protocol. See SNMP.  
 SNMP  
     advanced spectrum management feature [378](#)  
     benefits, advanced spectrum management [380](#)  
     ccsHoppingNotification attributes [410](#)  
     ccsSNRRRequestTable [407](#)  
     ccsSpectrumDataTable [408](#)  
     ccsSpectrumRequestTable [408](#)  
     ccsUpSpecMgmtTable [409](#)  
     MIB objects, using option 11 [184](#)  
     using to monitor spectrum management [407](#)  
 SNR [374](#)  
 software upgrade spectrum management [377](#)  
 sparse segment [367](#)  
 SPD. See Service Provider Descriptor.  
 spectrum analyzer [377](#)  
 spectrum groups [369](#)  
 Spectrum Management [362](#)  
 spectrum management  
     Advanced spectrum management [376, 377](#)  
     configuration tasks [382](#)  
     Dynamic Upstream Modulation [374](#)  
     Dynamic Upstream Modulation (CNR-based) [378](#)  
     frequency hopping [369, 372](#)  
     frequency management policy [368](#)  
     Guided and Scheduled spectrum management [370](#)  
     guided frequency hopping [373](#)  
     guidelines [370](#)  
     input power levels [376](#)  
     Intelligent spectrum management [376](#)  
     noise impairments [369](#)  
     prerequisites [354](#)  
     software upgrade enhancements [377](#)  
     telco return support [373](#)

time-scheduled frequency hopping [374](#)  
 traffic shaping [371](#)  
 upstream frequency changes [366](#)  
 upstream segments and combiner groups [367](#)  
 upstream signal channel overview [366](#)  
 standards, MIBs, RFCs  
   Internal DOCSIS Configurator File Generator [198](#)  
   spectrum management [426](#)  
 subband [366](#)  
 system clock [68, 126, 319, 450](#)

## T

telco return  
   Baseline Privacy Interface [430](#)  
   cable interface line card [430](#)  
   clear cable modem reset command [430](#)  
   feature overview [431](#)  
   operation [432](#)  
   prerequisites [430](#)  
   registration IP address [438](#)  
   segment downstream channels [430](#)  
   Service Provider Descriptor [435](#)  
   show cable flap-list command [430](#)  
 terms and acronyms [xix](#)  
 TFTP (Trivial File Transfer Protocol)  
   configuring TFTP service [45](#)  
 time-of-day server [446](#)  
 time-scheduled frequency hopping [374](#)  
 timestamp [33, 445](#)  
 ToD (time-of-day) server [33](#)  
 ToD (time-of-day) service [43, 44](#)  
 token-bucket police [371](#)  
 ToS [372, 379](#)  
 traffic shaping [371, 379](#)  
 two-way [434](#)  
 type of service. See ToS.

## U

uBR-MC16S cable interface line card [356, 376, 377](#)  
 UCD [366](#)  
 Upstream Channel Descriptor. See UCD.  
 upstream frequency [366, 369](#)  
 upstream ports [373](#)  
 upstream rate limiting [371](#)  
 upstream signal channel overview [366](#)  
 upstream traffic shaping [371](#)

## V

Voice over IP. See VoIP.  
 VoIP [358](#)