



Cisco Remote PHY Device Software Configuration Guide for Cisco 1x2 / Compact Shelf RPD Software 8.x

First Published: 2020-03-31

Americas Headquarters

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



CONTENTS

PART I

Remote PHY System Start Up Configuration 19

CHAPTER 1

Cisco Remote PHY System Overview 1

Introduction 1

Hardware Compatibility Matrix for Cisco Remote PHY Device 2

Benefits 2

Cisco CCAP RF Line Card for R-PHY 3

Cisco Digital Physical Interface Card 3

Cisco Remote PHY Device 4

Network Architecture 5

Network Topologies 5

Daisy Chain Architecture 6

CHAPTER 2

Cisco Remote PHY System Bring Up 7

Hardware Compatibility Matrix for Cisco Remote PHY Device 7

Information about Bring Up 8

How to Bring Up 8

Configuring DHCP Server 8

Configuring DHCP Server using IPv4 8

Configuring DHCP Server using IPv6 Stateless 10

Configuring DHCP Server using IPv6 Stateful 10

Configuring PTP 11

Configuring cBR-8 12

Setting Device Alias 13

Updating the Default RPD Password 14

CHAPTER 3	Network Authentication	19
	Hardware Compatibility Matrix for Cisco Remote PHY Device	19
	Information about Network Authentication	20
	How to Enable Network Authentication	20
	Installing Certificates in Radius Server	20
	Configuring Radius Server	21
	Configuring Switch	21
	Verifying Authentication Status	22

CHAPTER 4	Synchronizing Time on Cisco Remote PHY Devices	23
	Hardware Compatibility Matrix for Cisco Remote PHY Device	23
	Information about Time Synchronization	24
	Remote DTI	24
	Restrictions for Configuring Time Synchronization	24
	How to Configure Time Synchronization	25
	Configure Time Interface and PTP Domain	25
	Verifying Time Interface and PTP Domain Configuration	26
	Configure RPD PTP Connection	27
	Verifying RPD PTP Connection Configuration	27
	Associate R-DTI with RPD	27
	Verifying Associating R-DTI with RPD	28
	Verifying PTP Clock Functioning	30
	Verifying PTP Clock Running Domain	30
	Verifying Time Sync State	30
	Verifying Time Sync Statistics	31
	Configuration Examples	32
	Example: Configure Time Interface and PTP Domain	32
	Example: Configure RPD PTP Connection	32
	Example: Associate R-DTI with RPD	33
	Feature Information for Synchronizing Time on R-PHY Devices	33

CHAPTER 5	DEPI/UEPI/L2TP integration with Cisco Remote PHY Device	35
	Hardware Compatibility Matrix for Cisco Remote PHY Device	35

Information about DEPI/UEPI/L2TP integration with RPD	36
DEPI	36
UEPI	36
How to Configure DEPI/UEPI/L2TP integration with RPD	36
Configuring depi-class/l2tp-class Pair	36
Verifying depi-class/l2tp-class Pair Configuration	37
Verifying the RPD Status	37
Display DEPI Related Information	37
Feature Information for DEPI/UEPI/L2TP integration with RPD	38

CHAPTER 6**DEPI Latency Measurement 41**

Hardware Compatibility Matrix for Cisco Remote PHY Device	41
Information about DEPI Latency Measurement	42
How to Configure DLM	42
Configuring DLM	42
Verifying DLM Configuration	42
Example: DLM Configuration	43
Feature Information for DLM	43

CHAPTER 7**Multiple Cores 45**

Hardware Compatibility Matrix for Cisco Remote PHY Device	45
Information about Multiple Cores	46
Restrictions for Multiple Cores Configuration	46
How to Configure Multiple Cores	46
Configuring Multiple Cores	47
Verifying Multiple Cores Configuration	47

CHAPTER 8**GCPP Support for Remote PHY 49**

Information About GCPP Support	49
Hardware Compatibility Matrix for Cisco Remote PHY Device	50
GCPP Core	51
How to Configure GCPP Core	51
Adding GCPP Core IP Address	51
Configuring Cisco cBR for Enabling GCPP	51

Configuration Example 52
 Example: GCPP Configuration 52
 Feature Information for GCPP Support 52

CHAPTER 9

IKEv2 Mutual Authentication 53

Information about IKEv2 Mutual Authentication 53
 Configure IKEv2 Mutual Authentication 53
 CMTS Side Configuration 54
 RPD Node Side Configuration 54
 Feature Information for IKEv2 Mutual Authentication 54

CHAPTER 10

Power Configuration for Compact Shelf 57

Hardware Compatibility Matrix for Cisco Remote PHY Device 57
 Information about Power Configuration for Compact Shelf 58
 How to Configure Base Power, Downstream Power Level, and Upstream Power Level 58
 Configuring Maximum Carriers 58
 Configuring Base Channel Power Level 58
 Configuring RF Channel Power Level 59

CHAPTER 11

Link Layer Discovery Protocol 61

Hardware Compatibility Matrix for Cisco Remote PHY Device 61
 Link Layer Discovery Protocol 62
 Displaying LLDP Status 62
 Feature Information for LLDP 63

CHAPTER 12

TACACS+ 65

Hardware Compatibility Matrix for Cisco Remote PHY Device 65
 TACACS+ 66
 Configuring TACACS+ 66
 Displaying TACACS+ Configuration 66
 Feature Information for TACACS+ 67

PART II

Remote PHY System High Availability 69

CHAPTER 13**Cisco Remote PHY Line Card and Supervisor Redundancy 71**

- Hardware Compatibility Matrix for Cisco Remote PHY Device 71
- Information About Remote PHY Line Card and Supervisor Redundancy 72
 - Line Card Redundancy 72
 - Supervisor Redundancy 73
 - DPIC Link Redundancy 74
- How to Configure Remote PHY Line Card Redundancy 74
 - Configuring DPIC Ports 75
 - Configuring RPD 75
 - Configuring Remote PHY Line Card Redundancy 75
 - Verifying Remote PHY Line Card Redundancy Configuration 76
- How to Configure DPIC Link Redundancy 76
 - Configuring DPIC Link Redundancy 76
 - Verifying DPIC Link Redundancy 77
- Feature Information for Remote PHY Redundancy 78

PART III**Remote PHY System Configuration 79****CHAPTER 14****Cisco Remote PHY Controller Profile and RPD Configuration 81**

- Hardware Compatibility Matrix for Cisco Remote PHY Device 82
- Controller Profile and RPD 82
 - RPD Configurations 83
 - Prerequisites for Configuring Controller Profile and RPD 84
 - Restrictions for Configuring Controller Profile and RPD 84
- Configure Controller Profile and RPD 84
 - Configure Upstream Controller Profile 84
 - Verify Upstream Controller Profile Configuration 85
 - Configure RPD for US Controller Profile 86
 - Configure Downstream Controller Profile 87
 - Verify Downstream Controller Profile Configuration 87
 - Configure RPD for DS Controller Profile 87
 - Verify RPD Association with Controller Profile 88
 - Configure Analog Tx/Rx Modules Alarm Threshold 88

Verify Analog Tx/Rx Modules Alarm Threshold Configuration	88
Configure Downstream Sharing	89
Configure Controller in Fiber Node	89
Verify CM RPD Association	89
Display GCP Related Information	89
Display DEPI Related Information	91
Troubleshooting Tips	92
Configuration Examples	92
Example: Controller Profile Configuration	92
Example: Downstream Sharing Configuration	93
Feature Information for Remote PHY Controller Profile and RPD Configuration	93

CHAPTER 15

Cisco Remote PHY Device Downstream Virtual Splitting	95
Hardware Compatibility Matrix for Cisco Remote PHY Device	95
Information about RPD Downstream Virtual Splitting	96
Configure RPD Downstream Virtual Splitting	96
Configure Multicast DEPI Pool	96
Configure Redundant Multicast DEPI Pool	97
Enable Multicast Sharing under Downstream Controller Profile	98
Configure the RPD with the Same Downstream Controller and Profile	98
Configure the RPDs to different fiber-nodes	99
Configure the RPDs to MAC Domain	99
Enable Multicast on Cisco cBR-8 Router	99
Enable Multicast on Layer 2 Switch	100
Enable Multicast on Layer 3 Router	100
Verify RPD Downstream Virtual Splitting Configuration on cBR-8 Side	100
Verify RPD Virtual Downstream Splitting Configuration on Node Side	101
Example: RPD Downstream Virtual Splitting Configuration	102
Feature Information for RPD Downstream Virtual Splitting	103

CHAPTER 16

Cisco Remote PHY DS OFDM Channel Configuration	105
Hardware Compatibility Matrix for Cisco Remote PHY Device	105
Information About R-PHY DOCSIS 3.1 DS OFDM Channel	106
Configure DS OFDM Channel	106

Configure OFDM Channel Profile	106
Configure RPD Port/Controller and Channel	107
Configure RF Channel Bandwidth in Wideband Interface	108
Verify the Profile Ordering	108
Verify OFDM Channel Profile	108
Verify OFDM Channel	110
Verify OCD and DPD of MAC Domain	110
Verify Profile Management Data	111
Verify OCD and DPD Messages in RPD	112
Verify per-Profile Counter on RPD	113
Verify the Drop Counter in DPS	113
Configuration Example	115
Feature Information for RPHY DS OFDM Channel Configuration	115

CHAPTER 17**Virtual Combining of Upstream Channels on RPD 117**

Hardware Compatibility Matrix for Cisco Remote PHY Device	117
Information About Virtual Combining of Upstream Channels	118
Configure Virtual Combining of Upstream Channels	118
Configure RPD for Virtual Combining	118
Verify Upstream Virtual Combining Details	119
Configuration Example	120
Example for Configuring RPD for Virtual Combining	120
Feature Information for Virtual Combining of Upstream Channels	121

CHAPTER 18**Redundant Multicast DEPI Pool 123**

Redundant Multicast DEPI Pool	123
Configure Redundant Multicast DEPI Pool	124
Configuring Redundant Multicast DEPI Pool	124
Verify Assigned Multicast IP Addresses	125
Feature Information for Redundant Multicast DEPI Pool	125

CHAPTER 19**DOCSIS3.1 Downstream Resiliency for RPHY 127**

Hardware Compatibility Matrix for Cisco Remote PHY Device	127
Information about DOCSIS3.1 Downstream Resiliency for RPHY	128

Configure DOCSIS3.1 Downstream Resiliency for RPHY 129
 Configure DOCSIS3.1 Downstream Resiliency for RPHY 129
 Display OFDM Specific CM-STATUS Events 129
 Feature Information for DOCSIS3.1 Downstream Resiliency for RPHY 130

CHAPTER 20

Dynamic Bonding Group for RPHY 131

Hardware Compatibility Matrix for Cisco Remote PHY Device 132
 Configure Dynamic Bonding Group 132
 Enable Dynamic Bonding Group 132
 Enable DS-Resiliency and Configure Resiliency Bonding Group 133
 Enable ACFE 133
 Verify Dynamic Bonding Group Configuration 133
 Configure Load Balancing with Dynamic Bonding Group Enabled 135
 Enable Load Balancing for DOCSIS 3.0 and DOCSIS 3.1 136
 Enable DOCSIS 3.0 and DOCSIS 3.1 Static Load Balance 136
 Enable DOCSIS 3.0 and DOCSIS 3.1 General Load Balance Group 136
 Enable Dynamic Load Balance and Fixed-Primary Channel Movement 136
 Verify Static Load Balancing Configuration 136
 Verify Dynamic Load Balancing Configuration 139
 Feature Information for Dynamic Bonding Group 140

CHAPTER 21

Cisco Remote PHY Device IPv6 143

Hardware Compatibility Matrix for Cisco Remote PHY Device 143
 Information about RPD IPv6 144
 Configure RPD IPv6 Unicast Online 144
 Configure Unicast IPv6 144
 Configure RPD core interface 145
 Configure IPv6 PTP Clock Option 145
 Verify IPv6 PTP Clock Option Configuration 146
 Verify RPD IPv6 Configuration 147
 Configure IPv6 DS Splitting 147
 Configure the multicast IPv6 DEPI pool 148
 Enable Multicast Sharing under Downstream Controller Profile 148
 Configure the RPD with the Same Downstream Controller and Profile 148

Configure the RPDs to different fiber-nodes	148
Configure the RPDs to MAC Domain	148
Enable IPv6 multicast on Cisco cBR-8 Router	149
Verify the IPv6 DS Splitting Configuration	149
Feature Information for Remote-PHY Device IPv6	151

CHAPTER 22**DOCSIS 3.1 OFDMA Channel Configuration 153**

Hardware Compatibility Matrix for Cisco Remote PHY Device	153
Information about OFDMA Channel Configuration	154
Modulation Profile	154
OFDMA Channel Exclusion Band	154
Configure OFDMA Channel	155
Configure OFDMA Modulation Profile	155
Verify OFDMA Modulation Profile Configuration	156
Configure OFDMA Channel	156
Bind Upstream Controllers With RPHY Ports	157
Verify OFDMA Channel Configuration	157
Configure Exclusion / Unused Bands	159
Verify Exclusion / Unused Bands	160
Override OFDMA Modulation Profile Per Channel	160
Verify Override Configuration	161
Bind OFDMA Channel Profile to Controller	161
Bind OFDMA Upstream to Cable Interface	161
Determine DOCSIS 3.1 Cable Modems and the Cable Modems Using OFDMA Upstreams	162
Verify DOCSIS 3.1 Upstream OFDMA Channel Bonding Across DOCSIS 3.0 ATDMA Channels	163
Support for Line Card High Availability	164
Configure Line Card High Availability	164
Support for Line Card Process Restart	164
Configure Line Card Process Restart	164
Feature Information for DOCSIS 3.1 OFDMA Channel Configuration	165

CHAPTER 23**Spectrum Capture 167**

Hardware Compatibility Matrix for Cisco Remote PHY Device	167
Spectrum Capture	168

Verifying Spectrum Capture Configuration 168
 Feature Information for Spectrum Capture 169

CHAPTER 24

Viavi Integration 171

Hardware Compatibility Matrix for Cisco Remote PHY Device 171
 Viavi Integration 172
 Verifying Spectrum Capture Configuration 172
 Feature Information for Viavi Integration 173

PART IV

Remote PHY System Video Configuration 175

CHAPTER 25

Cisco Remote PHY Video Configuration 177

Hardware Compatibility Matrix for Cisco Remote PHY Device 177
 Hardware Compatibility Matrix for Cisco Remote PHY Device 178
 Information About R-PHY Video Configuration 178
 How to Configure R-PHY Video 179
 Configuring Downstream Controller Profile 179
 Configuring RPD 179
 Configuring Downstream Sharing 180
 Configuring Video 181
 Configuring Virtual Service Group 181
 Example: R-PHY Video Configuration 182
 Feature Information for Remote PHY Video 184

CHAPTER 26

Remote PHY DVB Video on Demand 185

Information About DVB VOD 185
 Overview of DVB VOD 185
 Session based Scrambling Setup 186
 Fail-to-Clear 186
 Tier based Scrambling Setup 187
 Restrictions for DVB 187
 How to Configure DVB 187
 Configuring RPHY DVB VoD 187
 Verifying the DVB Configuration 189

Troubleshooting Tips	191
Configuration Examples	191
Example: Basic Session-based Scrambling Configuration	192
Example: Basic Tier-based Scrambling Configuration	192
Example: Basic Session-based Dualcrypt Scrambling Configuration	193
Additional References	194
Feature Information for RPHY DVB VoD Support	194

CHAPTER 27**Cisco Remote PHY PowerKEY VOD 197**

Hardware Compatibility Matrix for Cisco Remote PHY Device	197
Information About PowerKEY VOD	198
Overview of PowerKEY VoD	198
How to Configure RPHY PowerKey VOD	198
Configuring the Encryption Type on the Line Card	198
Verifying the Encryption Configuration	199
Configuring the Encrypted Virtual Carrier Groups	199
Configuring the Encrypted Virtual Carrier Groups	199
Configuring the Service Distribution Groups and Binding	200
Configuring the Logical Edge Device and GQI Protocol	200
Verifying the PowerKEY VoD Configuration	201
Configuration Examples	203
Example: Configuring Encryption Type on the Line Card	203
Example: Configuring Encrypted Virtual Carrier Groups	203
Example: Configuring Service Distribution Groups and Binding	203
Feature Information for Rmote PHY PowerKEY VoD	204

CHAPTER 28**Cisco Remote PHY Pre-encrypted Broadcast Video 205**

Hardware Compatibility Matrix for Cisco Remote PHY Device	205
Information About Pre-encrypted Broadcast Video	206
Multicast Table-based Sessions	206
MPTS Pass-through Session	207
How to Configure Pre-encrypted Broadcast Video Sessions	207
Configure a Port-Channel Interface	207
Configuring Pre-encrypted Broadcast Sessions	207

Configuring the Service Distribution Groups and Binding	208
Configuration Example for Pre-encrypted Broadcast Video Session	208
Feature Information for RPHY Pre-encrypted Broadcast Video	208

CHAPTER 29**Remote PHY BFS QAM Configuration 211**

Hardware Compatibility Matrix for Cisco Remote PHY Device	211
Information About BFS QAM Support	212
How to Configure BFS QAM for EC 7.x	212
Mapping Cisco cBR-8 as a GQI QAM	213
Creating VCG with One QAM Channel	213
Creating SDG for BFS Sessions on Cisco cBR	213
Create VCG for BFS	214
Creating Logical Edge Device	214
Creating GQI QAM for BFS on EC 7.x	215
How to Configure BFS QAM for RPD	215
Creating SDG for BFS Sessions for RPD	215
Creating LED for RPD	216
Defining Cable RPD	216
How to Configure BFS QAM for EC 8.x	216
Creating VCG for VoD QAM Channels	217
Creating VCG for SDV QAM Channels	217
Creating SDG	217
Creating LEDs	218
Configuration Example for BFS QAM Configuration	218
Example: BFS QAM Configuration on Cisco cBR for EC 7.x	219
Example: BFS QAM Configuration on RPD	220
Example: BFS QAM Configuration on Cisco cBR for EC 8.x	220
Feature Information for BFS QAM Configuration	221

CHAPTER 30**Remote PHY Switched Digital Video 223**

Switched Digital Video Services	223
Session Cloning	224
Redundant Multicast Sources	224
Benefits of Switched Digital Video	225

Prerequisites for Switched Digital Video	225
Restrictions for Switched Digital Video	225
Information About Switched Digital Video	225
QAM Sharing	225
QAM Replication	226
MPTS Pass-through Session	226
How to Configure the Switched Digital Video Services	226
Configuring Multicast Routing	226
Configuring Multicast Label	227
Configuring Multicast Table-based Sessions	228
Configuring Source Switching	228
Verifying Switched Digital Video Configuration	228
Troubleshooting Switched Digital Video Configuration	230
Configuration Examples for Switched Digital Video	230
Feature Information for Switched Digital Video	234

CHAPTER 31
Remote PHY QAM Profile Configuration 235

Information About QAM Profile	235
How to Configure Remote PHY QAM Profile	236
Configuring the QAM Profile on Downstream Channels	236
Verifying QAM Profile on Downstream Channels	236
Configuration Example	237
Feature Information for QAM Profile Configuration	237

CHAPTER 32
Cisco Remote PHY Out of Band 239

Hardware Compatibility Matrix for Cisco Remote PHY Device	239
Information About Out of Band	240
OOB 55-1	240
Forward Channels	241
OOB 55-2	241
Prerequisites	242
How to Configure 55-1 OOB	242
Configuring Global 55-1 OOB	242
Configuring Profile for 55-1 OOB	243

	Configuring Remote PHY Device for 55-1 OOB	243
	Configuring OOB with VRF	244
	Configuring Two Forward Channels	244
	Configuring Virtual OM with Multicast Pool	244
	Verifying OOB DS Details	245
	Verifying OOB US Details	245
	Verifying OOB Channel Details	245
	Debugging OOB	245
	Example: OOB Configuration	245
	Feature Information for OOB	246
<hr/>		
PART V	Remote PHY Management	249
<hr/>		
CHAPTER 33	Secure Software Download	251
	Hardware Compatibility Matrix for Cisco Remote PHY Device	251
	Information About Secure Software Download	252
	Prerequisites for Upgrading Software using SSD	252
	How to Upgrade Software from RPD and Cisco cBR Using SSD	252
	Initiating RPD Software Upgrade from Cisco cBR	252
	Initiating Software Upgrade from RPD Using SSD	252
	Verifying Software Upgrade Using SSD Configuration	253
	Examples for Upgrading HA RPHY Software	253
	Example: HA RPHY Software Upgrade from Cisco cBR	253
	Example: HA RPHY Software Upgrade from FCC or Primary eRPD	254
	Feature Information for Secure Software Download	254
<hr/>		
CHAPTER 34	Cisco Remote PHY Fault Management	255
	Information About Fault Management	255
	RPD Event Reporting	255
	Restrictions for Configuring RPD Events	255
	How to Configure RPD Events	256
	Configuring RPD Events	256
	Configuring 55-1 Upstream RPD Events	256
	Applying the Event Profile to RPD	257

Enable RPD Event Trap	257
Getting RPD Events	258
Clearing All Events on Cisco eBR Database	258
Viewing the RPD Events	258
Viewing RPD Events Using Log	259
Configuration Examples	259
Example: RPD Event Configuration	259
Example: RPD 55-1 Upstream Event Configuration	260
Feature Information for R-PHY Fault Management	260

CHAPTER 35**Cisco Remote PHY Device Operations and Debugging 261**

Hardware Compatibility Matrix for Cisco Remote PHY Device	261
Information about RPD Operations and Debugging	262
Prerequisites for RPD Operations	262
How to Access and Debug RPD	262
Accessing RPD using SSH	262
Disabling SSH Login Password	263
Debugging RPD	263
Verifying Disabled SSH Password Login	264
Configuration Examples	264
Example: Generating a New NMS pubkey	264
Example: Adding NMS pubkey in RPD	265
Feature Information for RPD Operations and Debugging	265

CHAPTER 36**RPD Reset 267**

Hardware Compatibility Matrix for Cisco Remote PHY Device	267
Information about RPD Reset	268
Resetting RPD	268
Soft-reset	268
History of RPD Reset Instances	269
RPD TACACS	270
Feature Information for RPD Reset	270

CHAPTER 37**Archiving RPD Logs 273**

Hardware Compatibility Matrix for Cisco Remote PHY Device	273
Information About Archiving Logs	274
Archiving Logs Using SCP or TFTP	274
Archiving Logs Locally	276
Copying RPD Log Files using SCP	277
Feature Information for Archiving Logs	277

CHAPTER 38**SSH Account Management 279**

Hardware Compatibility Matrix for Cisco Remote PHY Device	279
Information About SSH Account Management	280
Configure SSH Account Management	280
Add a New SSH Account	280
Delete an SSH Account	280
Change an SSH Account Password	281
View SSH Account Details	281
Feature Information for SSH Account Management	281



PART I

Remote PHY System Start Up Configuration

- [Cisco Remote PHY System Overview, on page 1](#)
- [Cisco Remote PHY System Bring Up, on page 7](#)
- [Network Authentication, on page 19](#)
- [Synchronizing Time on Cisco Remote PHY Devices, on page 23](#)
- [DEPI/UEPI/L2TP integration with Cisco Remote PHY Device, on page 35](#)
- [DEPI Latency Measurement, on page 41](#)
- [Multiple Cores, on page 45](#)
- [GCPP Support for Remote PHY, on page 49](#)
- [IKEv2 Mutual Authentication, on page 53](#)
- [Power Configuration for Compact Shelf, on page 57](#)
- [Link Layer Discovery Protocol, on page 61](#)
- [TACACS+, on page 65](#)



CHAPTER 1

Cisco Remote PHY System Overview

Finding Feature Information

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

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

- [Introduction, on page 1](#)
- [Hardware Compatibility Matrix for Cisco Remote PHY Device, on page 2](#)
- [Benefits, on page 2](#)
- [Cisco CCAP RF Line Card for R-PHY, on page 3](#)
- [Cisco Digital Physical Interface Card, on page 3](#)
- [Cisco Remote PHY Device, on page 4](#)
- [Network Architecture, on page 5](#)
- [Network Topologies, on page 5](#)

Introduction

Driven by market evolution towards triple-play services, cable operators in emerging markets are seeking standardized and digital fiber-based solutions for economical and future proof access technologies. Much of the demand is driven by the need to provide higher bandwidth packet transport for Internet connectivity, video and voice services.

Data Over Cable Systems Interface Standard (DOCSIS®) is a standardized technology for services over cable and thus has strong interoperability between system providers. It also provides robust Quality of Service (QoS) methods, ensuring packet delivery during periods of network congestion. Traditionally, DOCSIS runs on linear fiber (or HFC) to provide service and is not naturally applicable for digital fiber. Cisco has bridged the gap by introducing a new access technology called the Remote PHY.

Existing Architecture

In the emerging markets, most triple-play consumers live in multi-tenant buildings (referred to as Multi Dwelling Units or MDU) with the number of residents usually being less than 500 residents per building or cluster. These buildings are typically served by fiber with one of several “final 100 meter” technologies

installed in the buildings. These technologies include fiber, twisted pair, Ethernet, and coaxial. Cable operators have access to the cable in the building and use this cable for their services. Several technologies exist for enabling two-way services over cable. These include a number of proprietary and vendor-specific methods. However, a standards-based approach to using cable is typically preferred by operators, since this ensures vendor interoperability.

Need for the Cisco Remote PHY Solution

DOCSIS and EuroDOCSIS are standards that define two-way operation over a cable network. DOCSIS provides the necessary Quality of Service (QoS) tools for ensuring voice call connectivity during periods of network congestion that are anticipated in triple-play networks. DOCSIS is a robust and mature technology for voice, video, and IP video services.

The Cisco Remote PHY solution leverages existing IP technologies like Ethernet PON (EPON), Gigabit-capable Passive Optical Networks (GPON), and Metro Ethernet (MetroE) equipment; it deploys DOCSIS in MDUs over digital fiber to enable two-way services over cable.

Hardware Compatibility Matrix for Cisco Remote PHY Device



Note Unless otherwise specified, the hardware components introduced in a given Cisco Remote PHY Device Software Release are supported in all subsequent releases.

Table 1: Hardware Compatibility Matrix for the Cisco Remote PHY Device

Cisco HFC Platform	Remote PHY Device
Cisco GS7000 Super High Output Node	Cisco 1x2 / Compact Shelf RPD Software 2.1 and Later Releases
Cisco GS7000 Super High Output Intelligent Node (iNode)	Cisco 1x2 / Compact Shelf RPD Software 4.1 and Later Releases Cisco Intelligent Remote PHY Device 1x2 <ul style="list-style-type: none"> • PID—iRPD-1X2= • PID—iRPD-1X2-PKEY=



Note The -PKEY suffix in the PID indicates units that enable the SCTE-55-2 Out-of-Band protocol support.

Benefits

The Cisco Remote PHY solution provides a cost-effective digital fiber-based DOCSIS solution that uses Ethernet PON (EPON), Gigabit-capable Passive Optical Networks (GPON), or Metro Ethernet (MetroE) as

the transmission network between the Cisco CMTS and CM. Both the PON technology and DOCSIS is used in the same network.

- Simple and low cost PON transmission as opposed to costly HFC transformation.
- Reduced investment cost including capital and operational expenditure.
- Low-cost yet highly stable Cisco GS7000 node (includes only the PHY layer).
- Reduced CMTS hardware complexity.
- No restriction on Converged Interconnect Network (CIN) network.
- Futureproof architecture. Easy to migrate as the hardware and control functions are on separate layers.
- End-to-end QoS assurance provided by DOCSIS.
- Support for all DOCSIS services.
- Support for existing DOCSIS network provisioning system.
- High access bandwidth.
- With deep fiber, the optical noise contribution to SNR is eliminated. As a result, the remote QAM modulator runs at higher orders of modulation as compared to a centralized QAM modulator.

Cisco CCAP RF Line Card for R-PHY

The Cisco CCAP RF line card for remote PHY architecture is available in two flavours:

- CBR-LC-8D31-16U30—This RF line card with the downstream and upstream PHY modules can be connected with the Cisco GS7000 node by configuring it using the **card cBR-CCAP-LC-40G r-phy** command.
- CBR-CCAP-LC-40G-R—This RF line card with no downstream and upstream PHY modules can be connected with the Cisco GS7000 node.
- CBR-CCAP-LC-G2-R—This line card supports a maximum of 8 RPDs in one service group.

Cisco Digital Physical Interface Card

The Cisco Digital Physical Interface Card (DPIC) transmits and receives RF signals between the subscriber and headend over the hybrid fiber-coaxial (HFC) system and is DOCSIS-compliant. This interface card is designed specifically for the Cisco cBR router. The PID is cBR-DPIC-8X10G.

The DPIC is installed in the CMTS and connected to the Cisco GS7000 node via the EPON, GPON, or Metro Ethernet. It supports both downstream and upstream traffic. Both the downstream and upstream traffic share the same ports.

The DPIC supports:

- Eight ten gigabit ethernet SFP+ interfaces
- 80 gigabit non-blocking switching architecture with 40+40 protection scheme

- 40 gigabit DOCSIS traffic bandwidth when connected with the Cisco CBR-CCAP-LC-40G-R line card
- Cisco SFP-10G-SR-S/Cisco SFP-10G-LR-S/Cisco SFP-10G-ZR-S/Cisco SFP-10G-ER-S optic modules
- MACSec and 1588 TC

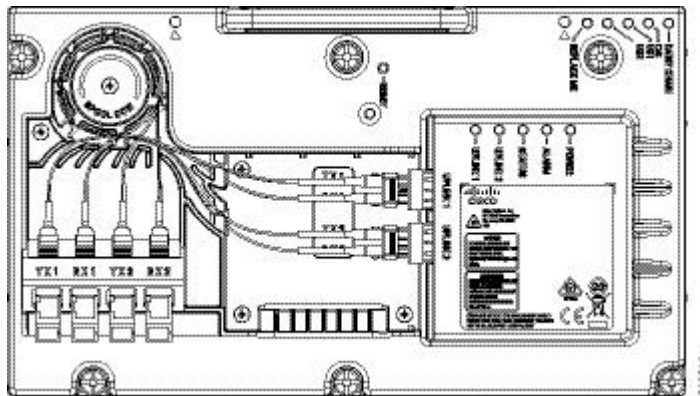
Cisco Remote PHY Device

The Cisco Remote PHY Device (RPD) has two variants – The standard RPD and the newer Intelligent RPD (iRPD). The standard RPD resides inside the Cisco GS7000 node while the Intelligent RPD (iRPD) resides inside the Intelligent Node. Below are some of its features:

- Full spectrum DOCSIS 3.0 support
- Full spectrum DOCSIS 3.1 support
- Converged broadcast, narrowcast, and VOD video support
- Out of Band (OOB) signaling support
- Dual 10GBE SFP/SFP+ backhaul connectivity
- Support of Daisy Chain architecture topology
- CCAP support
- Support of optical overlay architectures

Additionally, the Cisco Intelligent Remote PHY Device (iRPD) provides an interface to the Intelligent Node RF section. This interface supports control plane communication that allows more extensive diagnostic and configuration control. The Intelligent Node supports touch-less configuration, per port spectrum capture, power-savings mode, and other enhanced features.

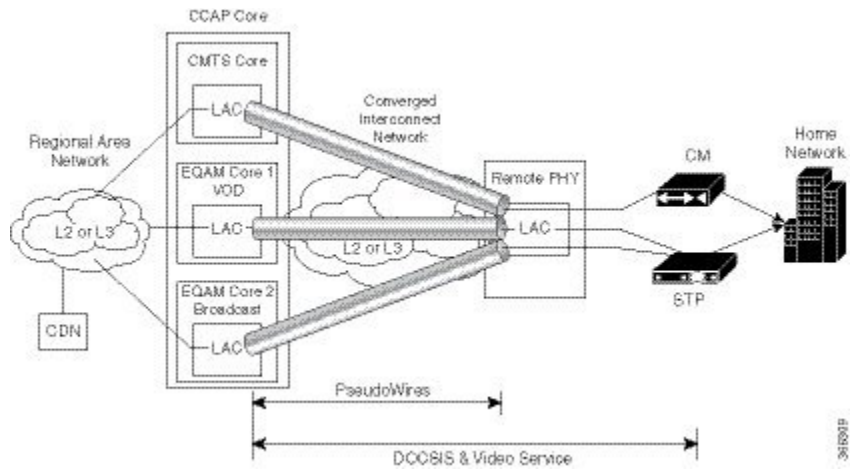
Figure 1: Cisco RPD



Network Architecture

The Cisco Remote PHY solution supports the *Single Controller Sharing* architecture. In this architecture, multiple Cisco GS7000 equipments share the downstream and upstream channels of a Cisco RF line card in a cisco cBR chassis.

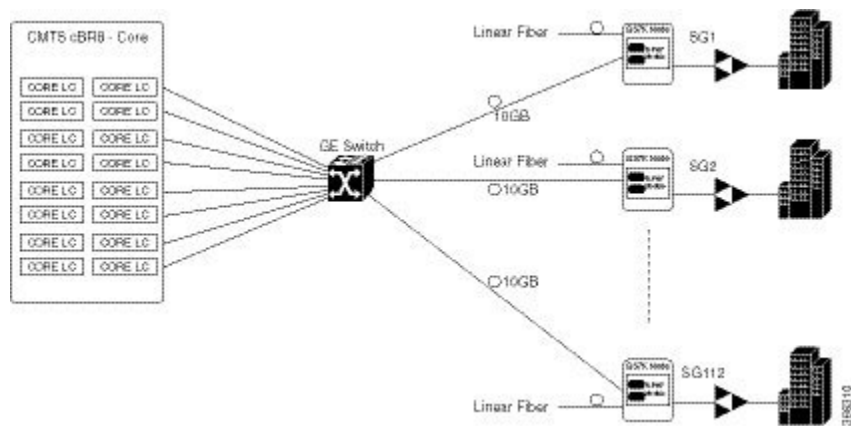
Figure 2: Single Controller Sharing Architecture



Network Topologies

The Cisco Remote PHY solution supports the following Ethernet-based networking topologies.

Figure 3: Standard Deployment

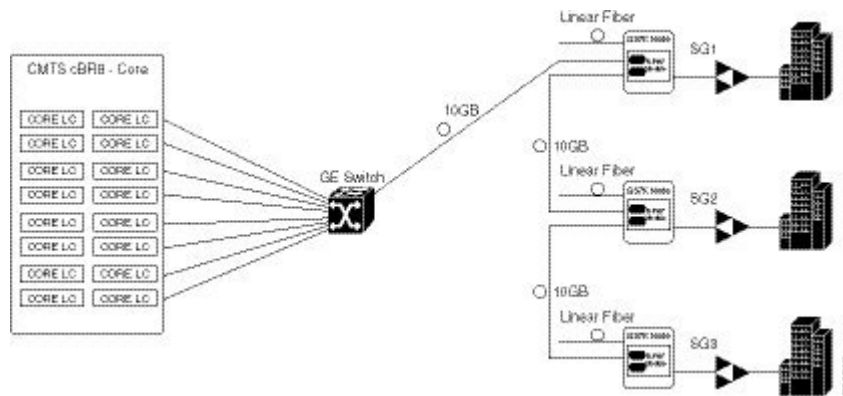


Note If you want to establish Equal-Cost Multi-Path (ECMP) connection between cBR-8 and RPD, pay attention to the ECMP configuration on both cBR-8 and the Converged Interconnect Network (CIN) routers. The number of maximum paths configured must be equal as or larger than the number of ECMP paths you want to set under the routing protocol for cBR-8 and the first adjacent CIN router.

Daisy Chain Architecture

Cisco Remote PHY devices support the daisy chain architecture. The daisy chain architecture includes multiple RPDs connected in series. This daisy chaining topology is transparent to CCAP core. The CCAP core is not notified about the chain topology because before the RPD sets up a GCP connection, notification flow is not configured.

Figure 4: Daisy Chain Deployment



Limitations

- In the daisy-chaining topology, if one RPD in the chain is down or any link in the middle breaks, the RPD in the downstream is disconnected, until the chain is restored again.
- You must be careful when resetting or clearing an RPD, as the CCAP core is not notified about the chain topology. If you clear or reset an upstream RPD in a daisy-chain, all RPDs after that specific RPD will be disconnected until the upstream RPD boots up.
- Each RPD reset needs a reprogramming of the FPGA. The connection is interrupted during this reset.
- The daisy-chaining topology uses both 10G ports of an RPD. Hence, features like link redundancy and port redundancy which need a second port are not supported.
- You should ensure that the total upstream traffic from all RPDs in the chain is not oversubscribing the 10G ports.
- The last RPD in the chain is not allowed to connect back to the switch to avoid a ring.
- The maximum number of RPDs in the chain is limited to six.



CHAPTER 2

Cisco Remote PHY System Bring Up

Finding Feature Information

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

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

- [Hardware Compatibility Matrix for Cisco Remote PHY Device, on page 7](#)
- [Information about Bring Up, on page 8](#)
- [How to Bring Up, on page 8](#)
- [Updating the Default RPD Password , on page 14](#)

Hardware Compatibility Matrix for Cisco Remote PHY Device



Note Unless otherwise specified, the hardware components introduced in a given Cisco Remote PHY Device Software Release are supported in all subsequent releases.

Table 2: Hardware Compatibility Matrix for the Cisco Remote PHY Device

Cisco HFC Platform	Remote PHY Device
Cisco GS7000 Super High Output Node	Cisco 1x2 / Compact Shelf RPD Software 2.1 and Later Releases
Cisco GS7000 Super High Output Intelligent Node (iNode)	Cisco 1x2 / Compact Shelf RPD Software 4.1 and Later Releases Cisco Intelligent Remote PHY Device 1x2 <ul style="list-style-type: none">• PID—iRPD-1X2=• PID—iRPD-1X2-PKEY=



Note The -PKEY suffix in the PID indicates units that enable the SCTE-55-2 Out-of-Band protocol support.

Information about Bring Up

Bring up process is prerequisite to the operation of the remote PHY system, just like the cable modem bring up in a DOCSIS system.

How to Bring Up

This section describes how to bring up RPD on Cisco cBR-8.

Configuring DHCP Server

You can choose to configure the DHCP server using any of the following methods.

Configuring DHCP Server using IPv4

To configure DHCP server using IPv4, follow the steps below:

1. Add option for CCAP-Core. Fill in the name, DHCP type, and vendor option string as shown in the figure below.

Design > DHCPv4 > Options

List/Add DHCP Option Definition Sets

Edit DHCP Option Definition Set rpd

Attribute	Value
Name*	rpd
DHCP Type*	V4
Description	
Vendor Option String	RPD
Vendor Option Regex String	
Vendor Option Enterprise Id	

2. Define option. Fill in the option number and name as shown in the figure below.

Design > DHCPv4 > Options

List/Add DHCP Option Definition Sets

Edit DHCP Option Definition Set *rpd*

rpd Option Definitions

List of Option Definitions for *rpd*

Number	Name
43	rpd-option-43
2	device-type
61	ccap-cores

366350

3. Define suboption. Fill in the name, type and repeat of suboption 61 as shown in the following figure.

Design > DHCPv4 > Options

List/Add DHCP Option Definition Sets

Edit DHCP Option Definition Set *rpd*

rpd Option Definitions

Attribute	Value
Number*	61
Name*	ccap-cores
Description	
type*	IP address
repeat	1+

4. Add the option into policy as shown in the following figure. Replace the IP address 120.102.15.1 in the figure to the DPIC port IP address.

DHCPv4 Vendor Options dhcp-cablelabs-config

Name	Number
<input type="text" value=""/>	
Configured Options	✗ [43] (<i>rpd</i>) rpd-option-43 (bin)

Configuring DHCP Server using IPv6 Stateless

The Cisco Remote PHY System supports the Stateless Address Auto Configuration (SLAAC). IPv6 address assignment of the RPD is governed by the configuration bits set in the ICMPv6 Router Advertisement (RA) message and the presence of a valid prefix in the Prefix Information Option (PIO). For more information about RPD IPv6 address assignment, refer to section 6.7 of Remote PHY Specification.

To configure DHCP server using IPv6 Stateless and enable SLAAC, follow the steps below:

1. Configure Prefix Type to “stateless” in CNR prefix.
2. Configure ICMPv6 Router RA message M Bit=0 and O Bit=1.



Note It is recommended that you follow the DHCP options listed in *Table 2 - Router Advertisement M Bit and O Bit Settings For SLAAC* of section 6.7.1 (CM-SP-R-PHY-I10) or 6.6.1 (CM-SP-R-PHY-I11) in the Remote PHY Specification.

To display the RPD get IPv6 address by SLAAC, use the **show dhcp** command.

```
R-PHY#show dhcp
Interface  IP-Address          Subnet-Mask
vbh0      2001:93:3:58:1204:9fff:fecl:100  ffff:ffff:ffff:ffff::
```

Details:

```
-----
Interface:          vbh0
AddrType:           IPv6<Stateless>
TimeServers:        2001:20:1:1::33
TimeOffset:         28800
LogServers:         2001:20:1:1::33
CCAPCores:         2001:93:3:58::1
```

Configuring DHCP Server using IPv6 Stateful

To configure DHCP server using IPv6 Stateful, follow the steps below:

1. Configure Prefix Type to “dhcp” in CNR prefix. See the following image.
2. Configure ICMPv6 Router RA message M Bit=1.

To display the RPD get IPv6 address by Stateful method, use the **show dhcp** command.

```
R-PHY#show dhcp
Interface  IP-Address          Subnet-Mask
vbh0      2001:93:3:58::d8   ffff:ffff:ffff:ffff::
```

Details:

```
-----
Interface:          vbh0
AddrType:           IPv6<Stateful>
TimeServers:        2001:20:1:1::33
TimeOffset:         28800
LogServers:         2001:20:1:1::33
CCAPCores:         2001:93:3:58::1
```

Configuring PTP

To configure PTP, use the following example as reference:

On the Cisco cBR-8 router:

```
interface Loopback1588
 ip address 159.159.159.4 255.255.255.255
interface TenGigabitEthernet5/1/3 /* connect to ASR903 */
 ip address 192.104.10.4 255.255.255.0

ip route 10.90.3.93 255.255.255.255 192.104.10.93 /* route to ASR903 loopback ip */

ptp clock ordinary domain 0
 servo tracking-type R-DTI
 clock-port slave-from-903 slave
 delay-req interval -4
 sync interval -5
 sync one-step
 transport ipv4 unicast interface Lo1588 negotiation
 clock source 10.90.3.93 /* ASR903 loopback ip */

ptp r-dti 1
 ptp-domain 0 /* same domain number with ptp server */
 clock-port 1
 ethernet 1 /* default value is same index with clock-port index, for RPD, ethernet
1=vbh0, ethernet 2=vbh1 */
 clock-source 10.90.3.93 gateway 93.3.10.2 /* clock-source is ASR093 loopback ip,
gateway is ASR903 BDI ID for node */
```

On ASR903 router as PTP primary clock:

```

ptp clock ordinary domain 0
clock-port Master-to-all-cBR8 master
sync interval -5
sync one-step
transport ipv4 unicast interface Lo1588 negotiation

interface Loopback1588
ip address 10.90.3.93 255.255.255.255

interface GigabitEthernet0/3/5
no ip address
negotiation auto
cdp enable
service instance 31 ethernet /* 31 is vlan id */
encapsulation dot1q 31
rewrite ingress tag pop 1 symmetric
bridge-domain 31
service instance 32 ethernet
encapsulation dot1q 32
rewrite ingress tag pop 1 symmetric
bridge-domain 32
interface BDI31 /* for cBR, SUP PIC */
ip address 192.104.10.93 255.255.255.0
no shut
interface BDI32 /* For RPD */
ip address 93.3.10.2 255.255.255.0
no shut

ip route 159.159.159.4 255.255.255.255 192.104.10.48 /* route to cbr-8 loopback ip */

```

Configuring cBR-8

To configure the cBR-8 to bring up the RPD, use the following example as reference:

```

/* D-PIC TenGiga interface config */
interface TenGigabitEthernet0/1/0
ip address 93.3.10.1 255.255.255.0
ip helper-address 20.1.0.33

/* Downstream/Upstream controller profile */
cable downstream controller-profile 101
rf-chan 0 95
type DOCSIS
frequency 381000000
rf-output NORMAL
qam-profile 1
docsis-channel-id 1

cable upstream controller 201
us-channel 0 channel-width 1600000 1600000
us-channel 0 docsis-mode atdma
us-channel 0 minislots-size 4
us-channel 0 modulation-profile 221
no us-channel 1 shutdown

/* RPD configuration */
cable rpd node1
identifier 0004.9f03.0061
core-interface Te0/1/0
rpd-ds 0 downstream-cable 0/0/0 profile 101
rpd-us 0 upstream-cable 0/0/0 profile 201

```



```

r-dti 1
rpd-event profile 0
rpd-55d1-us-event profile 0

interface Cable0/0/0
  load-interval 30
  downstream Downstream-Cable 0/0/0 rf-channel 0-23
  upstream 0 Upstream-Cable 0/0/0 us-channel 0
  upstream 1 Upstream-Cable 0/0/0 us-channel 1
  upstream 2 Upstream-Cable 0/0/0 us-channel 2
  upstream 3 Upstream-Cable 0/0/0 us-channel 3
  cable upstream bonding-group 1
    upstream 0
    upstream 1
    upstream 2
    upstream 3
  attributes 80000001
  cable bundle 1
  cable ip-init ipv6
interface Wideband-Cable0/0/0:0
  cable bundle 1
  cable rf-channels channel-list 0-7 bandwidth-percent 10
interface Wideband-Cable0/0/0:1
  cable bundle 1
  cable rf-channels channel-list 8-15 bandwidth-percent 10
cable fiber-node 200
  downstream Downstream-Cable 0/0/0
  upstream Upstream-Cable 0/0/0

```

Setting Device Alias

Configuring an RPD for the first time using the command **cable rpd name** triggers RPD provisioning. In Cisco IOS XE Gibraltar 16.12.1z and later releases, the RPD name configured during RPD configuration on the Cisco cBR is set as the device alias of the RPD. Device Alias is an alias for the RPD device, used by device configuration and management systems.



Note You can configure device alias of an RPD via MIB docsRphyCtrlRpdInitProvCtrlDeviceAlias. After an RPD reset, the device alias resets. The Cisco cBR sets the RPD name configured during RPD provisioning as the device alias.

The following example shows the use of **cable rpd name**.

```

/* RPD configuration */
cable rpd node1
  identifier 0000.5e00.0061
  core-interface Te0/1/0
    rpd-ds 0 downstream-cable 0/0/0 profile 101
    rpd-us 0 upstream-cable 0/0/0 profile 201
  r-dti 1
  rpd-event profile 0
  rpd-55d1-us-event profile 0

```

The following example shows the device alias.

```

Router#show cable rpd 0000.5e00.0061 identification
RPD ID                               : 0000.5e00.0061
Vendor Name                           : Cisco

```

```

Vendor Id                : 9
Model Number             : GS7K-RPD-1X2
Device Mac Address       : 0000.5e00.0061
Current Sw Version       : v8.3_20200516060512
Boot Rom Version         : Primary: U-Boot 2016.01 (Sep 11 2019 - 13:02:25
+0800) *;Golden: U-Boot 2016.01 (Feb 16 2017 - 09:03:06 +0800);
Device Description      : RPD
Device Alias             : node1
Serial Number            : CAT2038E3U0
Us Burst Receiver Vendor Id : 4413
Us Burst Receiver Model Number : BCM31610
Us Burst Receiver Driver Version : V11
Us Burst Receiver Serial Number : 00000000
Rpd Rcp Protocol Version : 1.0
Rpd Rcp Schema Version   : 1.0.13
Hw Revision              : 2.0
Current Sw Image Last Update : 2020-05-17 08:43:02.02
Current Sw Image Name     : RPD_V8_3_THROTTLE_20200516_103309.itb.sign.SSA
Current Sw Image Server Address : 192.0.2.21
Current Sw Image Server Type : IPV4
Current Sw Image Index    : 0
Asset Id                  : Asset-2
Vsp Selector              :
Status                     : Active

```

Updating the Default RPD Password

You should update the default RPD access credentials immediately after you log in to the RPD. From RPD 7.7, it is mandatory to update the SSH login password.

If you continue to use the default password, all downstream channels become inactive. A warning message appears of the Cisco cBR core and an event is generated for default password usage. The event is generated for RPD 6.7 and later. The RPD sends this event to the primary core to which it is connected.

The following message appears when you log in to the RPD y using the default credentials:

```

2020-01-13 04:48:26,584-rpd_logging.py-119-ERROR-0x80090807:Service Disabled - PLEASE CHANGE
RPD SSH PASSWORD IMMEDIATELY - default login credentials detected in use
2020-01-13 04:48:26,586-cli_main.py-216-WARNING-Default password detected in use

```

```

*****
***** SERVICE IMPACTING *****
***** PLEASE READ *****
*****

```

```

Default login credentials detected in use.
In order to enhance the security of your network,
default login credentials must be changed on this RPD.

```

```

@@@ RPD SERVICE HAS BEEN DISABLED !!! @@@

```

```

*****
***** CHANGE SSH PASSWORD *****
***** IMMEDIATELY *****
*****

```

```

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

```

```
SECURITY WARNING: ssh password login is accessible!
Please use pubkey login and set password login off!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

```
Welcome to Cisco R-PHY
```

```
R-PHY>
```

Check the current SSH account details using the following command. If you use the default credentials, you can see a similar output:

```
R-PHY#show ssh account
Account Num: 3
Current SSH Accounts:
admin *** Warning ! Default Password in Use ***
test
new
```

When the downstream port is inactive due to the use of default credentials, the OFDM channel and the QAM channel also become inactive. To check whether the downstream port is inactive, use the following command:

```
R-PHY#show downstream port configuration
Admin: UP
Muted: MUTED
BasePower: 21 dBmV
```

```
R-PHY#show downstream channel configuration
Chan State Frequency Type Annex Modulation Rate Interleave Power Muted

Chan State Type StartFreq Width PlcFreq CPrefix RollOff Interleave Spacing
Power Muted
158 UP OFDM 645000000 192000000 651000000 1024 128 16 50kHz
21.0 MUTED
```

*NOTE: Start frequency and channel width do not cover guardband override scenario.

Activate the Downstream Port

You can activate the downstream port using one of the following methods:

- Disable the SSH password and set up the RPD to use server generated SSH keys.
- Change the password for the admin user.
- Create a new user and delete the admin user.

Disable SSH Password

Disable the SSH password and set up the RPD to use server generated SSH keys.

1. Generate a new NMS key on SSH server

```
$ cat ~/.ssh/id_rsa.pub
$ ssh-keygen -t rsa
$ cat ~/.ssh/id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAtQCXVfMwRIwemejbTx0+U8taMq5n4Zetu
```

```
71xb+dtHV8Rr0wejiK1YJkT93n9hcBxsjHRu76bLp991+DDNL3+THljwnMQC1CsdvRmGXoe
GflmT9aTlGDf/ RW9ZyWY9t8Kep9VnANu2DWSoh0wg2pE49HFOJAbGfuFOvPEdwZGGDMQNws
Eq/3xAQjBxajQqfgu4IqjVzKoo4PM/xx9X4Z1aMwxs3Dvyn7L800o33mcDNsas13Ss1IjMSNfq
YpwOFvQve8c2onrYHUx2p3BwQOb/b0FzFQhZMTBxm/pDMXq/fkkD0uguklxOGnqAATMJsSHIN
0U0dvzbzhmrFRBBM4NzqQG5kNt7KvnWgx7HdalERvMyBC2MCGbFShmQFyWmHBHPPmLIxK98W
XutoR8fzsz+4hingZ4X9DMMNwTQ6WOzjuKq6iU= userid@example.cisco.com
```

2. Add this new NMS key to the RPD through RPD CLI

```
R-PHY#conf t
R-PHY(config)#ssh pubkey add ?
LINE          NMS's pubkey
R-PHY(config)#ssh pubkey add ssh-rsa AAAAB3NzaC1yc26876bhjdsK
EEEEAAAABlwAAAgErP3nFp0v0k3Nf4UvSTuOOQi2h0mAfAtQCXVfMriwemejbTx0+U8taM
q5n4Zetu71xb+dtHV8Rr0wejiK1YJkT93n9hcBxsjHRu76bLp991+DDNL3+THljwnMQC1
CsdvRmGXoeGflmT9aTlGDf/YfKxZMozMnR9q1GJFXlRAwGMsCR1llnV6IkFyh59P9Udkd
SSWv+QL8lCftWBmMnyt/CkqL98NK0Vp0gIYRv7UKCwhK40c8X7PhzxcmKVFTUv3bf9VIP
NA2esgzKDFp0JZkqCjrnXU1Xu0Oj8Twei7f0ytSrFvKuWp4XZbVDPwGH90BQR8gKHmq
urP3nFp0v0k3Nf4UvSTuOOQi2h0mAf+9wzm+ab4lToadUbMawHyFYyuU= xxx@xxx.xxx.com
R-PHY(config)#end
```

```
R-PHY#show ssh nms-pubkey ssh-rsa AAAAB3NzaC1yc2EAAAABlwAAAgEAtQCXVfM
riwemejbTx0+U8taMq5n4Zetu71xb+dtHV8Rr0wejiK1YJkT93n9hcBxsjHRu76bLp991
+DDNL3+THljwnMQC1CsdvRmGXoeGflmT9aTlGDf/YfKxZMozMnR9q1GJFXlRAwGMsCR1l
lnV6IkFyh59P9UdkdSSWv+QL8lCftWBmMnyt/CkqL98NK0Vp0gIYRv7UKCwhK40c8X7Ph
zxcmKVFTUv3bf9VIPNA2esgzKDFpRvMyBC2MCGbFShmQFyWmHBHPPmLIxK98WXutoR8fzsz
s+4hingZ4X9DMMNwTQ6WOzjuKq6iU= xxx@xxx.xxx.com
```

3. Disable RPD SSH password login

```
R-PHY#conf terminal
R-PHY(config)#ssh password ?
off          disable ssh password login
on          enable ssh password login
R-PHY(config)#ssh password off
Successfully Disabled Password, SoftReset in 10 seconds
```

Change the Password for the Admin User

```
R-PHY#config terminal
R-PHY(config)#ssh chpasswd admin
Please enter password for 'admin':
Please re-enter your password:
chpasswd: password for 'admin' changed

Successfully Changed from Default Password, SoftReset in 10 seconds
```

Create a New User and Delete the Admin User

```
R-PHY(config)#ssh add rpdadmin
Changing password for rpdadmin
New password:
Retype password:
passwd: password for rpdadmin changed by root
R-PHY(config)#ssh delete admin
Warning: Are you sure to delete this account? [No/Yes]
yes
delete account 'admin' successfully
R-PHY(config)#
```

Successfully Deleted user admin, SoftReset in 10 seconds



CHAPTER 3

Network Authentication

This document describes the Remote PHY device network authentication on the Cisco cBR Series Converged Broadband Router.

Finding Feature Information

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

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

- [Hardware Compatibility Matrix for Cisco Remote PHY Device, on page 19](#)
- [Information about Network Authentication, on page 20](#)
- [How to Enable Network Authentication, on page 20](#)

Hardware Compatibility Matrix for Cisco Remote PHY Device



Note Unless otherwise specified, the hardware components introduced in a given Cisco Remote PHY Device Software Release are supported in all subsequent releases.

Table 3: Hardware Compatibility Matrix for the Cisco Remote PHY Device

Cisco HFC Platform	Remote PHY Device
Cisco GS7000 Super High Output Node	Cisco 1x2 / Compact Shelf RPD Software 2.1 and Later Releases

Cisco HFC Platform	Remote PHY Device
Cisco GS7000 Super High Output Intelligent Node (iNode)	Cisco 1x2 / Compact Shelf RPD Software 4.1 and Later Releases Cisco Intelligent Remote PHY Device 1x2 <ul style="list-style-type: none"> • PID—iRPD-1X2= • PID—iRPD-1X2-PKEY=



Note The -PKEY suffix in the PID indicates units that enable the SCTE-55-2 Out-of-Band protocol support.

Information about Network Authentication

RPD must be able to operate in both authenticated and unauthenticated networks. Whether authentication is required for an RPD is determined by the network that it is connected to. In some cases, RPD is located in an untrusted network, and it must connect to devices inside the trusted network, which presents a potential security vulnerability. 802.1x is introduced to provide authentication services to eliminate the potential security issues.

802.1x is a Layer 2 protocol that uses EAP (Extensible Authentication Protocol) to provide authentication services. Following certificates are needed to use the network authentication:

- Cablelabs Root CA certificate: caRoot.pem
- CableLabs Device CA Certificate: deviceCA.pem
- RPD Certificate: rpdCert.pem, private key: rpd.key
- Cablelabs Service Provider CA Certificate: spCA.pem
- AAA Server Certificate: aaaCert.pem, private key: aaa.key

How to Enable Network Authentication

This section describes how to enable network authentication for RPD.

Installing Certificates in Radius Server

To install the certificate in Radius server, follow the steps below:

Step 1 Combine CA certificate for AAA server.

Example:

```
cat spCA.pem caRoot.pem > ca_root_srv.pem
```


Step 2 In freeRadius Server, copy "ca_root_srv.pem", "spCA.pem", "aaaCert.pem" and "aaa.key" to "/etc/freeradius/certs".

Configuring Radius Server

To install the certificate in RPD, follow the steps below:

Step 1 Define a new client in /etc/freeradius/clients.conf.

Example:

```
client rphytest_ng13 {
    ipaddr = 20.5.0.36
    secret = rphytest
    shortname = ng13_switch
    require_message_authenticator = yes
}
```

The "ipaddr" is the switch's management ip address.

Step 2 In "/etc/freeradius/eap.conf", change the following lines in "tls" to specify the server's private key file and certificate files.

Example:

```
tls {
    ...
    private_key_file = ${certdir}/aaa.key
    certificate_file = ${certdir}/aaaCert.pem
    CA_file = ${cadir}/ca_root_srv.pem
}
```

Step 3 Start radius in radius sever.

Example:

```
sudo freeradius
```

Make sure only one freeradius instance is running.

Configuring Switch

To configure the switch, follow the steps below:



Note This procedure is for Catalyst 3750 switch, other switch may use different commands.

Step 1 Add the following configuration in global configuration mode.

Example:

```
dot1x system-auth-control /* enable 802.1x */
aaa new-model
```

```
aaa authentication dot1x default group radius
radius-server host 10.79.41.103 auth-port 1812 key rphytest
```

Step 2 Add the following configuration under interface which connects to RPD.

Example:

```
authentication port-control auto
dot1x pae authenticator
```

Verifying Authentication Status

To displays dot1x authentication information for RPD, use the **show dot1x** command as shown in the following example:

```
Router# show dot1x summary
  Interface      Core-id      EAP_Received  Status
  vbh0           CORE-3415960568  True          UP

Router# show dot1x detail
Interface      Core-id      EAP_Received  Status
vbh0           CORE-3415960568  True          UP
ssid=01:80:c2:00:00:03
freq=0
ssid=
id=0
mode=station
pairwise_cipher=NONE
group_cipher=NONE
key_mgmt=IEEE 802.1X (no WPA)
wpa_state=COMPLETED
ip_address=30.85.40.47
address=00:04:9f:00:03:73
Supplicant PAE state=AUTHENTICATED
suppPortStatus=Authorized
EAP state=SUCCESSselected
Method=13 (EAP-TLS)EAP TLS
cipher=ECDHE-RSA-AES256-SHA
tls_session_reused=0
eap_session_id=0c5379e5c46014cc924ac1151521ba6a1498f919d5e881a701b7272be7f812e7e5a75881768c74d311795a3b1f0e37bfa7fff7dc4685c36f216ec59850
uuid=ab722cfb-84dc-5835-a905-edfec20f78c3
```



CHAPTER 4

Synchronizing Time on Cisco Remote PHY Devices

This section explains how to synchronize time on the Remote PHY (R-PHY) devices and CCAP core of the Cisco cBR Router.

- [Hardware Compatibility Matrix for Cisco Remote PHY Device, on page 23](#)
- [Information about Time Synchronization, on page 24](#)
- [How to Configure Time Synchronization, on page 25](#)
- [Configuration Examples, on page 32](#)
- [Feature Information for Synchronizing Time on R-PHY Devices, on page 33](#)

Hardware Compatibility Matrix for Cisco Remote PHY Device



Note Unless otherwise specified, the hardware components introduced in a given Cisco Remote PHY Device Software Release are supported in all subsequent releases.

Table 4: Hardware Compatibility Matrix for the Cisco Remote PHY Device

Cisco HFC Platform	Remote PHY Device
Cisco GS7000 Super High Output Node	Cisco 1x2 / Compact Shelf RPD Software 2.1 and Later Releases
Cisco GS7000 Super High Output Intelligent Node (iNode)	Cisco 1x2 / Compact Shelf RPD Software 4.1 and Later Releases Cisco Intelligent Remote PHY Device 1x2 <ul style="list-style-type: none">• PID—iRPD-1X2=• PID—iRPD-1X2-PKEY=



Note The -PKEY suffix in the PID indicates units that enable the SCTE-55-2 Out-of-Band protocol support.

Information about Time Synchronization

In a Remote PHY system, synchronizing its local timestamp and reference frequency to the cable converged access platform core function (CCAP Core) is important. The protocol used for this feature, the Precision Time Protocol (PTP), helps in synchronizing time between a CCAP core function and a series of remote PHY devices (RPD) that enable R-PHY and provides support for converged DOCSIS, video, and out-of-band (OOB) services.

Cisco CBR-8 supports PTP Ordinary Clock (OC) slave mode, in which the PTP slave ports are from the backhaul 10GE Ethernet ports or the management Ethernet ports of SUP PIC.

Remote DTI

Remote DOCSIS Timing Interface (R-DTI) is the network synchronization protocol used between CCAP-core and R-PHY. When traffic from the CCAP-Core is received on the downstream receiver, the following processes occur:

- Terminates DEPI framing
- Extracts the payload, frames it, modulates, and transmits it out

During the upstream process, the signal is received from the coax and the system demodulates it. From the FEC payload, the DOCSIS frames are extracted and placed in the UEPI encapsulation. The frames are then transmitted through the upstream transmitter to the CCAP core. A local CPU manages DEPI and GCP control planes, and interfaces with network management. A clocking circuit interfaces with the R-DTI and manages clocking for the R-DTI entity.

The GS7000 R-PHY supports map re-stamp option.

Restrictions for Configuring Time Synchronization

The following restrictions are applicable to configuring time synchronization on Cisco cBR-8.

- Cisco cBR-8 supports PTP slave on both SUP-PIC and DPIC.
- Cisco RPD PTP does not support pass-through mode. Pass-through mode means RPDs are communicating with PTP server through cBR-8, and cBR-8 is PTP unaware of the communication between RPDs with PTP server.

How to Configure Time Synchronization

Configure Time Interface and PTP Domain

To configure time interface and PTP domain, use the following procedure.

```
enable
configure terminal
interface type [slot_#/]port_#
interface Loopback1588
    ip address <IP Address/subnet>

interface TenGigabitEthernet<slot/port>
    ip address <IP Address/subnet>

ip route < PTP master IP Address/subnet> < loopback IP Address>

ptp clock ordinary domain 0 (This is for CBR PTP connection)
    servo tracking-type R-DTI
    clock-port slave-from-903 slave
    delay-req interval -4
    sync interval -5
    sync one-step
    transport ipv4 unicast interface Lo1588 negotiation
    clock source < PTP master loopback IP Address>
```

The following table explains the parameters used in this example:

Table 5: Parameters for Time Interface and PTP Domain Configuration

Parameter	Description	Value Range	Default Value
ptp r-dti [id]		1-64	
description	R-DTI name or description		
ptp-domain [id]	Domain number of IEEE 1588	0-127	
local-priority [value]	Set local priority	128	128
priority1 [value]	Set priority1	0-255	128
priority2 [value]	Set priority2	0-255	255
mode [value]	R-DTI mode	other, subordinate primary	subordinate
profile [value]	Set PTP ITU-T profile	default/G.8275.2	default
clock-port [id]	Configure clock port	1-32	
state [value]	Set Ethernet port admin status	other, up, down, testing	up

Parameter	Description	Value Range	Default Value
ethenet [value]	Set Ethernet port for clock port	0-32	The default value is clock port index
clock source [ip] gateway [ip]	Set clock address	ipv4 address, ipv6 address	
clock alternate-first	Select alternate source first		
transport [value]	Set transport encapsulation	other, ipv4, ipv6	ipv4
transport cos [value]	COS of 802.1Q	0-7	6
transport dscp [value]	DSCP of IP differentiated services	0-63	47
local-priority [value]	Set local priority	1-255	128
sync interval [value]	Set an interval for sync packets	0-7(-7 -0)	
announce interval [value]	Set an interval for announcement packets	0-3(-3 -0)	
delay-req interval [value]	Set an interval for PTP delay-req packets	0-7(-7 -0)	
announce timeout [value]	Set timeout interval for announcement packets	3-255	
unicast grant-duration [value]	Set the grant duration time in seconds for unicast	60-1000	300
description	Clock port name or description		

Verifying Time Interface and PTP Domain Configuration

The following example shows how to verify the time interface and PTP domain configuration:

```
Router# show ptp clock running domain 0
Load for five secs: 5%/2%; one minute: 6%; five minutes: 6%
No time source, 15:16:20.421 CST Wed Mar 15 2017

                PTP Ordinary Clock [Domain 0]
State           Ports Pkts sent Pkts rcvd Redundancy Mode
PHASE_ALIGNED  1      3687693  11177073 Hot standby
                PORT SUMMARY
                PTP Master
Name           Tx Mode Role  Transport State Sessions Port Addr
slave-from-903 unicast slave Lo1588  Slave 2      10.10.10.11
```

```

SESSION INFORMATION
slave-from-903 [Lo1588] [Sessions 2]
Peer addr      Pkts in Pkts out In Errs Out Errs
10.10.10.11    5588900 1843789 0      0
10.10.10.12    5588173 1843904 0      0

```

Configure RPD PTP Connection

To configure RPD PTP connection, use the following commands.

```

enable
configure terminal
interface type [slot_#/]port_#
ptp r-dti 1 (RPD PTP connection)
ptp-domain 0 /* same domain number with ptp server */
  clock-port 1
    ethernet 1 /* default value is same index with clock-port index, for RPD, ethernet
1=vbh0, ethernet 2=vbh1 */
      clock source ip <IP Address> gateway ip <IP Address>
      clock source ip <IP Address> gateway ip <IP Address> alternate
      !--<clock-source is PTP master loopback ip, gw is the next hop to reach the ptp master
>--!

```

Verifying RPD PTP Connection Configuration

The following example shows how to verify the RPD PTP Connection configuration:

```

Router# show ptp clock 0 config
Domain/Mode      : 0/OC_SLAVE
Priority 1/2/local : 128/255/128
Profile          : 001b19000100-000000 E2E
Total Ports/Streams : 1 /2
--PTP Port 1, Enet Port 1 ----
Port local Address :10.10.10.11
Unicast Duration :300 Sync Interval : -4
Announce Interval : 0 Timeout : 11
Delay-Req Intreval : -4 Pdelay-req : -4
Priority local :128 COS: 6 DSCP: 47
==Stream 0 : Port 1 Master IP: 10.10.10.11
==Stream 1 : Port 1 Master IP: 10.10.10.11

```

Associate R-DTI with RPD

To associate R-DTthe local prefix SID associated to the segment ID, use the following commands.

```

enable
configure terminal
interface type [slot_#/]port_#
cable rpd node1
identifier 0044.4f04.0044 (node vbh0 mac)
  core-interface Te3/1/0
  rpd-ds 0 downstream-cable 3/0/0 profile 3
  rpd-us 0 upstream-cable 3/0/0 profile 3
r-dti 1
rpd-event profile 0
rpd-55d1-us-event profile 0

```

Verifying Associating R-DTI with RPD

The following example shows how to verify whether the RPD is associated to R-DTI:

```
Router# show running-config
Load for five secs: 8%/2%; one minute: 9%; five minutes: 9%
Time source is user configuration, 11:00:17.381 CST Wed Mar 22 2017
Building configuration...
Current configuration : 107879 bytes
!
! Last configuration change at 10:59:23 CST Wed Mar 22 2017
!
version 16.6
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service internal
no platform punt-keepalive disable-kernel-core
platform ipcc1 log-history 0
platform punt-policer 10 10
platform punt-policer 10 10 high
platform punt-policer 80 10
platform punt-sbr1 subscriber rate no-drop
platform shell
!
hostname RphyNode-L09
!
boot-start-marker
boot system harddisk:cbrsup-universalk9.16.05.01prd9.SPA.bin
boot-end-marker
!
!
----
!
cable tag 10
  name docsis1.0
  docsis-version docsis10
!
cable tag 11
  name docsis1.1
  docsis-version docsis11
!
-----
cable load-balance docsis-group 1
  restricted
  upstream Upstream-Cable 3/0/3 us-channel 0-3
  method utilization
  threshold load 15
  threshold load minimum 2
  policy pure-ds-load
  init-tech-list 4
  interval 60
  tag docsis1.0
  tag docsis1.1
  tag docsis2.0
  tag docsis3.0
!
---
cable metering ipdr-d3 session 1 type 1
cable metering source-interface TenGigabitEthernet4/1/1
cable modem remote-query 30 public
cable modem vendor 00.02.00 "Apache-ACB"
cable modem vendor E8.6D.52 "Motorola"
cable modem vendor 00.1F.E1 "Ambit"
cable modem vendor 00.1F.E2 "Ambit"
```



```
cable modem vendor 00.D0.DD "Sunrise"
!
!
----
!
no network-clock synchronization automatic
!
ptp clock boundary domain 0
  servo tracking-type R-DTI
  clock-port slave-from-903 slave
  delay-req interval -4
  sync interval -5
  sync one-step
  transport ipv4 unicast interface Lol1588 negotiation
  clock source 10.10.10.11
  clock source 192.168.0.0
  clock-port master-local master
  transport ipv4 unicast interface Lol1588 negotiation
!
-----
r-dti 2
  rpd-event profile 0
  rpd-55dl-us-event profile 0
!
ptp r-dti 2
  ptp-domain 0
  clock-port 1
    clock source ip 10.10.10.11
    clock source ip 192.168.0.0 alternate
!
ptp r-dti 3
  ptp-domain 0
  clock-port 1
    clock source ip 10.10.10.11
    clock source ip 192.168.0.0 alternate
!
ptp r-dti 10
  ptp-domain 0
  clock-port 1
    clock source ip 10.10.10.11
    clock source ip 192.168.0.0 alternate
  announce interval -3
  announce timeout 3
!
ptp r-dti 11
  ptp-domain 0
  priority1 101
  priority2 102
  local-priority 100
  clock-port 2
    ethernet 1
    clock alternate-first
    clock source ip 10.10.10.11
    clock source ip 192.168.0.0 alternate
  transport cos 0
  transport dscp 63
  sync interval -1
  announce timeout 255
  delay-req interval -7
  unicast grant-duration 60
  local-priority 255
!
ptp r-dti 12
  ptp-domain 0
```

```

clock-port 1
  ethernet 0
  clock source ip 10.10.10.11
!
ptp r-dti 60
  ptp-domain 0
!
cable video
!
end

```

Verifying PTP Clock Functioning

To verify whether the PTP Clock is running, use the following commands:

```

Router#show ptp clock running
Load for five secs: one minute: 5%; five minutes:
Time source is NTP, 14 CST Fri Feb 17 2017
PTP Ordinary clock [Domain 0]
State          Ports pkts sent pkts rcvd Redundancy Mode
PHASE-ALIGNED 1      7339500  22245593  Hot standby
  Port Summary
Name          Tx Mode Role  Transport State Sessions PTP Master Port Addr
slave-from-903 unicast slave  L01588  Slave 2      10.10.10.11

```

Verifying PTP Clock Running Domain

The following example shows how to verify the PTP clock running domain:

```

Router#show ptp clock running domain 0
Load for five secs: 5%/2%; one minute: 6%; five minutes: 6%
No time source, 15:16:20.421 CST Wed Mar 15 2017
          PTP Ordinary Clock [Domain 0]
State          Ports Pkts sent Pkts rcvd Redundancy Mode
PHASE_ALIGNED 1      3687693  11177073  Hot standby
  PORT SUMMARY
          PTP Master
Name          Tx Mode Role  Transport State Sessions Port Addr
slave-from-903 unicast slave  L01588  Slave 2      10.10.10.11

          SESSION INFORMATION
slave-from-903 [L01588] [Sessions 2]
Peer addr      Pkts in Pkts out In Errs Out Errs
10.10.10.11    5588900 1843789 0      0
192.168.0.10   5588173 1843904 0      0

```

Verifying Time Sync State

To verify the status of time synchronization, use the show ptp clock <n> state command as given in the following example:

```

Router# show ptp clock 0 state
apr state      : PHASE_LOCK
clock state    : SUB_SYNC
current tod    : 1485414295   Thu Jan 26 07:04:55 2017
active stream  : 0
==stream 0    :
  port id     :                0
  master ip   :                10.10.10.11
  stream state :                PHASE_LOCK

```

```

Master offset :          -405
Path  delay   :          -17071
Forward delay :          -17476
Reverse delay :          -16623
Freq offset  :          -291143
1Hz  offset  :           -676
==stream  1  :
port id      :            0
master ip    :          192.168.0.11
stream state :          PHASE_LOCK
Master offset :          -369
Path  delay   :          -1619
Forward delay :          -1988
Reverse delay :          -1260
Freq offset  :          -297905
1Hz  offset  :           -664

```

Verifying Time Sync Statistics

To verify the statistics of the time synchronization, use the `show ptp clock <n> state` command as given in the following example:

```

Router# show ptp clock 0 statistics
AprState 4 :
2@0-00:06:51.568 1@0-00:06:41.930 0@0-00:04:17.925
4@0-00:03:58.724
ClockState 5 :
5@0-00:07:12.640 4@0-00:07:10.182 3@0-00:07:06.825
2@0-00:06:51.825 1@0-00:06:51.530
BstPktStrm 1 :
0@0-00:06:42.029
SetTime 1 :
1000000000@0-00:04:00.045
StepTime 1 :
125126755@0-00:06:14.670
AdjustTime 64 :
-676@0-07:34:32.546 -733@0-07:33:31.545 -838@0-07:32:30.546
-892@0-07:31:29.545 -935@0-07:30:28.545 -1033@0-07:29:27.545
-914@0-07:28:26.546 916@0-07:26:24.545 2507@0-07:25:18.170
streamId msgType rx rxProcessed lost tx
0 SYNC 433439 433439 4294574083 0
0 DELAY REQUEST 0 0 0 433439
0 P-DELAY REQUEST 0 0 0 0
0 P-DELAY RESPONSE 0 0 0 0
0 FOLLOW UP 0 0 0 0
0 DELAY RESPONSE 433437 433437 4294548766 0
0 P-DELAY FOLLOWUP 0 0 0 0
0 ANNOUNCE 27098 27098 0 0
0 SIGNALING 285 285 0 285
0 MANAGEMENT 0 0 0 0
TOTAL 894259 894259 8589122849 433724
1 SYNC 433435 433435 4294574085 0
1 DELAY REQUEST 0 0 0 433439
1 P-DELAY REQUEST 0 0 0 0
1 P-DELAY RESPONSE 0 0 0 0
1 FOLLOW UP 0 0 0 0
1 DELAY RESPONSE 10351 10351 4104 0
1 P-DELAY FOLLOWUP 0 0 0 0
1 ANNOUNCE 27098 27098 4294901760 0
1 SIGNALING 285 285 0 285
1 MANAGEMENT 0 0 0 0
TOTAL 471169 471169 8589479949 433724

```

Configuration Examples

This section provides examples for configuring Cisco cBR for time synchronization.

Example: Configure Time Interface and PTP Domain

The following example shows how to configure time interface and PTP domain:

```
enable
configure terminal
interface Loopback1588
ip address 10.10.10.11 255.255.255.224

interface TenGigabitEthernet5/1/3 (connect to PTP primary)
ip address 192.168.0.13 255.255.255.224

ip route 10.10.10.11 255.255.255.224 192.168.0.12 (route to PTP primary loopback ip)

ptp clock ordinary domain 0 (This is for cbr ptp connection)
servo tracking-type R-DTI
clock-port slave-from-903 slave
delay-req interval -4
sync interval -5
sync one-step
transport ipv4 unicast interface Lo1588 negotiation
clock source 10.10.1.11 (PTP primary loopback ip)
```

Example: Configure RPD PTP Connection

The following example shows how to configure RPD PTP connection:

```
enable
configure terminal
ptp r-dti 1
ptp-domain 0
mode slave
priority1 128
priority2 255
local-priority 128
clock-port 1
  ethernet 1
  ...
clock-port 2
  ethernet 2
  ...
clock-port 1
  ethernet 1
  state up
  transport ipv4
  clock source ip 10.10.1.12 gw 10.10.1.1
  clock source ip 192.168.0.0 gateway ip 10.10.1.2 alternate
  transport cos 6
  transport dscp 47
  sync interval -4
  announce interval 0
  announce timeout 11
  delay-req interval -4
  unicast grant-duration 300
  local-priority 128
```

Example: Associate R-DTI with RPD

The following example shows how to associate R-DTI with RPD:

```
enable
configure terminal
cable rpd node1
  identifier 0004.9f03.0061 (node vbh0 mac)
  core-interface Te3/1/0
  rpd-ds 0 downstream-cable 3/0/0 profile 3
  rpd-us 0 upstream-cable 3/0/0 profile 3
r-dti 1
  rpd-event profile 0
  rpd-55d1-us-event profile 0
```

Feature Information for Synchronizing Time on R-PHY Devices

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



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

Table 6: Feature Information for Synchronizing Time on R-PHY Devices

Feature Name	Releases	Feature Information
Synchronizing Time on R-PHY Devices	Cisco 1x2 / Compact Shelf RPD Software 3.1	This feature was integrated into the Cisco Remote PHY Device.



CHAPTER 5

DEPI/UEPI/L2TP integration with Cisco Remote PHY Device

This document describes how to configure the DEPI/UEPI/L2TP integration with RPD on the Cisco cBR Series Converged Broadband Router.

Finding Feature Information

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

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

- [Hardware Compatibility Matrix for Cisco Remote PHY Device](#), on page 35
- [Information about DEPI/UEPI/L2TP integration with RPD](#), on page 36
- [How to Configure DEPI/UEPI/L2TP integration with RPD](#), on page 36
- [Feature Information for DEPI/UEPI/L2TP integration with RPD](#), on page 38

Hardware Compatibility Matrix for Cisco Remote PHY Device



Note Unless otherwise specified, the hardware components introduced in a given Cisco Remote PHY Device Software Release are supported in all subsequent releases.

Table 7: Hardware Compatibility Matrix for the Cisco Remote PHY Device

Cisco HFC Platform	Remote PHY Device
Cisco GS7000 Super High Output Node	Cisco 1x2 / Compact Shelf RPD Software 2.1 and Later Releases

Cisco HFC Platform	Remote PHY Device
Cisco GS7000 Super High Output Intelligent Node (iNode)	Cisco 1x2 / Compact Shelf RPD Software 4.1 and Later Releases Cisco Intelligent Remote PHY Device 1x2 <ul style="list-style-type: none"> • PID—iRPD-1X2= • PID—iRPD-1X2-PKEY=



Note The -PKEY suffix in the PID indicates units that enable the SCTE-55-2 Out-of-Band protocol support.

Information about DEPI/UEPI/L2TP integration with RPD

DEPI

Downstream External PHY Interface (DEPI) is the downstream interface between the CCAP Core and the RPD. R-DEPI is based on DEPI. More specifically, it is an IP pseudowire between the MAC and PHY in an MHA v2 system that contains both a data path for DOCSIS frames, video packets, and OOB packets, as well as a control path for setting up, maintaining, and tearing down sessions.

UEPI

Upstream External PHY Interface (UEPI) is the upstream interface between the RPD and the CCAP Core. Like DEPI, it is an IP pseudowire between the PHY and MAC in an MHA v2 system that contains both a data path for DOCSIS frames, and a control path for setting up, maintaining, and tearing down sessions.

How to Configure DEPI/UEPI/L2TP integration with RPD

This section describes how to configure DEPI/UEPI/L2TP integration with RPD.

Configuring depi-class/l2tp-class Pair

It's not permitted to change the default l2tp-class configuration (rphy-l2tp-global-class) for R-DEPI by user, because the parameter values are fine tuned to accommodate most common cases.

If user wants to use parameter values other than the default ones, they can use manually defined depi-class/l2tp-class pair. To do so, follow the example below:

```
Router# configure terminal
Router(config)# l2tp-class l2tp_demo
Router(config-l2tp-class)#exit
Router(config)# depi-class depi_demo
Router(config-depi-class)#l2tp-class l2tp_demo
Router(config-depi-class)#exit
```



```
Router(config)#cable rpd node
Router(config-rpd)#core-interface Tel/1/7
Router(config-rpd-core)#depi depi_demo /* Be sure to configure when the RPD core is offline*/
Router(config-rpd-core)#end
```

Verifying depi-class/l2tp-class Pair Configuration

To verifying depi-class/l2tp-class pair configuration, use the **show running-config** command as shown in the example below:

```
Router# show running-config | section rpd
alias exec scr show cable rpd
cable rpd node
identifier 0004.9f00.0901
core-interface Tel/1/7
  principal
  rpd-ds 0 downstream-cable 1/0/31 profile 155
  rpd-us 0 upstream-cable 1/0/63 profile 100
  depi depi_demo
r-dti 1
rpd-event profile 0
rpd-55dl-us-event profile 0
```

When the RPD core is online, use the **show l2tp tunnel** command as shown in the example below:

```
Router# show l2tp tunnel
LocTunID  RemTunID  Remote Name  State  Remote Address  Sessn L2TP Class/
Count  VPDN Group
2375973187 4191827509 OpenRPD      est    120.100.1.20   86    l2tp_demo
2982856686 2223617345 OpenRPD      est    120.100.1.20   86    l2tp_demo
```

Verifying the RPD Status

To verify the RPD status, use the **show cable rpd** command as shown in the example below:

```
Router# show cable rpd
Load for five secs: 6%/1%; one minute: 5%; five minutes: 5%
No time source, *04:52:03.936 UTC Tue Jan 17 2017

MAC Address      IP Address      I/F      State      Role  HA   Name
0004.9f00.0901  91.0.10.10     Tel/1/0  init(l2tp)  Pri  Act  node
```

Display DEPI Related Information

To display the Downstream External PHY Interface (DEPI) related information, use the command as shown in the following example:

```
Router#show cable rpd depi

DEPI Tunnel and Session Information Total tunnels 1 sessions 26
LocTunID  RemTunID  Remote Device  State  Remote Address  Sessn L2TP Class
Count
338514820 671581873  0004.9f00.0901 est    10.10.10.11    26    rphy-l2tp-gl...

LocID      RemID      Pseudowire      State  Last Chg Uniq ID  Type Mode RemSt
0x41040008 0x00000B02 US1/0/0:2(R)    est    00:34:57 21    P    PSP  UP
0x41010000 0x00000600 US1/0/0:0(D)    est    00:34:57 11    P    PSP  UP
0x00002006 0x00000405 DS1/0/0:5       est    00:34:57 6     P    PSP  UP
0x00002004 0x00000403 DS1/0/0:3       est    00:34:57 4     P    PSP  UP
```

```

0x4100000C 0x00000D03 US1/0/0:3 (M)    est    00:34:57 23    P    PSP    UP
0x00002002 0x00000401 DS1/0/0:1    est    00:34:57 2    P    PSP    UP
0x00002007 0x00000406 DS1/0/0:6    est    00:34:57 7    P    PSP    UP
0x00002008 0x00000407 DS1/0/0:7    est    00:34:57 8    P    PSP    UP
0x4101000C 0x00000603 US1/0/0:3 (D)    est    00:34:57 24    P    PSP    UP
0x41000004 0x00000D01 US1/0/0:1 (M)    est    00:34:57 15    P    PSP    UP
0x00002001 0x00000400 DS1/0/0:0    est    00:34:57 1    P    PSP    UP
0x41080008 0x00000F02 US1/0/0:2 (S)    est    00:34:57 22    P    PSP    UP
0x41010004 0x00000601 US1/0/0:1 (D)    est    00:34:57 16    P    PSP    UP
0x41020000 0x00000800 US1/0/0:0 (B)    est    00:34:57 12    P    PSP    UP
0x00002009 0x00000408 DS1/0/0:8    est    00:34:57 9    P    PSP    UP
0x41010008 0x00000602 US1/0/0:2 (D)    est    00:34:57 20    P    PSP    UP
0x41000008 0x00000D02 US1/0/0:2 (M)    est    00:34:57 19    P    PSP    UP
0x4108000C 0x00000F03 US1/0/0:3 (S)    est    00:34:57 26    P    PSP    UP
0x00002003 0x00000402 DS1/0/0:2    est    00:34:57 3    P    PSP    UP
0x41080000 0x00000F00 US1/0/0:0 (S)    est    00:34:57 14    P    PSP    UP
0x41040004 0x00000B01 US1/0/0:1 (R)    est    00:34:57 17    P    PSP    UP
0x41080004 0x00000F01 US1/0/0:1 (S)    est    00:34:57 18    P    PSP    UP
0x41000000 0x00000D00 US1/0/0:0 (M)    est    00:34:56 10    P    PSP    UP
0x00002005 0x00000404 DS1/0/0:4    est    00:34:56 5    P    PSP    UP
0x4104000C 0x00000B03 US1/0/0:3 (R)    est    00:34:56 25    P    PSP    UP
0x41040000 0x00000B00 US1/0/0:0 (R)    est    00:34:56 13    P    PSP    UP

```

```
outer#show cable rpd 0004.9f03.0214 te7/1/0 depi tunnel
```

```
Load for five secs: 7%/2%; one minute: 6%; five minutes: 6%
No time source, *12:41:44.228 CST Mon Mar 20 2017
```

```

LocTunID   RemTunID   Remote Device   State   Remote Address   Sessn L2TP Class
Count
3388764998 1054297851 0004.9f03.0214 est    10.10.10.11     29    rphy-l2tp-gl...

```

Table 8: show cable rpd depi Field Descriptions

Field	Description
LocID	Local session ID.
RemID	Remote session ID.
US1/0/0:2(R)	US means UEPI session, DS means DEPI session. This string means UEPI session on line card slot 1, controller 0, rf-channel 2.
est in State	Established state.
P in Type	On primary line card.

Feature Information for DEPI/UEPI/L2TP integration with RPD

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



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

Table 9: Feature Information for DEPI/UEPI/L2TP integration with RPD

Feature Name	Releases	Feature Information
DEPI/UEPI/L2TP integration with RPD	Cisco 1x2 / Compact Shelf RPD Software 3.1	This feature was integrated into the Cisco Remote PHY Device.



CHAPTER 6

DEPI Latency Measurement

This document describes how to configure the DEPI latency measurement on the Cisco cBR Series Converged Broadband Router.

Finding Feature Information

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

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

- [Hardware Compatibility Matrix for Cisco Remote PHY Device, on page 41](#)
- [Information about DEPI Latency Measurement, on page 42](#)
- [How to Configure DLM, on page 42](#)
- [Example: DLM Configuration, on page 43](#)
- [Feature Information for DLM, on page 43](#)

Hardware Compatibility Matrix for Cisco Remote PHY Device



Note Unless otherwise specified, the hardware components introduced in a given Cisco Remote PHY Device Software Release are supported in all subsequent releases.

Table 10: Hardware Compatibility Matrix for the Cisco Remote PHY Device

Cisco HFC Platform	Remote PHY Device
Cisco GS7000 Super High Output Node	Cisco 1x2 / Compact Shelf RPD Software 2.1 and Later Releases

Cisco HFC Platform	Remote PHY Device
Cisco GS7000 Super High Output Intelligent Node (iNode)	Cisco 1x2 / Compact Shelf RPD Software 4.1 and Later Releases Cisco Intelligent Remote PHY Device 1x2 <ul style="list-style-type: none"> • PID—iRPD-1X2= • PID—iRPD-1X2-PKEY=



Note The -PKEY suffix in the PID indicates units that enable the SCTE-55-2 Out-of-Band protocol support.

Information about DEPI Latency Measurement

The DEPI Latency Measurement (DLM) packet is a specific type of data packet used for measuring the network latency between the CCAP core and the RPD. There are two types of DLM packets, ingress DLM packet and egress DLM packet. The ingress DLM measures the latency between the CCAP core and the ingress point in the RPD, and the egress DLM measures the latency between the CCAP core and the egress point of the RPD. For now, only the ingress DLM is supported. Egress DLM will be supported in the future if required.

How to Configure DLM

This section describes how to configure DLM on Cisco cBR-8.

Configuring DLM

To configure DLM, complete the following procedure. DLM is disabled by default, only enabled when configured.

```

configure terminal
cable rpd name
core-interface interface_name
network-delay dlm interval_in_seconds
  
```

Verifying DLM Configuration

To verify the DLM configuration, use the **show cable rpd dlm** command as shown in the example below:

```

Router# show cable rpd 0000.bbaa.0002 dlm
Load for five secs: 4%/1%; one minute: 4%; five minutes: 4%
Time source is NTP, 13:12:36.253 CST Sun Jan 1 2017
DEPI Latency Measurement (ticks) for 0000.bbaa.0002
  Last Average DLM:          4993
  Average DLM (last 10 samples): 4990
  Max DLM since system on:   5199
  
```

```

Min DLM since system on:      4800
Sample #      Latency (usecs)
x-----x-----
0              491
1              496
2              485
3              492
4              499
5              505
6              477
7              474
8              478
9              471

```

The table below shows descriptions for the fields displayed by this command:

Table 11: show cable rpd dlm Field Descriptions

Field	Description
Last Average DLM	It means the last time average DLM (AD). At first, the Last Average DLM (LAD) is always 0, when the absolute value of (LAD - AD) exceeds or equal to 75us, LAD will be updated to be the value of AD, MAP advance triggered to update, AD will keep updating with the last (latest) 10 samples.

Example: DLM Configuration

The following example shows how to configure DLM:

```

Router# configure terminal
Router(config)#cable rpd 1
Router(config-rpd)#core-interface tenGigabitEthernet 3/1/0
Router(config-rpd-core)#network-delay dlm 10

```

Feature Information for DLM

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



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

Table 12: Feature Information for DLM

Feature Name	Releases	Feature Information
DEPI Latency Measurement	Cisco 1x2 / Compact Shelf RPD Software 3.1	This feature was integrated into the Cisco Remote PHY Device.



CHAPTER 7

Multiple Cores

This document describes the multiple cores in the Remote PHY system.

Finding Feature Information

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

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

- [Hardware Compatibility Matrix for Cisco Remote PHY Device, on page 45](#)
- [Information about Multiple Cores, on page 46](#)
- [How to Configure Multiple Cores, on page 46](#)

Hardware Compatibility Matrix for Cisco Remote PHY Device



Note Unless otherwise specified, the hardware components introduced in a given Cisco Remote PHY Device Software Release are supported in all subsequent releases.

Table 13: Hardware Compatibility Matrix for the Cisco Remote PHY Device

Cisco HFC Platform	Remote PHY Device
Cisco GS7000 Super High Output Node	Cisco 1x2 / Compact Shelf RPD Software 2.1 and Later Releases

Cisco HFC Platform	Remote PHY Device
Cisco GS7000 Super High Output Intelligent Node (iNode)	Cisco 1x2 / Compact Shelf RPD Software 4.1 and Later Releases Cisco Intelligent Remote PHY Device 1x2 <ul style="list-style-type: none"> • PID—iRPD-1X2= • PID—iRPD-1X2-PKEY=



Note The -PKEY suffix in the PID indicates units that enable the SCTE-55-2 Out-of-Band protocol support.

Information about Multiple Cores

The RPD can be managed by more than one CCAP core. An RPD is controlled by exactly one principal CCAP core and zero or more auxiliary CCAP core(s). Each CCAP core manages a subset of RPD resources, e.g., particular channels or RF ports.

Principal core is responsible for the configuration of common parameters for the RPD and for certain device management functions. Principal core can provide DOCSIS, video or OOB service. Auxiliary cores are responsible for providing video or OOB services. They are restricted to the resource set assigned to them by the principal core.

Restrictions for Multiple Cores Configuration

The following restrictions are applicable to multiple cores configuration:

- Maximum four cores are supported.
- DOCSIS controllers can only be configured to principal core, while video controllers can be configured to all cores.
- Only one core can be principal, the rest will be auxiliary.
- Principal core needs to be configured explicitly.
- At least one DOCSIS downstream controller and one upstream controller are needed for principal core.
- No upstream controller for auxiliary core and at least one downstream controller is needed for auxiliary core.
- Only single CMTS is supported.
- No downstream frequency and channel id overlap is allowed for all the cores.

How to Configure Multiple Cores

This section describes how to configure multiple cores on Cisco cBR-8.

Configuring Multiple Cores

To configure the multiple cores, follow the example below:

```
Router(config)# cable rpd sjc_block22 /* unique name for each rpd */
Router(config-rpd)# description rpd for sjc block 22
Router(config-rpd)# identifier 1122.3344.5566 /* unique id for each rpd.*/
Router(config-rpd)# rpd-ds 0 power-level 5 /* DS max-carrier and power-level info */
Router(config-rpd)# rpd-ds 0 dedicated-cw-tone cw1 /* DS pilot tone info */
Router(config-rpd)# core-interface Te3/1/0 /* Core side interface (D-PIC interface) for
services below */
Router(config-rpd-core)# principal /* Specify the principal core */
Router(config-rpd-core)# rpd-ds 0 controller downstream-cable 3/0/0 profile 100 /* DS docsis
channel config*/
Router(config-rpd-core)# rpd-ds 0 controller downstream-cable 3/0/1 profile 200 /* DS docsis
channel config*/
Router(config-rpd-core)# rpd-ds 0 downstream-cable 3/0/2 profile 300 /* DS video channel
config*/
Router(config-rpd-core)# rpd-ds 0 downstream-cable 3/0/3 profile 400 /* DS video channel
config*/
Router(config-rpd-core)# rpd-us 0 upstream-cable 3/0/0 profile 101 /* US 0 docsis channel
config*/
Router(config-rpd-core)# rpd-us 1 upstream-cable 3/0/1 profile 101 /* US 1 docsis channel
config*/
Router(config-rpd-core)# depi depi_rpd_block22 /* RPD DEPI configuration.*/
Router(config-rpd-core)# exit
Router(config-rpd)# core-interface Te9/1/1 /* Support multiple core-interface for cases
such as video is using separate LC*/
Router(config-rpd-core)# rpd-ds 0 downstream-cable 9/0/1 profile 200 /* DS video channel
config*/
Router(config-rpd-core)# depi depi_rpd_block22 /* RPD DEPI configuration.*/
Router(config-rpd-core)# exit
Router(config-rpd)# r-dti 1
Router(config-rpd)# rpd-event profile 0
Router(config-rpd)# rpd-55dl-us-event profile 0
```

Verifying Multiple Cores Configuration

To display the information of the principal and auxiliary cores, use the **show cable rpd** command as shown in the example below:

```
Router# show cable rpd
MAC Address      IP Address      I/F           State      Role HA Name
0004.9f00.0907  120.100.2.20   Tel1/1/6     online     Pri   Act  node
0004.9f00.0907  120.100.2.20   Tel1/1/0     online     Aux   Act  node
0004.9f00.0907  120.100.2.20   Tel1/1/1     online     Aux   Act  node
0004.9f00.0907  120.100.2.20   Tel1/1/2     online     Aux   Act  node
```



Note Only the active cores are displayed, stand-by cores are hidden.



CHAPTER 8

GCPP Support for Remote PHY

This document provides information on the Generic Control Protocol Principal (GCPP) support on Cisco cBR-8 series routers.

Finding Feature Information

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

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

- [Information About GCPP Support, on page 49](#)
- [How to Configure GCPP Core, on page 51](#)
- [Configuration Example, on page 52](#)
- [Feature Information for GCPP Support, on page 52](#)

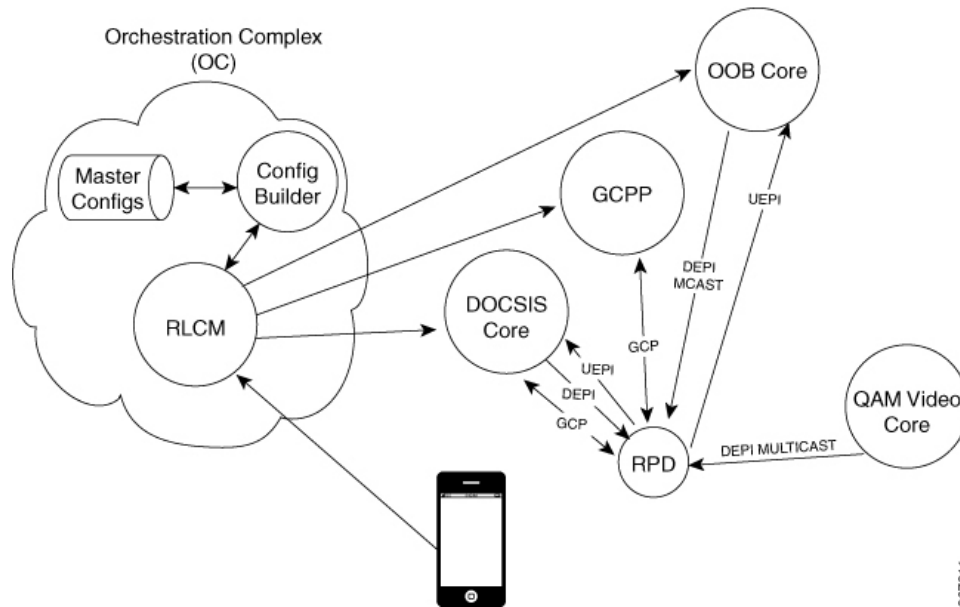
Information About GCPP Support

The Generic Control Protocol (GCP) sets up a control plane tunnel over a generic transport protocol such as TCP or UDP. GCP is used to program the remote PHY system upstream and downstream parameters from the CMTS. It is also used to control the remote PHY system.

The Remote PHY architecture with GCPP (Generic Control Protocol Principal) server, includes separate DOCSIS, QAM video and OOB cores. To enable the use of multiple RPHY cores, the architecture utilizes a GCP Principal Core (GCPP). Initially, the RPDs contact and authenticate with the GCPP core, which also configures the RPDs in its domain in coordination with the Cores (DOCSIS, QAM video, and OOB).

Without the GCPP core, cBR8 is the principal core for RPD. However, in this GCPP architecture, the GCPP server is the principal core and the Cisco cBR8 is an auxiliary core.

Figure 5: Remote PHY Architecture with GCPP



The Cisco 2x2 RPD software supports configurable GCP keepalive timeout parameter.

Hardware Compatibility Matrix for Cisco Remote PHY Device



Note Unless otherwise specified, the hardware components introduced in a given Cisco Remote PHY Device Software Release are supported in all subsequent releases.

Table 14: Hardware Compatibility Matrix for the Cisco Remote PHY Device

Cisco HFC Platform	Remote PHY Device
Cisco GS7000 Super High Output Node	Cisco 1x2 / Compact Shelf RPD Software 2.1 and Later Releases
Cisco GS7000 Super High Output Intelligent Node (iNode)	Cisco 1x2 / Compact Shelf RPD Software 4.1 and Later Releases Cisco Intelligent Remote PHY Device 1x2 <ul style="list-style-type: none"> • PID—iRPD-1X2= • PID—iRPD-1X2-PKEY=



Note The -PKEY suffix in the PID indicates units that enable the SCTE-55-2 Out-of-Band protocol support.

GCPP Core

GCPP core provides containerized services for automating deployments, managing applications, the initial authentication of the RPDs, and configuring RPD features and video services. The Principal Core does not provide any services (video or data).

The GCPP configures RPDs using GCP with the details of the other Cores that will configure it and the resources that will be configured by those Cores. The GCPP then performs the RPD operational configuration and the video and OOB service configuration. By the end of this process, the RPD will have its operational configuration and video and OOB services set up.

The GCPP core performs the following three primary functions:

- Initial authentication of the RPD
- Initial configuration of the RPD, including the list of cores to which it connects and the resources that those other cores will configure
- Configuration of the multicast sources that the RPD uses to populate QAM video (broadcast and narrowcast) channels

GCPP allows integrating videos on a standardized, single video platform. It also provides the configuration of the RPD's video channels, removing the requirements from the Video Core to support RPD authentication and GCP configuration.

How to Configure GCPP Core

This section contains the following:

Adding GCPP Core IP Address

Add the GCPP core IP address in the original CNR RPD policy if your RPD helper address is cnr8/auto-cnr. Or add the DHCP pool with the GCPP core/CCAP core in the USD.

Configuring Cisco cBR for Enabling GCPP

To set the GCPP server as the core server, configure Cisco cBR to remove the principal keyword under RPD configuration.

```
cable rpd <RPD name>
  identifier <RPD ID>
  core-interface <slot/subslot/port>
    principal      <<<<<<<<<< remove it, gcpp is the principal core
  rpd-ds <port-ID> downstream-cable <slot/sub-slot/controller> profile <ID>
  rpd-us <port-ID> upstream-cable <slot/sub-slot/controller> profile <ID>
  core-interface <slot/subslot/port>
    rpd-ds <port-ID> downstream-cable <slot/sub-slot/controller> profile <ID>
r-dti <ID>
  rpd-event profile <ID>
  rpd-55d1-us-event profile <ID>
```

Configuration Example

This section provides example of Cisco cBR-8 Converged Broadband Router configuration when GCPP is the core.

Example: GCPP Configuration

```
cable rpd pl_0719
  identifier 0004.9f00.0719
  core-interface Te6/1/2
    rpd-ds 0 downstream-cable 6/0/17 profile 7
    rpd-us 0 upstream-cable 6/0/17 profile 7
  core-interface Te6/1/1
    rpd-ds 0 downstream-cable 6/0/3 profile 17
r-dti 6
  rpd-event profile 0
  rpd-55d1-us-event profile 0
```

Feature Information for GCPP Support

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



Note

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

Table 15: Feature Information for GCPP Support

Feature Name	Releases	Feature Information
GCPP Support	Cisco 1x2 RPD Software 4.1	This feature was introduced on the Cisco Remote PHY Devices.



CHAPTER 9

IKEv2 Mutual Authentication

This document describes the Remote PHY device IKEv2 mutual authentication on the Cisco cBR Series Converged Broadband Router.

Finding Feature Information

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

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

- [Information about IKEv2 Mutual Authentication, on page 53](#)
- [Configure IKEv2 Mutual Authentication, on page 53](#)
- [Feature Information for IKEv2 Mutual Authentication, on page 54](#)

Information about IKEv2 Mutual Authentication

When the RPD connects to the CCAP Core, a mutual authentication using IKEv2 with public key signatures is optionally required and a secure control session may be established which can be secured using IPsec.

Mutual authentication is optionally required between the RPD and CCAP Core, and a secure connection may not be required in all cases. Whether authentication is required for an RPD is determined by the network that it is connected to. In some cases, RPD is located in an untrusted network, and it must connect to devices inside the trusted network, which presents a potential security vulnerability.

Authentication is initiated by RPD. Whether the RPD is required to authenticate is under control of the CCAP Core.

Configure IKEv2 Mutual Authentication

This section describes how to configure IKEv2 mutual authentication for RPD.

CMTS Side Configuration

Global Configuration

To enable IKEv2 mutual authentication, use **cable rphy auth enable** command in the global configuration mode.

Per PRD Configuration

To configure the IKEv2 mutual authentication per PRD, use **ikev2-core authentication {enable | disable | bypass}** command in the RPD configuration mode.

To display the authentication state, use **show cable rpd** command as shown in the following example:

```
Router#show cable rpd
Load for five secs: 5%/1%; one minute: 4%; five minutes: 5%
Time source is NTP, 10:08:45.016 CST Mon Sep 4 2017
MAC Address      IP Address      I/F      State      Role  HA    Auth  Name
0004.9f00.0719   6.6.6.100      Te6/1/2  online     Pri  Act  Y     p1_0719
0004.9f00.0719   6.6.6.100      Te6/1/1  online     Aux  Act  Y     p1_0719
badb.ad13.411c   6.6.6.101      Te6/1/2  onlissne   Pri  Act  Y     p2_411c
badb.ad13.411c   6.6.6.101      Te6/1/1  online     Aux  Act  Y     p2_411c
```



Note If RPD IKEv2 authentication is enabled, and RPD Core is authenticated, then the column of “auth” will show “Y”. If RPD IKEv2 authentication is enabled, and RPD Core is not authenticated, then the column of “auth” will show “N”. If RPD IKEv2 authentication is disabled, the column of “auth” will show “N/A”.

RPD Node Side Configuration

To configure the IKEv2 mutual authentication on RPD node, use **ikev2 authentication {enable | disable}** command on RPD node.

To display the authentication configuration state, use **show ikev2** command as shown in the following examples:

```
R-PHY#show ikev2 configuration
IKEv2 authentication is currently enabled, next boot is enabled!

R-PHY#show ikev2 session
Local      Remote      Status
6.6.6.100  6.6.6.1    UP
```

Feature Information for IKEv2 Mutual Authentication

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



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

Table 16: Feature Information for IKEv2 Mutual Authentication

Feature Name	Releases	Feature Information
IKEv2 Mutual Authentication	Cisco 1x2 / Compact Shelf RPD Software 4.1	This feature was introduced on the Cisco Remote PHY Device.



CHAPTER 10

Power Configuration for Compact Shelf

This document describes how to configure the RF channel's power level, the input power level for the upstream radio frequency (RF) carrier, and the base channel power level for Compact Shelf.

Finding Feature Information

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

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

- [Hardware Compatibility Matrix for Cisco Remote PHY Device](#), on page 57
- [Information about Power Configuration for Compact Shelf](#), on page 58
- [How to Configure Base Power, Downstream Power Level, and Upstream Power Level](#), on page 58
- [Configuring Maximum Carriers](#), on page 58
- [Configuring Base Channel Power Level](#), on page 58
- [Configuring RF Channel Power Level](#), on page 59

Hardware Compatibility Matrix for Cisco Remote PHY Device



Note Unless otherwise specified, the hardware components introduced in a given Cisco Remote PHY Device Software Release are supported in all subsequent releases.

Table 17: Hardware Compatibility Matrix for the Cisco Remote PHY Device

Cisco HFC Platform	Remote PHY Device
Cisco GS7000 Super High Output Node	Cisco 1x2 / Compact Shelf RPD Software 2.1 and Later Releases

Cisco HFC Platform	Remote PHY Device
Cisco GS7000 Super High Output Intelligent Node (iNode)	Cisco 1x2 / Compact Shelf RPD Software 4.1 and Later Releases Cisco Intelligent Remote PHY Device 1x2 <ul style="list-style-type: none"> • PID—iRPD-1X2= • PID—iRPD-1X2-PKEY=



Note The -PKEY suffix in the PID indicates units that enable the SCTE-55-2 Out-of-Band protocol support.

Information about Power Configuration for Compact Shelf

For Compact Shelf, new commands have been added to configure RF channel's power level, the input power level for the upstream radio frequency (RF) carrier, and the base channel power level.

How to Configure Base Power, Downstream Power Level, and Upstream Power Level

This section describes how to configure base power, downstream power level, and upstream power level on Compact Shelf.

Configuring Maximum Carriers

To configure the maximum number of carriers, complete the following procedure. The default number of maximum carriers specified is 158. The maximum number of carrier ranges from 1–158.

```
configure terminal
cable rpd name
rpd-ds port max-carrier value
```

This is an example of maximum carrier configuration:

```
Router# configure terminal
Router(config)#cable rpd node6
Router(config-rpd)#rpd-ds 0 max-carrier 128
```

Configuring Base Channel Power Level

To set the base channel power level, complete the following procedure. The base channel power level range is 25–34.

```
configure terminal
cable rpd name
rpd-ds port base-power value
```

This is an example of base channel power level configuration.

```
Router# configure terminal
Router(config)#cable rpd node6
Router(config-rpd)# rpd-ds 0 base-power 30
```

Configuring RF Channel Power Level

To adjust the RF channel's power level, complete the following procedure. The RF channel power level range is 7–23

```
configure terminal
cable rpd name
rpd-ds port rf-channel number power-adjust value
```

This is an example of RF channel power level.

```
Router# configure terminal
Router(config)#cable upstream controller-profile 221
Warning: changes to this profile will affect the following controllers:
        9/0/10,

Confirm to continue? [no]: yes
Router(config-controller-profile)#us
Router(config-controller-profile)#us-channel 0 pow
Router(config-controller-profile)#us-channel 0 power-level ?
    <-7 - 25> Power level in dBmV(-4~25 for rphy-node, -7~23 for rphy-shelf)

Router(config-controller-profile)#us-channel 0 power-level 23
```




CHAPTER 11

Link Layer Discovery Protocol

This document describes how to display the RPD LLDP neighbors and counters information. It also describes how to use the **show lldp neighbors/statistics** command.

Finding Feature Information

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

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

- [Hardware Compatibility Matrix for Cisco Remote PHY Device, on page 61](#)
- [Link Layer Discovery Protocol, on page 62](#)
- [Displaying LLDP Status, on page 62](#)
- [Feature Information for LLDP, on page 63](#)

Hardware Compatibility Matrix for Cisco Remote PHY Device



Note Unless otherwise specified, the hardware components introduced in a given Cisco Remote PHY Device Software Release are supported in all subsequent releases.

Table 18: Hardware Compatibility Matrix for the Cisco Remote PHY Device

Cisco HFC Platform	Remote PHY Device
Cisco GS7000 Super High Output Node	Cisco 1x2 / Compact Shelf RPD Software 2.1 and Later Releases

Cisco HFC Platform	Remote PHY Device
Cisco GS7000 Super High Output Intelligent Node (iNode)	Cisco 1x2 / Compact Shelf RPD Software 4.1 and Later Releases Cisco Intelligent Remote PHY Device 1x2 <ul style="list-style-type: none"> • PID—iRPD-1X2= • PID—iRPD-1X2-PKEY=



Note The -PKEY suffix in the PID indicates units that enable the SCTE-55-2 Out-of-Band protocol support.

Link Layer Discovery Protocol

LLDP (Link Layer Discovery Protocol) is a vendor-neutral link layer protocol in the Internet Protocol Suite used by network devices for advertising their identities and capabilities on an IEEE 802 local area network, principally wired Ethernet.

In Cisco 1x2 / Compact Shelf RPD Software 6.1, LldpEnable TLV is introduced to enable or disable the LLDP protocol.

This TLV will be documented in a forthcoming revision of the Cablelabs Remote PHY Specification. The TLV Type is 15.6.1. A Boolean value is defined to enable/disable LLDP operation on the RPD. 0 means LLDP is disabled. 1 means LLDP is enabled. Default value is 1.

Displaying LLDP Status

To display RPD LLDP neighbors and counters information, use **show lldp neighbors/statistics** command as shown in the following example.

```
R-PHY#show lldp neighbors
-----
LLDP neighbors:
-----
Interface:   eth0, via: LLDP, RID: 1, Time: 0 day, 21:10:24
Chassis:
  ChassisID:  mac 00:1c:0e:82:c3:26
  SysName:    K02-NM-SW.cisco.com
  SysDescr:   Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 12.2(37)SE,
  RELEASE SOFTWARE (fc2)
              Copyright (c) 1986-2007 by Cisco Systems, Inc.
              Compiled Thu 10-May-07 16:43 by antonino
  MgmtIP:    10.74.54.231
  Capability: Bridge, off
  Capability: Router, off
Port:
  PortID:    local Fa0/38
  PortDescr: FastEthernet0/38
-----
Interface:   vbh0, via: LLDP, RID: 2, Time: 0 day, 04:12:02
```

```

Chassis:
  ChassisID:      mac 00:de:fb:95:17:01
  SysName:        Cloud-Leaf-C
  SysDescr:       Cisco NX-OS(tm) n6000, Software (n6000-uk9), Version 7.3(3)N1(1), Interim
                  version 7.3(3)N1(0.535), RELEASE SOFTWARE Copyright (c) 2002-2012, 2016-2017 by Cisco
                  Systems, Inc. Compiled 11/18/2017 2:00:00
  MgmtIP:         10.74.54.173
  Capability:     Bridge, on
Port:
  PortID:         local Eth1/26
  PortDescr:      Ethernet1/26
UnknownTLVs:
  TLV:            OUI: 00,01,42, SubType: 1, Len: 1 01
  TLV:            OUI: 00,01,42, SubType: 2, Len: 16
                  24,00,24,00,24,00,24,00,24,00,24,00,24,00,24,00
  TLV:            OUI: 00,01,42, SubType: 6, Len: 4 06,00,00,00
-----

```

```
R-PHY#show lldp statistics
```

```
-----
LLDP statistics:
-----
```

```
Interface:      eth0
  Transmitted:  5099
  Received:     3818
  Discarded:    0
  Unrecognized: 6
  Ageout:       0
  Inserted:     2
  Deleted:      0
-----
```

```
Interface:      vbh0
  Transmitted:  2548
  Received:     2554
  Discarded:    6
  Unrecognized: 8
  Ageout:       0
  Inserted:     1
  Deleted:      0
-----
```

If the LLDP is disabled, the output of the **show lldp statistics** command will be:

```
R-PHY#show lldp statistics
lldp disabled
```

Feature Information for LLDP

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



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

Table 19: Feature Information for LLDP

Feature Name	Releases	Feature Information
LLDP	Cisco 1x2 / Compact Shelf RPD Software 5.4	This feature was integrated into the Cisco Remote PHY Device.
Disable LLDP by TLV	Cisco 1x2 / Compact Shelf RPD Software 6.1	This feature was integrated into the Cisco Remote PHY Device.



CHAPTER 12

TACACS+

- [Hardware Compatibility Matrix for Cisco Remote PHY Device, on page 65](#)
- [TACACS+, on page 66](#)
- [Configuring TACACS+, on page 66](#)
- [Displaying TACACS+ Configuration, on page 66](#)
- [Feature Information for TACACS+, on page 67](#)

Hardware Compatibility Matrix for Cisco Remote PHY Device



Note Unless otherwise specified, the hardware components introduced in a given Cisco Remote PHY Device Software Release are supported in all subsequent releases.

Table 20: Hardware Compatibility Matrix for the Cisco Remote PHY Device

Cisco HFC Platform	Remote PHY Device
Cisco GS7000 Super High Output Node	Cisco 1x2 / Compact Shelf RPD Software 2.1 and Later Releases
Cisco GS7000 Super High Output Intelligent Node (iNode)	Cisco 1x2 / Compact Shelf RPD Software 4.1 and Later Releases Cisco Intelligent Remote PHY Device 1x2 <ul style="list-style-type: none">• PID—iRPD-1X2=• PID—iRPD-1X2-PKEY=



Note The -PKEY suffix in the PID indicates units that enable the SCTE-55-2 Out-of-Band protocol support.

TACACS+

Terminal Access Controller Access Control System (TACACS) is a security protocol that provides centralized validation of users who are attempting to gain access to a router or NAS. TACACS+, a more recent version of the original TACACS protocol, provides separate authentication, authorization, and accounting (AAA) services.



-
- Note**
1. RPD can configure 8 TACACS servers at the most. All configured servers use the same secret key.
 2. If multiple TACACS servers are configured, RPD will try to connect TACACS server in the order in which the servers are configured until the connection is established successfully.
 3. RPD and TACACS server must use same address family.
-

Configuring TACACS+

To enable TACACS+, user needs to setup a TACACS server with secret key configured. Then add this TACACS server's IPv4/IPv6 address and key to RPD configuration.

```
R-PHY(config)#tacacs add-server 10.0.0.113
Server '10.0.0.113' is configured on RPD successfully.
```

```
R-PHY(config)#tacacs add-key
Please add a secret key:
Please re-enter your secret key:
Add secret key successfully.
```

User can also delete server and change the secret key.

```
R-PHY(config)#tacacs delete-server 10.0.0.112
Delete server '10.0.0.112' successfully.
```

```
R-PHY(config)#tacacs change-key
Please change secret key:
Please re-enter your secret key:
Change secret key successfully.
```

Displaying TACACS+ Configuration

To display the configured TACACS server, use the **show tacacs-server** command as shown in the following example:

```
R-PHY#show tacacs-server
TACACS server configured:
10.0.0.113
```

Feature Information for TACACS+

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

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

Table 21: Feature Information for TACACS+

Feature Name	Releases	Feature Information
TACACS+	Cisco 1x2 / Compact Shelf RPD Software 6.4	This feature was integrated into the Cisco Remote PHY Device.



PART II

Remote PHY System High Availability

- [Cisco Remote PHY Line Card and Supervisor Redundancy, on page 71](#)



CHAPTER 13

Cisco Remote PHY Line Card and Supervisor Redundancy

This document provides information about Remote PHY line card and Supervisor redundancy.

- [Hardware Compatibility Matrix for Cisco Remote PHY Device, on page 71](#)
- [Information About Remote PHY Line Card and Supervisor Redundancy, on page 72](#)
- [How to Configure Remote PHY Line Card Redundancy, on page 74](#)
- [How to Configure DPIC Link Redundancy, on page 76](#)
- [Feature Information for Remote PHY Redundancy, on page 78](#)

Hardware Compatibility Matrix for Cisco Remote PHY Device



Note Unless otherwise specified, the hardware components introduced in a given Cisco Remote PHY Device Software Release are supported in all subsequent releases.

Table 22: Hardware Compatibility Matrix for the Cisco Remote PHY Device

Cisco HFC Platform	Remote PHY Device
Cisco GS7000 Super High Output Node	Cisco 1x2 / Compact Shelf RPD Software 2.1 and Later Releases
Cisco GS7000 Super High Output Intelligent Node (iNode)	Cisco 1x2 / Compact Shelf RPD Software 4.1 and Later Releases Cisco Intelligent Remote PHY Device 1x2 <ul style="list-style-type: none">• PID—iRPD-1X2=• PID—iRPD-1X2-PKEY=



Note The -PKEY suffix in the PID indicates units that enable the SCTE-55-2 Out-of-Band protocol support.

Information About Remote PHY Line Card and Supervisor Redundancy

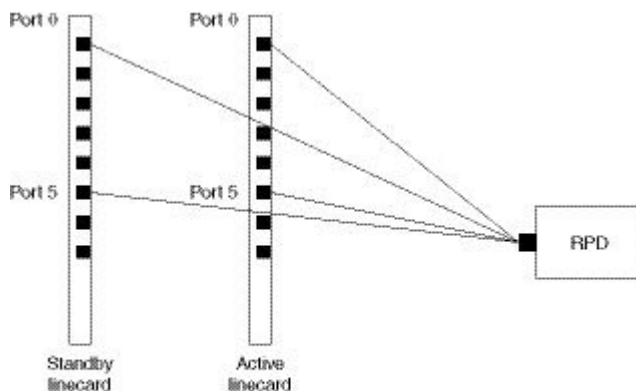
This section provides details of line card and Supervisor redundancy.

Line Card Redundancy

In Remote PHY (R-PHY) configuration, RPDs connect to both active linecard and standby linecard, and have active connections to active linecard, standby connections to standby linecard. From RPD side, it connects to active core and standby core independently.

Each RPD has one principal core, and may have several auxiliary cores. LCHA needs to support multiple cores. These cores are on the same linecard or different linecards. The port on the standby linecard can protect all the same ports on the active linecards.

Figure 6: Multiple cores on the same line card

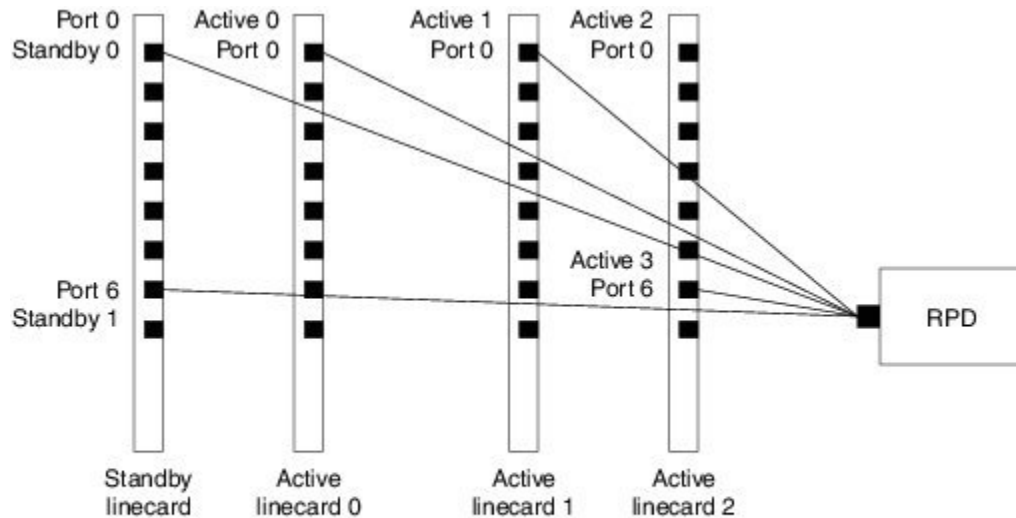


■ The Giga port

In the figure above, the RPD has multiple cores connected to the same active linecard. In order to support LCHA, RPD needs to connect to the same port on the standby linecard. In this way, RPD has several standby cores to protect the active cores. The standby core have the same resource as the active core.

When multiple cores connect to different active linecards, if they connect to different ports of the linecard, there will have different standby cores. If active core connects to the same port on different linecard, they share one standby core.

Figure 7: Multiple cores on different line cards



■ The Giga port

In the figure above, RPD have two standby cores. One standby core connects to port 6 of the standby linecard, it can protect the active core which connects to port 6 of the active linecard 2. The other standby core connects to port 0 of the standby linecard, it can protect the active cores connect to port 0 of linecard 0 and linecard 1. So for the standby core 0, it contains the resource for both active core 0 and active core 1.

When active linecard 0 fails over to standby linecard, the standby core 1 will be deleted, the standby core 0 will bring the resource of active core 0 to active. When linecard 2 fails over to standby linecard, the standby core 0 will be deleted, and standby core 1 will become active for active core 3.

For more information about Line Card Redundancy, see [Line Card Redundancy](#).

Supervisor Redundancy

Compared to the SUP high availability recover process in iCMTS configuration, the Remote PHY SUP high availability recover process has RPD status change as shown in the example below:

```
show cable rpd 0004.9f00.0625 lcha-cores
MAC Address      IP Address      I/F      State      Role  HA   Name
0004.9f00.0625  120.105.6.10  Te0/1/1  recovering  Pri  Act  node1
0004.9f00.0625  120.105.6.10  Te9/1/1  recovering  NA   Sby  node1

show cable rpd 0004.9f00.0625 lcha-cores
MAC Address      IP Address      I/F      State      Role  HA   Name
0004.9f00.0625  120.105.6.10  Te0/1/1  init(l2tp)  Pri  Act  node1
0004.9f00.0625  120.105.6.10  Te9/1/1  init(l2tp)  NA   Sby  node1

show cable rpd 0004.9f00.0625 lcha-cores
MAC Address      IP Address      I/F      State      Role  HA   Name
0004.9f00.0625  120.105.6.10  Te0/1/1  online      Pri  Act  node1
0004.9f00.0625  120.105.6.10  Te9/1/1  online      NA   Sby  node1
```

The status of the RPD changes from recovering to online, indicating that the SUP redundancy is working in the Remote PHY configuration.

For more information about SUP redundancy, see [Supervisor Redundancy](#).

DPIC Link Redundancy

The Cisco cBR Series Remote PHY Digital Physical Interface Card (DPIC) provides the Ethernet network connection between the CCAP core and Remote PHY devices.

You can enable or disable RPHY link redundancy feature for a chassis. The redundancy state of a link is described using the link *mode* and *role*.

The redundancy mode is the term that is used for the configured or administered designation of a link, and is determined during the link configuration. The redundancy mode does not change during a switchover. There are two redundancy modes:

- **Primary mode:** This is the default working link of a core interface. The primary link is fixed to port 0, 2, 4, 6 when the link high availability is enabled.
- **Secondary mode:** This mode provides protection to the primary link. The secondary link is fixed to port 1, 3, 5, 7 when the link high availability is enabled.

The redundancy role is a dynamic entity that indicates the runtime or operational status of a port. The role changes only during a link switchover. The entity has two states:

- **Active role:** This link carries the RPHY data stream of the core interface. When the primary link is switched over to the secondary link, the secondary link becomes the active link of the core interface.
- **Standby role:** This link does not run any RPHY data traffic, but gets prepared to become active when the current active link has failed. According to the physical state of the standby link, the standby link can be further distinguished into a standby-hot link and standby-cold link. A standby-hot retains the link in the UP state. The 10-Gigabit Ethernet transceiver and TX power are enabled in this case, and the 10-Gigabit Ethernet port state is UP in the directly connected switch or router. The link of standby port is shut down, the TX power turned off and the 10-Gigabit Ethernet port state in the directly connected switch or router is down.

cBR supports both standby-hot and standby-cold redundancy modes.

In 1+1 core link redundancy configuration, the secondary link is the backup link for the primary link. At any given time, only one link (the active link) carries the RPHY control and data traffic for a core interface. The standby link provides protection for only one primary link. Current 8x10G DPIC has eight 10G ports on front panel and 4x10G XFI ports to Cylons-R 40G. Each 10G XFI port provides two core interfaces sharing the total 10G bandwidth. For an 8-port DPIC card, you can provide four 1+1 redundant groups.

When link high availability is enabled in the chassis, the secondary card supports link HA as do the other linecards. Each linecard makes its link switchover decisions that is independently based on the physical link state.

How to Configure Remote PHY Line Card Redundancy

This section describes how to configure Remote PHY (R-PHY) Line Card Redundancy on Cisco cBR-8.

Configuring DPIC Ports

The Remote PHY LCHA, typically has separate paths for primary and secondary interfaces on the RPD. Hence, you should configure separate VRFs for DPIC interfaces on the secondary LC.



Note Sub-interfaces are not supported for DPIC interfaces on linecards in slots 0-3 and 6-9.

The following example shows how to configure DPIC port to support Remote PHY Line Card Redundancy:

```
Router# configure terminal
Router(config)# interface TenGigabitEthernet8/1/0
Router(config-if)# vrf forwarding te80
Router(config-if)# ip address 80.6.16.166 255.255.255.0
Router(config-if)# exit
Router(config)# interface TenGigabitEthernet8/1/1
Router(config-if)# vrf forwarding te81
Router(config-if)# ip address 80.6.16.167 255.255.255.0
Router(config-if)# exit
Router(config)# interface TenGigabitEthernet6/1/0
Router(config-if)# vrf forwarding te60
Router(config-if)# ip address 80.6.16.186 255.255.255.0
Router(config-if)# exit
Router(config)# interface TenGigabitEthernet6/1/1
Router(config-if)# vrf forwarding te61
Router(config-if)# ip address 80.6.16.187 255.255.255.0
```

Configuring RPD

The following example shows how to configure RPD to support Remote PHY Line Card Redundancy:

```
Router# configure terminal
Router(config)# cable rpd node1
Router(config-rpd)# identifier 0004.9f03.0055
Router(config-rpd)# core-interface te8/1/0
Router(config-rpd-core)# principal
Router(config-rpd-core)# rpd-ds 0 downstream-cable 8/1/0 profile 0
Router(config-rpd-core)# rpd-us 0 upstream-cable 8/1/0 profile 0
Router(config-rpd-core)# exit
Router(config-rpd)# core-interface te8/1/1
Router(config-rpd-core)# rpd-ds 0 downstream-cable 8/1/1 profile 0
Router(config-rpd-core)# rpd-us 0 upstream-cable 8/1/1 profile 0
Router(config-rpd-core)# exit
Router(config-rpd)# exit
Router(config)# cable rpd node2
Router(config-rpd)# identifier 0004.9f03.0163
Router(config-rpd)# core-interface te8/1/2
Router(config-rpd-core)# principal
Router(config-rpd-core)# rpd-ds 0 downstream-cable 8/0/1 profile 1
Router(config-rpd-core)# rpd-us 0 upstream-cable 8/0/2 profile 2
```

Configuring Remote PHY Line Card Redundancy

The following example shows how to configure Remote PHY Line Card Redundancy:

```
Router# configure terminal
Router(config)# redundancy
Router(config-red)# mode sso
```

```

Router(config-red)# linecard-group 0 internal-switch
Router(config-red-lc)# class 1:N
Router(config-red-lc)# member slot 8 primary
Router(config-red-lc)# member slot 6 secondary
Router(config-red-lc)# no revertive

```

Verifying Remote PHY Line Card Redundancy Configuration

To verify the Remote PHY line card redundancy configuration, use the example below:

```

Router# show redundancy linecard all

```

Slot	Subslot	LC Group	My State	Peer State	Peer Slot	Peer Subslot	Role	Mode
8	-	0	Active	Stdby Warm	6	-	Active	Primary
6	-	0	-	-	Multiple	None	Standby	Secondary

```

Router# show cable rpd lcha-cores

```

MAC Address	IP Address	I/F	State	Core Role	HA Role
0004.9f03.0055	80.6.16.15	Te6/1/0	online	Principal	Standby
0004.9f03.0055	80.6.16.15	Te8/1/0	online	Principal	Active
0004.9f03.0163	80.6.16.16	Te6/1/1	online	Principal	Standby
0004.9f03.0163	80.6.16.16	Te8/1/1	online	Principal	Active

```

Router# show cable rpd

```

MAC Address	IP Address	I/F	State	Core Role	HA Role
0004.9f03.0055	80.6.16.15	Te6/1/0	online	Principal	Active
0004.9f03.0163	80.6.16.16	Te6/1/1	online	Principal	Active

How to Configure DPIC Link Redundancy

This section describes how to configure DPIC Link Redundancy on Cisco cBR-8.

Configuring DPIC Link Redundancy

The link redundancy is disabled by default. You need to enable the link redundancy feature manually.

- To set the DPIC link in the UP state, use the **cable rphy link redundancy hot** command.
- To set the DPIC link in the standby-down state, use the **cable rphy link redundancy cold** command.
For example:

```

Router# cable rphy link redundancy cold

```

```

RPHY Link HA: Cold mode enabled

```

Core Interface	Port	Mode	Role	Status
Te 2/1/0	0	Primary	Active	Up
Te 2/1/0	1	Secondary	Standby	Ready
Te 2/1/2	2	Primary	Active	Up
Te 2/1/2	3	Secondary	Standby	Ready
Te 2/1/4	4	Primary	Active	Up
Te 2/1/4	5	Secondary	Standby	Ready
Te 2/1/6	6	Primary	Active	Up
Te 2/1/6	7	Secondary	Standby	Ready

- To disable the link redundancy, run the **no cable rphy link redundancy** command.

Verifying DPIC Link Redundancy

To verify the DPIC link redundancy, go through the following steps:

- To check the link redundancy of any of the DPIC slots, run the **show redundancy digi-pic slot <0-9>** command. See the following example:

```
Router# show redundancy digi-pic slot 0:
```

```
RPHY Link HA: Hot mode enabled
Core Interface Port Mode          Role      Status
-----
Te 0/1/0          0    Primary    Active    Up
Te 0/1/0          1    Secondary  Standby   Up ("Ready" in standby-cold mode)
Te 0/1/2          2    Primary    Active    Up
Te 0/1/2          3    Secondary  Standby   Down
Te 0/1/4          4    Primary    Standby   Up ("Ready" in standby-cold mode)
Te 0/1/4          5    Secondary  Active    Up
Te 0/1/6          6    Primary    Active    Down
Te 0/1/6          7    Secondary  Standby   Down
```

- To view the DPIC history, use the **show redundancy digi-pic history slot <0-9>** command. See the following example:

```
Router# show redundancy digi-pic history slot 2
```

```
Jun 25 2018 14:41:14 - 2/1/0: Auto switchover from port:1 link:down to port:0 link up,
  success.
Jun 25 2018 14:40:54 - 2/1/0: Auto switchover from port:0 link:down to port:1 link up,
  success.
Jun 25 2018 14:39:20 - 2/1/0: Enable LINKHA success.
Jun 25 2018 14:39:20 - 2/1/2: Enable LINKHA success.
Jun 25 2018 14:39:20 - 2/1/4: Enable LINKHA success.
Jun 25 2018 14:39:20 - 2/1/6: Enable LINKHA success.
Jun 25 2018 14:38:56 - 2/1/0: Disable LINKHA success.
Jun 25 2018 14:38:56 - 2/1/2: Disable LINKHA success.
Jun 25 2018 14:38:56 - 2/1/4: Disable LINKHA success.
Jun 25 2018 14:38:56 - 2/1/6: Disable LINKHA success.
Jun 25 2018 14:37:20 - 2/1/0: Manual switchover from port:1 to port:0, success.
Jun 25 2018 14:37:16 - 2/1/0: Manual switchover from port:0 to port:1, success.
Jun 25 2018 14:36:31 - 2/1/0: Enable LINKHA success.
Jun 25 2018 14:36:31 - 2/1/2: Enable LINKHA success.
Jun 25 2018 14:36:31 - 2/1/4: Enable LINKHA success.
Jun 25 2018 14:36:31 - 2/1/6: Enable LINKHA success.
```

- To check the link redundancy of the TenGigabitEthernet 0/1/4, use the **show redundancy digi-pic interface TenGigabitEthernet 0/1/4** command. See the following example:

```
Router# show redundancy digi-pic interface TenGigabitEthernet 0/1/4
```

```
Link HA      : Hot mode enabled
HA State     : In Failover
Reason       : Manual Switchover
```

```
Port Mode      Role      Status
-----
  4 Primary      Standby   Up ("Ready" in standby-cold mode)
  5 Secondary   Active    Up
```

You can view the DPIC history of the TenGigabitEthernet using the **show redundancy digi-pic history interface TenGigabitEthernet <0-9>/1/<0, 2, 4, 6>** command. See the following example:

```

Router# show redundancy digi-pic history interface TenGigabitEthernet 2/1/0

Jun 25 2018 14:41:14 - 2/1/0: Auto switchover from port:1 link:down to port:0 link up,
success.
Jun 25 2018 14:40:54 - 2/1/0: Auto switchover from port:0 link:down to port:1 link up,
success.
Jun 25 2018 14:39:20 - 2/1/0: Enable LINKHA success.
Jun 25 2018 14:38:56 - 2/1/0: Disable LINKHA success.
Jun 25 2018 14:37:20 - 2/1/0: Manual switchover from port:1 to port:0, success.
Jun 25 2018 14:37:16 - 2/1/0: Manual switchover from port:0 to port:1, success.
Jun 25 2018 14:36:31 - 2/1/0: Enable LINKHA success.
Jun 25 2018 14:36:02 - 2/1/0: Disable LINKHA success.
Jun 22 2018 00:01:24 - 2/1/0: Enable LINKHA success.
Jun 22 2018 00:00:12 - 2/1/0: Enable LINKHA success.
Jun 22 2018 00:00:08 - 2/1/0: Disable LINKHA success.
Jun 21 2018 23:59:21 - 2/1/0: Enable LINKHA success.
Jun 21 2018 23:52:21 - 2/1/0: Enable LINKHA success.
Jun 21 2018 23:50:21 - 2/1/0: Enable LINKHA success.
Jun 21 2018 23:50:17 - 2/1/0: Disable LINKHA success.
Jun 21 2018 23:43:30 - 2/1/0: Enable LINKHA success.
Jun 21 2018 23:42:02 - 2/1/0: Enable LINKHA success.
Jun 21 2018 23:41:53 - 2/1/0: Disable LINKHA success.
Jun 21 2018 20:43:05 - 2/1/0: Enable LINKHA success.

```

Feature Information for Remote PHY Redundancy

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



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

Table 23: Feature Information for Remote PHY Redundancy

Feature Name	Releases	Feature Information
Remote PHY LCHA	Cisco 1x2 / Compact Shelf RPD Software 3.1	This feature was integrated into the Cisco Remote PHY Device.
Remote PHY SUPHA	Cisco 1x2 / Compact Shelf RPD Software 3.1	This feature was integrated into the Cisco Remote PHY Device.
DPIC Link Redundancy	Cisco 1x2 / Compact Shelf RPD Software 5.1	This feature was integrated into the Cisco Remote PHY Device.



PART III

Remote PHY System Configuration

- [Cisco Remote PHY Controller Profile and RPD Configuration, on page 81](#)
- [Cisco Remote PHY Device Downstream Virtual Splitting, on page 95](#)
- [Cisco Remote PHY DS OFDM Channel Configuration, on page 105](#)
- [Virtual Combining of Upstream Channels on RPD, on page 117](#)
- [Redundant Multicast DEPI Pool, on page 123](#)
- [DOCSIS3.1 Downstream Resiliency for RPHY, on page 127](#)
- [Dynamic Bonding Group for RPHY, on page 131](#)
- [Cisco Remote PHY Device IPv6, on page 143](#)
- [DOCSIS 3.1 OFDMA Channel Configuration, on page 153](#)
- [Spectrum Capture, on page 167](#)
- [Viavi Integration, on page 171](#)



CHAPTER 14

Cisco Remote PHY Controller Profile and RPD Configuration

The Remote PHY (R-PHY) Controller Profile includes upstream controller-profile and downstream controller-profile. Upstream controller-profile is used to specify the upstream (US) channels and related parameters, which are part of a specific profile, similar to the following:

- Channel width
- DOCSIS mode
- Frequency
- Minislot size
- Modulation-profile

The downstream controller-profile is used to specify the RF channels and their RF parameters that belong to a specific profile, including the following details:

- Channel type (DOCSIS, Video Sync, Video Async)
- Frequency
- RF output
- QAM-profile (annex, modulation, inter-leaver, symbol rate, and so on)

Finding Feature Information

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

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

- [Hardware Compatibility Matrix for Cisco Remote PHY Device, on page 82](#)
- [Controller Profile and RPD, on page 82](#)
- [Configure Controller Profile and RPD, on page 84](#)

- [Troubleshooting Tips, on page 92](#)
- [Configuration Examples, on page 92](#)
- [Feature Information for Remote PHY Controller Profile and RPD Configuration, on page 93](#)

Hardware Compatibility Matrix for Cisco Remote PHY Device



Note Unless otherwise specified, the hardware components introduced in a given Cisco Remote PHY Device Software Release are supported in all subsequent releases.

Table 24: Hardware Compatibility Matrix for the Cisco Remote PHY Device

Cisco HFC Platform	Remote PHY Device
Cisco GS7000 Super High Output Node	Cisco 1x2 / Compact Shelf RPD Software 2.1 and Later Releases
Cisco GS7000 Super High Output Intelligent Node (iNode)	Cisco 1x2 / Compact Shelf RPD Software 4.1 and Later Releases Cisco Intelligent Remote PHY Device 1x2 <ul style="list-style-type: none"> • PID—iRPD-1X2= • PID—iRPD-1X2-PKEY=



Note The -PKEY suffix in the PID indicates units that enable the SCTE-55-2 Out-of-Band protocol support.

Controller Profile and RPD

The Controller Profile functions in a similar way to the controller integrated-cable Slot/Bay/Port (for downstream controller) or upstream-cable Slot/Bay/Port (for upstream controller) in I-CMTS. However if a Controller Profile is not associated to an RPD, physical resources cannot be allocated.

You can either unicast or multicast this profile. Multicast profile is used for DS sharing. You can multicast the same traffic to all RPDs in the multicast group, or to applications such as switched digital video (SDV) or BC video.

An R-PHY configuration consists of one principal core interface and one auxiliary core interface. The principal core specifies the DPIC interface to which the RPD connects. Auxiliary core interfaces specify the external DPIC interfaces that can be used for downstream sharing. Auxiliary core is used in this release only for video multicast and video OOB.

Configuring Controller Profile and cable RPD are the prerequisites for configuring R-PHY video.

The following table lists the DSCP value for different kinds of items.

Item	Per-Hop-Behavior (PHB)	DSCP Value
DOCSIS data (L2TP)	Best Effort	0
PTP	EF	46
GCP	Best Effort	0
MAP/UCD (L2TP, DOCSIS control)	EF	46
BWR and RNG-REG	EF	46
Video	CS4	32
MDD (L2TP, DOCSIS control), voice	CS5	40

RPD Configurations

Compared to the iCMTS configuration, R-PHY configuration supports the following features:

- Up to 512 RPDs per CBR-8 chassis and 64 RPDs per CBR-CCAP-LC-40G-R line card
- 128 separate service groups per CBR-8 chassis
- 32 downstream controllers and up to 768 downstream channels per CBR-CCAP-LC-40G-R line card
- Up to 158 downstream channels (0-157) per downstream controller
- 64 upstream controllers and 128 upstream channels per CBR-CCAP-LC-40G-R line card



Note In Cisco IOS XE Fuji 16.8.1 and earlier releases, although 128 maximum upstream SCQAM channels per CBR-CCAP-LC-40G-R line card could be configured, the upstream maximum throughput per CBR-CCAP-LC-40G-R line card is 3 Gbps which is due to USJIB limitation. So, if the the upstream maximum throughput per CBR-CCAP-LC-40G-R line card is higher than 3 Gbpsm, upstream service cannot be guranteed.

Cisco IOS XE Fuji 16.9.1 and later releases support 10 Gbps of upstream throughput on the CBR-CCAP-LC-40G and CBR-CCAP-LC-40G-R line cards on the Cisco cBR Series Converged Broadband Router.

In the R-PHY configuration, the following mapping relationships are supported between the controller and the port on RPD:

- Downstream 1:N ($N \geq 2$) mapping: one DS controller is shared by several RPDs and one DS controller is mapped to one DS port of all these RPDs, that is “DS virtual split”, all these DS ports share the same signals from the same DS controller.
- Downstream N:1 mapping: several DS controllers are mapped into the same DS port of one RPD. Notice: the DS channels in these DS controller should use different rf-channel numbers

- Downstream N:N mapping: mixed 1:N and N:1 mapping. For example: several DS controllers are mapped into one DS port of one RPD. But at the same time they are “virtual split” DS controllers and are shared by several RPDs.
- Upstream 1:N(N<=8) mapping: one US controller can be shared by N (N<=8) US ports of multiple RPDs. Currently max two US ports are supported on one RPD, and for each US port, one US controller can be configured.

For the two US ports of one RPD, the same US controller number can be configured.



Note Downstream 1:1 mapping is not supported under 512 RPD configuration, but still supported under smaller scale configuration.

Prerequisites for Configuring Controller Profile and RPD

The following restrictions are applicable to configuring controller profiles:

- All channels within the profiles of an RPD must be unique. Frequencies must not overlap each other.
- The principal core must contain at least one DOCSIS downstream profile
- Auxiliary core should contain only video and out-of-band profiles
- A DS controller can be associated to only one profile

Restrictions for Configuring Controller Profile and RPD

The following restrictions are applicable to configuring upstream controller profiles:

- Legacy controller configuration commands are not supported
- Legacy controller configuration cannot be shown in running-configuration

Configure Controller Profile and RPD

Configure Upstream Controller Profile

To configure the upstream controller-profile, use the cable upstream controller-profile command, as given in the following example:

```
Router#cable upstream controller-profile 4
  cable def-phy-burst 0
  us-channel 0 chan-class-id 0
  us-channel 0 channel-width 1600000 1600000
  us-channel 0 docsis-mode atdma
  us-channel 0 equalization-coefficient
  us-channel 0 frequency 50000000
  us-channel 0 hop-priority frequency modulation channel-width
  us-channel 0 ingress-noise-cancellation 100
  us-channel 0 maintain-psd
```



```

us-channel 0 max-logical-chans 1
us-channel 0 minislots-size 4
us-channel 0 modulation-profile 221
us-channel 0 power-level 0
us-channel 0 rng-holdoff 0
us-channel 0 shutdown
us-channel 0 specsvl error-adaptive-profile 1
us-channel 0 threshold cnr-profiles 25 13
us-channel 0 threshold corr-fec 3
us-channel 0 threshold hysteresis 3
us-channel 0 threshold snr-profiles 25 13
us-channel 0 threshold uncorr-fec 1
...
end

```

Verify Upstream Controller Profile Configuration

To verify the Upstream controller profile configuration, use the **show cable downstream controller-profile** command or **show running-config | section upstream controller-profile <ID>** command, as shown in the following example:

```

Router#show cable upstream controller-profile 0
Load for five secs: 2%/0%; one minute: 3%; five minutes: 3%
Time source is NTP, 15:14:27.916 CST Fri Feb 24 2017

Upstream controller-profile 0
Description:
Upstream controller-profile 0 is being used by controller Upstream-Cable:
8/0/1, 8/0/0
Controller Upstream-Cable
...
Upstream-channel 0
chan-class-id           : 0x0
channel-width           : 1600000 1600000
docsis-mode             : atdma
...

```

Example for the **show running-config | section upstream controller-profile <ID>** command

```

Router#show running-config | s cable upstream controller-profile 0
cable upstream controller-profile 0
us-channel 0 channel-width 1600000 1600000
us-channel 0 docsis-mode atdma
us-channel 0 equalization-coefficient
us-channel 0 frequency 6000000
us-channel 0 minislots-size 4
us-channel 0 modulation-profile 221
no us-channel 0 shutdown
us-channel 1 channel-width 1600000 1600000
us-channel 1 docsis-mode atdma
us-channel 1 equalization-coefficient
us-channel 1 frequency 7600000
us-channel 1 minislots-size 4
us-channel 1 modulation-profile 221
no us-channel 1 shutdown
us-channel 2 channel-width 1600000 1600000
us-channel 2 docsis-mode atdma
us-channel 2 equalization-coefficient
us-channel 2 frequency 9200000
us-channel 2 minislots-size 4
us-channel 2 modulation-profile 221
no us-channel 2 shutdown
us-channel 3 channel-width 1600000 1600000

```

```

us-channel 3 docsis-mode atdma
us-channel 3 equalization-coefficient
us-channel 3 frequency 10800000
us-channel 3 minislots-size 4
us-channel 3 modulation-profile 221
no us-channel 3 shutdown
us-channel 4 channel-width 1600000 1600000
us-channel 4 docsis-mode atdma
us-channel 4 frequency 12400000
us-channel 4 minislots-size 4
us-channel 4 modulation-profile 221
no us-channel 4 shutdown
us-channel 5 channel-width 1600000 1600000
us-channel 5 docsis-mode atdma
us-channel 5 frequency 14000000
us-channel 5 minislots-size 4
us-channel 5 modulation-profile 221

```

Configure RPD for US Controller Profile

To configure RPD for associating an upstream controller-profile, using the **rpds <port-id> Upstream-Cable <slot/sub-slot/controller> [profile <id>]** command, as given in the following example:

```

Router#cable rpd 1
  identifier 0004.9f00.0743
  core-interface Te8/1/0
  principal
  rpd-us 0 upstream-cable 8/0/0 profile 0
  rpd-us 1 upstream-cable 8/0/1 profile 4
  r-dti 11
  rpd-event profile 0
  rpd-55d1-us-event profile 0
---
end

```

The Remote PHY (R-PHY) Controller Profile now provides a new summary that displays the Per RPD us port description. The summary helps distinguish between the different controllers that share the same description of us-channels.

For example, the **show cable modem rpd all summary** command displays the following information:

```

Router#show cable modem rpd all summary

Load for five secs: 5%/0%; one minute: 5%; five minutes: 5%
No time source, *15:36:49.777 UTC Thu Mar 8 2018

RPD ID: badb.ad13.417c
Interface          Cable Modem          Description
  Total Reg Oper  Unreg Offline Wideband initRC initD initIO initO
C9/0/4/U0  1    0  0    1    0    0    1    0    0    0  badb.ad13.417c us
0
C9/0/4/U1  2    0  0    2    0    0    2    0    0    0  badb.ad13.417c us
0
C9/0/4/U3  1    0  0    1    0    0    1    0    0    0  badb.ad13.417c us
0
C9/0/5/U0  2    0  0    2    0    0    2    0    0    0  badb.ad13.417c us
1
C9/0/5/U1  1    0  0    1    0    0    1    0    0    0  badb.ad13.417c us
1

RPD ID: badb.ad13.41fa
Interface          Cable Modem          Description
  Total Reg Oper  Unreg Offline Wideband initRC initD initIO initO

```

```

C9/0/2/U0 2 0 0 2 0 1 1 0 0 1 badb.ad13.41fa
us 0
C9/0/2/U1 1 0 0 1 0 0 1 0 0 0 badb.ad13.41fa
us 0
C9/0/2/U3 1 0 0 1 0 0 1 0 0 0 badb.ad13.41fa
us 0
C9/0/3/U1 1 0 0 1 0 0 1 0 0 0 badb.ad13.41fa
us 1
C9/0/3/U2 2 0 0 2 0 0 2 0 0 0 badb.ad13.41fa
us 1
C9/0/3/U3 1 0 0 1 0 0 1 0 0 0 badb.ad13.41fa
us 1

```



Note The length of configurable limitation is 20 characters while there are 80 characters reserved.

Configure Downstream Controller Profile

To configure downstream controller profile, use the following commands:

```

configure terminal
cable downstream controller-profile <profile ID>
multicast-pool <id>
rf-chan 20 47
type video <SYNC | ASYNC>
frequency 231000000
rf-output NORMAL
qam-profile <profile ID>

```

The *multicast-pool <id>* defines the DEPI multicast group. The type video *<SYNC / ASYNC>* defines synchronous or asynchronous mode.

Verify Downstream Controller Profile Configuration

To verify the Downstream controller profile configuration, use the show cable downstream controller-profile command as shown in the following example:

```

Router#show running-config | section downstream controller-profile
cable downstream controller-profile 0
rf-chan 0 3
type DOCSIS
frequency 111000000
rf-output NORMAL
qam-profile 1
docsis-channel-id 1

```

Configure RPD for DS Controller Profile

To configure RPD for associating a downstream controller-profile, use the following commands:

```

configure terminal
cable rpd RPD01
identifier 0004.9f31.0435
core-interface Te3/1/0
principal
rpd-ds 0 downstream-cable 3/0/0 profile 1
rpd-ds 0 downstream-cable 3/0/1 profile 2

```

```

rpd-us 0 upstream-cable 3/0/0 profile 1
core-interface te6/1/0
rpd-ds 0 downstream-cable 6/0/0 profile 2
r-dti 1
rpd-event profile 0
rpd-55d1-us-event profile 0

```

The **rpd-ds 0 downstream-cable 3/0/0 profile 1** associates controller 3/0/0 with profile 1, which is a DOCSIS profile.

The **rpd-ds 0 downstream-cable 3/0/1 profile 2** associates controller 3/0/1 with profile 3, which is a video profile.

The *core-interface te6/1/0* defines an auxiliary interface for this RPD. This auxiliary interface is used to configure downstream sharing across line cards.

Verify RPD Association with Controller Profile

To verify the downstream controller profile association with RPD, use the **show running-config | section cable rpd <ID>** command as shown in the following example:

```

Router#show running-config | section cable rpd RPD01
cable rpd toi-test1
  identifier 0000.1cbf.0000
  core-interface Te2/1/0
  principal
  rpd-ds 0 downstream-cable 2/0/9 profile 0
  rpd-event profile 0
  rpd-55d1-us-event profile 0

```

Configure Analog Tx/Rx Modules Alarm Threshold

To adjust the alarm threshold of the analog Tx/Rx module in RPD node, use **analog** commands as shown in the following example:

```

configure terminal
cable rpd RPD01
  identifier 0004.9f31.0435
  core-interface Te3/1/0
  principal
  rpd-ds 0 downstream-cable 3/0/0 profile 1
  rpd-ds 0 downstream-cable 3/0/1 profile 2
  rpd-us 0 upstream-cable 3/0/0 profile 1
  r-dti 1
  rpd-event profile 0
  rpd-55d1-us-event profile 0
analog rx-power major-lo-th 0 minor-lo-th 50 normal-th 150 minor-hi-th 200
analog tx-power major-lo-th 0 minor-lo-th 50 normal-th 100 minor-hi-th 150

```

Verify Analog Tx/Rx Modules Alarm Threshold Configuration

To verify the analog Tx/Rx module alarm threshold configuration, use **show environment** commands in RPD as shown in the following example:

```

R-PHY#show environment table 49
sensor_id: 49
name: TX1_OPT_PWR_MON
.....
Configuration Values:

```

state	low	high
MAJOR-LOW	N/A	0.00
MINOR-LOW	0.00	0.59
NORMAL	0.60	1.09
MINOR-HIGH	1.10	1.59
MAJOR-HIGH	1.60	N/A

Configure Downstream Sharing

This configuration is optional. DS sharing is used for multicast (MC) traffic. To configure downstream sharing, use the following commands:

```
configure terminal
cable rpd RPD01
core-interface Te3/1/0
principal
rpd-ds 0 downstream-cable 3/0/1 profile 2
cable rpd RPD02
core-interface te3/1/0
principal
rpd-ds 0 downstream-cable 3/0/1 profile 2
```



Note All RDPs in the same multicast group should have the same controller and profile association.

Configure Controller in Fiber Node

To configure the controllers in fiber-node, use the **cable fiber-node** command, as given in the following example:

```
cable fiber-node 113
downstream Downstream-Cable 8/0/0
upstream Upstream-Cable 8/0/1
```

Verify CM RPD Association

To verify the RPD associated with the cable modem, use the **show cable modem rpd** command as shown in the following example:

```
Router# show cable modem rpd 0004.9f03.0249
Load for five secs: 4%/2%; one minute: 3%; five minutes: 4%
Time source is NTP, 10:48:11.763 CST Tue Feb 28 2017
```

MAC Address	IP Address	I/F	MAC State	Prim Sid	RxPwr (dBmV)	Timing Offset	Num CPE	I P
0023.be5a.bb6c	10.10.10.12	C6/0/0/UB	w-online	5	0.00	862	0	N
1859.3356.8876	10.10.10.13	C6/0/0/UB	w-online	6	0.50	907	0	N

Display GCP Related Information

To display Generic Control Plane (GCP) related information of the RPD, use the command as shown in the following example:

Display GCP Related Information

```
Router#show cable rpd 0004.9f03.0280 Te3/1/0 gcp-state
```

```
MAC Address      IP Address      I/F      State      Role HA Name
0004.9f03.0280  10.10.10.11    Te3/1/0  ready      Pri Act 2
```

```
A06#show cable rpd 0004.9f03.0280 Te3/1/0 gcp-state
```

```
MAC Address      IP Address      I/F      State      Role HA Name
0004.9f03.0280  10.10.10.11    Te3/1/0  ready      Pri Act 2
```

```
Router#show cable rpd name node tel1/1/0 gcp-session
```

```
GCP Session ID : 10
Core Address    : 10.100.10.11:8190
RPD Address     : 10.10.10.11:60656
Next Hop MAC    : 0004.9F00.0901
Session State   : Active
```

```
Packet Statistics:
```

```
=====
Rx           : 5038
Tx           : 5034
Rx Dropped  : 0
Tx Dropped  : 0
```

```
Message Statistics:
```

```
=====
Rx           : 5948
Tx           : 5954
Rx Dropped  : 7
Tx Dropped  : 0
Rx Illegal  : 0
Tx Illegal  : 0
```

```
Router#show cable rpd 120.102.6.7 te9/1/1 gcp-transaction
```

```
Load for five secs: 3%/1%; one minute: 4%; five minutes: 4%
No time source, *10:22:57.158 CST Thu Mar 16 2017
```

RPD ID	I/F	TRANS ID	GCP MSG TYPE	RCP MSG TYPE	TIMESTAMP
0004.9f31.1007 10:22:54.440	Te9/1/1	7452	GCP_MSG_ID_EDS_RSP	TYPE_REX	2017-03-16
0004.9f31.1007 10:22:54.415	Te9/1/1	7452	GCP_MSG_ID_EDS	TYPE_REX	2017-03-16
0004.9f31.1007 10:22:54.240	Te9/1/1	7451	GCP_MSG_ID_EDS_RSP	TYPE_REX	2017-03-16
0004.9f31.1007 10:22:54.215	Te9/1/1	7451	GCP_MSG_ID_EDS	TYPE_REX	2017-03-16
0004.9f31.1007 10:22:54.040	Te9/1/1	7450	GCP_MSG_ID_EDS_RSP	TYPE_REX	2017-03-16
0004.9f31.1007 10:22:54.015	Te9/1/1	7450	GCP_MSG_ID_EDS	TYPE_REX	2017-03-16
0004.9f31.1007 10:22:53.836	Te9/1/1	7449	GCP_MSG_ID_EDS_RSP	TYPE_REX	2017-03-16
0004.9f31.1007 10:22:53.815	Te9/1/1	7449	GCP_MSG_ID_EDS	TYPE_REX	2017-03-16
0004.9f31.1007 10:22:50.236	Te9/1/1	7448	GCP_MSG_ID_EDS_RSP	TYPE_REX	2017-03-16
0004.9f31.1007 10:22:50.215	Te9/1/1	7448	GCP_MSG_ID_EDS	TYPE_REX	2017-03-16
0004.9f31.1007 10:22:50.038	Te9/1/1	7447	GCP_MSG_ID_EDS_RSP	TYPE_REX	2017-03-16
0004.9f31.1007 10:22:50.015	Te9/1/1	7447	GCP_MSG_ID_EDS	TYPE_REX	2017-03-16

```

0004.9f31.1007 Te9/1/1 7446 GCP_MSG_ID_EDS_RSP TYPE_REX 2017-03-16
10:22:49.839
0004.9f31.1007 Te9/1/1 7446 GCP_MSG_ID_EDS TYPE_REX 2017-03-16
10:22:49.815

```

Display DEPI Related Information

To display the Downstream External PHY Interface (DEPI) related information, use the command as shown in the following example:

```
Router#show cable rpd depi
```

```

DEPI Tunnel and Session Information Total tunnels 1 sessions 26
LocTunID  RemTunID  Remote Device  State  Remote Address  Sessn L2TP Class
Count
338514820  671581873  0004.9f00.0901  est    10.10.10.11    26    rphy-l2tp-gl...

```

```

LocID      RemID      Pseudowire      State  Last Chg Uniq ID  Type Mode RemSt
0x41040008 0x00000B02 US1/0/0:2(R)    est    00:34:57 21    P    PSP  UP
0x41010000 0x00000600 US1/0/0:0(D)    est    00:34:57 11    P    PSP  UP
0x00002006 0x00000405 DS1/0/0:5       est    00:34:57 6     P    PSP  UP
0x00002004 0x00000403 DS1/0/0:3       est    00:34:57 4     P    PSP  UP
0x4100000C 0x00000D03 US1/0/0:3(M)    est    00:34:57 23    P    PSP  UP
0x00002002 0x00000401 DS1/0/0:1       est    00:34:57 2     P    PSP  UP
0x00002007 0x00000406 DS1/0/0:6       est    00:34:57 7     P    PSP  UP
0x00002008 0x00000407 DS1/0/0:7       est    00:34:57 8     P    PSP  UP
0x4101000C 0x00000603 US1/0/0:3(D)    est    00:34:57 24    P    PSP  UP
0x41000004 0x00000D01 US1/0/0:1(M)    est    00:34:57 15    P    PSP  UP
0x00002001 0x00000400 DS1/0/0:0       est    00:34:57 1     P    PSP  UP
0x41080008 0x00000F02 US1/0/0:2(S)    est    00:34:57 22    P    PSP  UP
0x41010004 0x00000601 US1/0/0:1(D)    est    00:34:57 16    P    PSP  UP
0x41020000 0x00000800 US1/0/0:0(B)    est    00:34:57 12    P    PSP  UP
0x00002009 0x00000408 DS1/0/0:8       est    00:34:57 9     P    PSP  UP
0x41010008 0x00000602 US1/0/0:2(D)    est    00:34:57 20    P    PSP  UP
0x41000008 0x00000D02 US1/0/0:2(M)    est    00:34:57 19    P    PSP  UP
0x4108000C 0x00000F03 US1/0/0:3(S)    est    00:34:57 26    P    PSP  UP
0x00002003 0x00000402 DS1/0/0:2       est    00:34:57 3     P    PSP  UP
0x41080000 0x00000F00 US1/0/0:0(S)    est    00:34:57 14    P    PSP  UP
0x41040004 0x00000B01 US1/0/0:1(R)    est    00:34:57 17    P    PSP  UP
0x41080004 0x00000F01 US1/0/0:1(S)    est    00:34:57 18    P    PSP  UP
0x41000000 0x00000D00 US1/0/0:0(M)    est    00:34:56 10    P    PSP  UP
0x00002005 0x00000404 DS1/0/0:4       est    00:34:56 5     P    PSP  UP
0x4104000C 0x00000B03 US1/0/0:3(R)    est    00:34:56 25    P    PSP  UP
0x41040000 0x00000B00 US1/0/0:0(R)    est    00:34:56 13    P    PSP  UP

```

```
outer#show cable rpd 0004.9f03.0214 te7/1/0 depi tunnel
```

```

Load for five secs: 7%/2%; one minute: 6%; five minutes: 6%
No time source, *12:41:44.228 CST Mon Mar 20 2017

```

```

LocTunID  RemTunID  Remote Device  State  Remote Address  Sessn L2TP Class
Count
3388764998 1054297851 0004.9f03.0214  est    10.10.10.11    29    rphy-l2tp-gl...

```

Table 25: show cable rpd depi Field Descriptions

Field	Description
LocID	Local session ID.

Field	Description
RemID	Remote session ID.
US1/0/0:2(R)	US means UEPI session, DS means DEPI session. This string means UEPI session on line card slot 1, controller 0, rf-channel 2.
est in State	Established state.
P in Type	On primary line card.

Troubleshooting Tips

Refer to the following troubleshooting tips if configuration errors occur.

If you configure DS controller profile and cable RPD, you can check the controller status, regardless of the status of the RPD. If the channel's state is DOWN, use verbose option to view the reason.

```
Router#show controllers downstream-Cable 6/0/1 rf-channel 20 <verbose>
Chan State Admin Frequency Type Annex Mod srate Interleaver dcid output
20 UP UP 231000000 VIDEO-SYNC B 256 5361 I128-J1 - NORMAL
```

Configuration Examples

This section provides example configurations for the R-PHY Controller Profile.

Example: Controller Profile Configuration

Upstream Controller Profile Configuration

```
configure terminal
cable upstream controller-profile 2
 cable def-phy-burst 0
 us-channel 0 chan-class-id 0
 us-channel 0 channel-width 1600000 1600000
 us-channel 0 docsis-mode atdma
 us-channel 0 equalization-coefficient
 us-channel 0 frequency 50000000
 us-channel 0 hop-priority frequency modulation channel-width
 us-channel 0 ingress-noise-cancellation 100
 us-channel 0 maintain-psd
 us-channel 0 max-logical-chans 1
 us-channel 0 minislots-size 4
 us-channel 0 modulation-profile 221
 us-channel 0 power-level 0
 us-channel 0 rng-holdoff 0
 us-channel 0 shutdown
 us-channel 0 specsvl error-adaptive-profile 1
 us-channel 0 threshold cnr-profiles 25 13
 us-channel 0 threshold corr-fec 3
 us-channel 0 threshold hysteresis 3
 us-channel 0 threshold snr-profiles 25 13
 us-channel 0 threshold uncorr-fec 1
 ...
end
```


Downstream Controller Profile Configuration

```
configure terminal
cable downstream controller-profile 1
multicast-pool 20
Rf-channel 0 15
Type docsis
Frequency 111000000
Rf-output NORMAL
Qam-profile 1
Docsis-channel-id 1
cable downstream controller-profile 2
multicast-pool 20
Rf-channel 20 47
Type video sync
Frequency 231000000
Rf-output NORMAL
Qam-profile 14
```

Example: Downstream Sharing Configuration

```
cable rpd RPD01
identifier 0004.9f31.0979
core-interface te6/1/0
principal
rpd-ds 0 downstream-cable 6/0/0 profile 1
rpd-ds 0 downstream-cable 6/0/1 profile 2
rpd-us 0 upstream-cable 6/0/0 profile 1
r-dti 6
rpd-event profile 0
rpd-55dl-us-event profile 0
cable rpd RPD2
identifier 0004.9f31.1437
core-interface Te3/1/0
principal
rpd-ds 0 downstream-cable 3/0/0 profile 1
rpd-us 0 upstream-cable 3/0/0 profile 1
core-interface Te6/1/0
rpd-ds 0 downstream-cable 6/0/1 profile 2
r-dti 3
rpd-event profile 0
rpd-55dl-us-event profile 0
```

Feature Information for Remote PHY Controller Profile and RPD Configuration

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



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

Table 26: Feature Information for Remote PHY Controller Profile and RPD Configuration

Feature Name	Releases	Feature Information
Large Scale Controller Support (32DS/64US) with node	Cisco 1x2 / Compact Shelf RPD Software 3.1	This feature was integrated into the Cisco Remote PHY Device.
256 RPD Support per Chassis	Cisco 1x2 / Compact Shelf RPD Software 3.1	This feature was integrated into the Cisco Remote PHY Device.
Controller profile configuration	Cisco 1x2 / Compact Shelf RPD Software 3.1	This feature was integrated into the Cisco Remote PHY Device.
US 128 channels	Cisco 1x2 / Compact Shelf RPD Software 3.1	This feature was integrated into the Cisco Remote PHY Device.



CHAPTER 15

Cisco Remote PHY Device Downstream Virtual Splitting

This document provides information on how to configure downstream virtual splitting on Remote PHY systems.

Finding Feature Information

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

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

- [Hardware Compatibility Matrix for Cisco Remote PHY Device, on page 95](#)
- [Information about RPD Downstream Virtual Splitting, on page 96](#)
- [Configure RPD Downstream Virtual Splitting, on page 96](#)
- [Example: RPD Downstream Virtual Splitting Configuration, on page 102](#)
- [Feature Information for RPD Downstream Virtual Splitting, on page 103](#)

Hardware Compatibility Matrix for Cisco Remote PHY Device



Note Unless otherwise specified, the hardware components introduced in a given Cisco Remote PHY Device Software Release are supported in all subsequent releases.

Table 27: Hardware Compatibility Matrix for the Cisco Remote PHY Device

Cisco HFC Platform	Remote PHY Device
Cisco GS7000 Super High Output Node	Cisco 1x2 / Compact Shelf RPD Software 2.1 and Later Releases

Cisco HFC Platform	Remote PHY Device
Cisco GS7000 Super High Output Intelligent Node (iNode)	Cisco 1x2 / Compact Shelf RPD Software 4.1 and Later Releases Cisco Intelligent Remote PHY Device 1x2 <ul style="list-style-type: none"> • PID—iRPD-1X2= • PID—iRPD-1X2-PKEY=



Note The -PKEY suffix in the PID indicates units that enable the SCTE-55-2 Out-of-Band protocol support.

Information about RPD Downstream Virtual Splitting

The primary use case for multicast delivery between CCAP-core and the RPD is for the delivery of broadcast video services from a single CCAP-core element to a number of RPDs. This allows the system to scale by allowing a single CCAP-core element to generate and serve streams to all the RPDs that are configured to receive the same broadcast lineup. Since broadcast serving groups are quite large (~100,000 or more subscribers), using multicast to deliver the same copy to hundreds of remote PHY devices provides significant cost savings for operators. This mechanism can be used for broadcast video delivered via MPEG QAM channels or for that delivered via IP over DOCSIS. It is meant for the replication of an entire QAM channel to multiple RPDs.

Configure RPD Downstream Virtual Splitting

This section describes how to configure RPD Downstream Virtual Splitting on Cisco cBR-8.



Note To know more about the commands referenced in this module, see the [Cisco IOS Command List](#).

Configure Multicast DEPI Pool

To configure the multicast DEPI pool, complete the following procedure:

```
configure terminal
cable depi multicast pool id
{ip|ipv6} address ip mask
```

To verify the multicast DEPI pool configuration, use the **show cable depi multicast pool** command as shown in the example below:

```
Router# show cable depi multicast pool
Load for five secs: 4%/0%; one minute: 5%; five minutes: 5%
No time source, *09:23:41.545 CST Mon Apr 23 2018
POOL ID      Net IP          Net Mask        Redundant DESCRIPTION
1            227.0.0.0      255.255.255.0  FALSE
```

```

2          228.0.0.0          255.255.254.0    FALSE
127       227.226.225.0    255.255.255.0    FALSE    to TE9/1/1+TE9/1/7

POOL ID   IPv6                                Redundant DESCRIPTION
6         FF3A::9000:0/126              FALSE

```

Configure Redundant Multicast DEPI Pool

When a secondary line card is configured, multicast IP addresses are assigned to its downstream controllers from the redundant multicast DEPI pool.

To configure the redundant multicast DEPI pool, complete the following procedure:

```

configure terminal
cable depi multicast pool id
redundant

```

To verify the multicast DEPI pool configuration, use the **show cable depi multicast pool** command as shown in this example:

```

Router# show cable depi multicast pool
Load for five secs: 4%/0%; one minute: 4%; five minutes: 4%
No time source, *14:14:13.780 CST Tue Aug 7 2018
POOL ID   Net IP          Net Mask        Redundant DESCRIPTION
1         227.0.0.0       255.255.0.0     FALSE
127      227.226.225.0  255.255.255.0  FALSE    to TE9/1/1+TE9/1/7

POOL ID   IPv6                                Redundant DESCRIPTION
2         FF39::8000:0/120  FALSE
4         FF39::9000:0/112  TRUE

```

To view the IPv6 addresses assigned to the secondary linecard downstream controllers, use the **show cable depi multicast ipv6 all** command as shown in this example:

```

Router# show cable depi multicast ipv6 all
Load for five secs: 5%/0%; one minute: 5%; five minutes: 4%
No time source, *14:15:08.476 CST Tue Aug 7 2018
IPv6                                POOL ID   CONTROLLER
FF39::9000:0                         4         0/0/0 (1-Te0/1/0)
FF39::9000:8                         4         0/0/1 (2-Te0/1/0)
FF39::9000:10                       4         0/0/2 (3-Te0/1/0)
FF39::9000:18                       4         0/0/3 (4-Te0/1/0)
FF39::9000:20                       4         0/0/4 (5-Te0/1/0)

```



Note

- To view the IPv4 addresses, use the **show cable depi multicast ip all** command.
- One redundant DEPI pool is available for either IPv4 or IPv6 addresses.
- If you do not configure redundant pool, secondary linecard downstream controllers use the same IP as the downstream controllers in the primary linecard.
- You cannot use the redundant multicast pool in the downstream controller profile configuration.
- DEPI multicast pool can be configured as redundant pool if DEPI multicast pool contains less than 266 IP addresses, and if line card high availability is configured on the Cisco cBR-8.

Enable Multicast Sharing under Downstream Controller Profile

To enable the multicast sharing under downstream controller profile, complete the following procedure:

```
configure terminal
cable downstream controller-profile id
multicast-pool id
```

Then configure the other parameters of the controller profile and related RF channels.

Starting from Cisco 1x2 / Compact Shelf RPD Software 3.1, user can change the multicast pool for the downstream sharing controllers without configuring the RPD. See the following example for detailed configuration:

```
Router#config terminal
Router(config)#cable downstream controller-profile 111
Warning: changes to this profile will affect the following controllers:
Downstream controller-profile 111 is being used by controller Downstream-Cable:
        6/0/0, 6/0/1,
```

```
Confirm to continue? [no]: yes
Router(config-controller-profile)#multicast-pool 50
This profile is being used by the following RPDs:
Controller RPD DS Port List:
  RPD ID           I/F           Name
  -----
  0004.9f03.0214   Te6/1/0      rpd_b
  000c.2923.9991   Te6/1/0      rpd_a      ...
```

```
Confirm to continue? [no]: yes
```

To verify the multicast sharing is enabled under the downstream controller profile, use the **show cable downstream controller-profile** command as shown in the example below:

```
Router# show cable downstream controller-profile 1
Load for five secs: 8%/1%; one minute: 10%; five minutes: 10%
No time source, *07:14:32.551 CST Tue Nov 15 2016
Downstream controller-profile 1
Description:
Downstream controller-profile 1 is being used by controller Downstream-Cable:
  3/0/0,
  Admin: UP
  MaxOfdmSpectrum: 0
  MaxCarrier: 128
  BasePower: 33.0 dBmV
  Mode: normal
  Frequency profile: unconfigured
  DS Splitting: Yes
  Multicast Pool ID: 1
```

Configure the RPD with the Same Downstream Controller and Profile

To configure the RPDs with the same downstream controller and profile, complete the following procedure:

```
configure terminal
cable rpd name
identifier id
core-interface TenGigabitEthernet slot/subslot/port
principal
rpd-ds 0 downstream-cable slot/subslot/port profile id
```

```

rpd-us 0 upstream-cable slot/subslot/port profile id
r-dti id
rpd-event profile id
rpd-55d1-us-event profile id

```



Note Configure at least 2 RPDs with the same downstream controller and profile to implement the multicast DEPI.

Configure the RPDs to different fiber-nodes

To configure the RPDs to different fiber-nodes, complete the following procedure:

```

configure terminal
cable fiber-node id
downstream Downstream-Cable slot/subslot/port
upstream Upstream-Cable slot/subslot/port

```



Note Configure at least 2 fiber-nodes with the same downstream controller to implement the multicast DEPI.

Configure the RPDs to MAC Domain

To configure the RPDs to the MAC domain, complete the following procedure:

```

configure terminal
interface cable slot/subslot/port
downstream Downstream-Cable slot/subslot/port rf-channel id
upstream index Upstream-Cable slot/subslot/port us-channel index
cable upstream index jumbo-grants
cable upstream balance-scheduling
cable upstream bonding-group id
upstream id
attributes 800000F0
cable bundle id
cable map-advancestatic value
cable sid-cluster-group num-of-cluster value
cable sid-cluster-switching max-request value

```



Note Different RPDs can be configured to share the same downstream controller under one MAC domain or different MAC domains.

Enable Multicast on Cisco cBR-8 Router

To enable the multicast on cBR-8, complete the following procedure:

```
configure terminal
ip multicast-routing distributed
```

Enable Multicast on Layer 2 Switch

To enable multicast on Layer 2 switch, complete the following procedure:

```
configure terminal
ip igmp snooping
vlan configuration vlan
ip igmp snooping querier ip
```

Only need to create IGMP Snooping Group on one switch between DPIC and RPD.

Create IGMP Snooping Group under vlan which is used for connection between DPIC and RPD.

IP address used for IGMP snooping querier can be any address that is not conflict with the existing IP address in the system.

Enable Multicast on Layer 3 Router

To enable multicast on Layer 3 router, complete the following procedure:

```
configure terminal
ip pim ssm default
interface gigabitEthernet 0/0/0
ip pim sparse-dense-mode
ip igmp version 3
```

SSM must be enabled on all routers between DPIC and RPD.

All PIM neighbor must be enabled on all routers.

PIM neighbor can use sparse-dense-mode or sparse-mode.

Verify RPD Downstream Virtual Splitting Configuration on cBR-8 Side

To verify the RPD Downstream Virtual Splitting configuration on cBR-8 side, complete the procedure as shown in the example below, and check if these criteria are met:

- The remote session ID begins with 0x8 in the output of the **show cable rpd depi | in Ds** command.

```
Router# show cable rpd depi | in Ds
0x40003F21 0x80003D22 1377638051 Ds3/0/0:0      est  04:20:36 1      P
0x40003F31 0x80003D32 1377638051 Ds3/0/0:16     est  04:20:35 3      P
0x40003F41 0x80003D42 1377638051 Ds3/0/0:32     est  04:20:35 5      P
0x40003F39 0x80003D3A 1377638051 Ds3/0/0:24     est  04:20:35 4      P
0x40003F29 0x80003D2A 1377638051 Ds3/0/0:8      est  04:20:34 2      P
0x40103F21 0x80003D22 1404837649 Ds3/0/0:0      est  00:07:21 14     P
0x40103F39 0x80003D3A 1404837649 Ds3/0/0:24     est  00:07:21 17     P
0x40103F41 0x80003D42 1404837649 Ds3/0/0:32     est  00:07:21 18     P
0x40103F29 0x80003D2A 1404837649 Ds3/0/0:8      est  00:07:21 15     P
0x40103F31 0x80003D32 1404837649 Ds3/0/0:16     est  00:07:21 16     P
```

- There is assigned IP and pool ID in the output of the **show cable depi multicast ip all** command.

```
Router# show cable depi multicast ip all
Load for five secs: 7%/2%; one minute: 8%; five minutes: 8%
```



```
No time source, *23:00:55.344 CST Sun Nov 13 2016
ASSIGNED IP      POOL ID    CONTROLLER
225.225.225.0    1           3/0/0
```

- The cable modem is online in the output of the **show cable modem rpd** command.

```
Router# show cable modem
```

```
Load for five secs: 8%/3%; one minute: 9%; five minutes: 9%
No time source, *16:06:52.191 CST Thu Mar 2 2017
```

D	MAC Address	IP Address	I/F	MAC	Prim	RxPwr	Timing	Num
I								
P				State	Sid	(dBmv)	Offset	CPE
N	5039.558a.6c1c	40.242.0.17	C7/0/0/U1	online	5	0.50	816	0
N	5039.558a.754a	40.242.9.201	C7/0/0/U0	online	6	0.00	814	0
N	5039.558a.754e	40.242.9.207	C7/0/0/U0	online	7	0.00	814	0
N	5039.558a.6b98	40.242.0.16	C7/0/0/U0	online	8	0.00	817	0
N	0025.2e34.4380	40.242.62.172	C7/0/1/U1	online	2	0.00	783	0

```
Router# show cable rpd
```

```
Load for five secs: 8%/3%; one minute: 9%; five minutes: 9%
No time source, *16:06:55.706 CST Thu Mar 2 2017
```

MAC Address	IP Address	I/F	State	Role	HA	Name
0004.9f03.0214	120.105.4.7	Te7/1/0	online	Pri	Act	rp_d_b
000c.2923.9991	120.105.4.6	Te7/1/0	online	Pri	Act	rp_d_a
000c.2923.9991	120.105.4.6	Te6/1/0	online	Aux	Act	rp_d_a

```
Router# show cable modem rpd 0004.9f03.0214
```

```
Load for five secs: 8%/3%; one minute: 9%; five minutes: 9%
No time source, *16:07:07.790 CST Thu Mar 2 2017
```

D	MAC Address	IP Address	I/F	MAC	Prim	RxPwr	Timing	Num
I								
P				State	Sid	(dBmv)	Offset	CPE
N	5039.558a.6c1c	40.242.0.17	C7/0/0/U1	online	5	0.50	816	0
N	5039.558a.754a	40.242.9.201	C7/0/0/U0	online	6	0.00	814	0
N	5039.558a.754e	40.242.9.207	C7/0/0/U0	online	7	0.00	814	0

Verify RPD Virtual Downstream Splitting Configuration on Node Side

To verify the RPD Downstream Virtual Splitting configuration on node side, complete the procedure on RPD as shown in the example below, and check if these criteria are met:

- All L2TP session ID must start with 800.

```
RPD# show l2tp session
```

```
L2TP Tunnel Information Total tunnels 1 sessions 13
LocSessID RemSessID LocTunID RemTunID State Type Last Chg
```

Example: RPD Downstream Virtual Splitting Configuration

```

80003d22 40103f21 9fef9255 53bc1f11 est MCM 07:10:54 2016-11-13
80003d2a 40103f29 9fef9255 53bc1f11 est MCM 07:10:57 2016-11-13
80003d42 40103f41 9fef9255 53bc1f11 est MCM 07:10:56 2016-11-13
80003d32 40103f31 9fef9255 53bc1f11 est MCM 07:10:59 2016-11-13
80003d3a 40103f39 9fef9255 53bc1f11 est MCM 07:10:56 2016-11-13

```

- All downstream DEPI SrcIP must be multicast IP that is the same as cBR-8 side.

```

RPD# show downstream depi configuration
Channel PwSubtype      SessionId SrcIp
0       MCM             2147499298 225.225.225.0
8       MCM             2147499306 225.225.225.0
16      MCM             2147499314 225.225.225.0
24      MCM             2147499322 225.225.225.0
32      MCM             2147499330 225.225.225.0

```

Example: RPD Downstream Virtual Splitting Configuration

The following example shows how to configure RPD Downstream Virtual Splitting:

```

Router# configure terminal
Router(config)# cable depi multicast pool 1
Router(config-multicast-pool)# ip address 225.225.225.0 255.255.255.0
Router(config-multicast-pool)# exit
Router(config)# cable downstream controller-profile 0
Router(config-controller-profile)# multicast-pool 1
Router(config-controller-profile)# max-carrier 128
Router(config-controller-profile)# base-channel-power 34
Router(config-controller-profile)# rf-chan 0 95
Router (config-prof-rf-chan)# type DOCSIS
Router (config-prof-rf-chan)# frequency 285000000
Router (config-prof-rf-chan)# rf-output NORMAL
Router (config-prof-rf-chan)# qam-profile 1
Router (config-prof-rf-chan)# power-adjust 0
Router (config-prof-rf-chan)# docsis-channel-id 1
Router (config-prof-rf-chan)# end
Router# configure terminal
Router(config)# cable rpd node_1
Router(config-rpd)# identifier 0004.9f03.0214
Router(config-rpd)# core-interface Te9/1/0
Router(config-rpd-core)# principal
Router(config-rpd-core)# rpd-ds 0 downstream-cable 9/0/0 profile 0
Router(config-rpd-core)# rpd-us 0 upstream-cable 9/0/0 profile 221
Router(config-rpd-core)# exit
Router(config-rpd)# r-dti 20
Router(config-rpd)# rpd-event profile 0
Router(config-rpd)# rpd-55d1-us-event profile 0
Router(config-rpd)# exit
Router(config)# cable rpd node_2
Router(config-rpd)# identifier 000c.2923.9991
Router(config-rpd)# core-interface Te9/1/0
Router(config-rpd-core)# principal
Router(config-rpd-core)# rpd-ds 0 downstream-cable 9/0/0 profile 0
Router(config-rpd-core)# rpd-us 0 upstream-cable 9/0/1 profile 221
Router(config-rpd-core)# exit
Router(config-rpd)# r-dti 20
Router(config-rpd)# rpd-event profile 0
Router(config-rpd)# rpd-55d1-us-event profile 0
Router(config-rpd)# exit
Router(config)# cable fiber-node 100
Router(config-fiber-node)# downstream Downstream-Cable 9/0/0

```

```

Router(config-fiber-node)# upstream Upstream-Cable 9/0/0
Router(config-fiber-node)# exit
Router(config)# cable fiber-node 101
Router(config-fiber-node)# downstream Downstream-Cable 9/0/0
Router(config-fiber-node)# upstream Upstream-Cable 9/0/1
Router(config-fiber-node)# exit
Router(config)# interface Cable 9/0/0
Router(config-if)# downstream Downstream-Cable 9/0/0 rf-channel 0
Router(config-if)# downstream Downstream-Cable 9/0/0 rf-channel 8
Router(config-if)# upstream 0 Upstream-Cable 9/0/0 us-channel 0
Router(config-if)# upstream 1 Upstream-Cable 9/0/0 us-channel 1
Router(config-if)# upstream 2 Upstream-Cable 9/0/0 us-channel 2
Router(config-if)# upstream 3 Upstream-Cable 9/0/0 us-channel 3
Router(config-if)# upstream 4 Upstream-Cable 9/0/1 us-channel 0
Router(config-if)# upstream 5 Upstream-Cable 9/0/1 us-channel 1
Router(config-if)# upstream 6 Upstream-Cable 9/0/1 us-channel 2
Router(config-if)# upstream 7 Upstream-Cable 9/0/1 us-channel 3
Router(config-if)# cable upstream 0 jumbo-grants
Router(config-if)# cable upstream balance-scheduling
Router(config-if)# cable upstream bonding-group 1
Router(config-upstream-bonding)# upstream 0
Router(config-upstream-bonding)# upstream 1
Router(config-upstream-bonding)# upstream 2
Router(config-upstream-bonding)# upstream 3
Router(config-upstream-bonding)# attributes 800000F0
Router(config-upstream-bonding)# exit
Router(config-if)# cable upstream bonding-group 2
Router(config-upstream-bonding)# upstream 4
Router(config-upstream-bonding)# upstream 5
Router(config-upstream-bonding)# upstream 6
Router(config-upstream-bonding)# upstream 7
Router(config-upstream-bonding)# attributes 8000000F
Router(config-upstream-bonding)# exit
Router(config-if)# cable bundle 1
Router(config-if)# cable map-advance static 1000
Router(config-if)# cable sid-cluster-group num-of-cluster 2
Router(config-if)# cable sid-cluster-switching max-request 2
Router(config-if)# exit
Router(config)# ip multicast-routing distributed
Router(config)# interface TenGigabitEthernet 9/1/0
Router(config-if)# ip address 192.168.3.1 255.255.255.0
Router(config-if)# end

```

Feature Information for RPD Downstream Virtual Splitting

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



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

Table 28: Feature Information for RPD Downstream Virtual Splitting

Feature Name	Releases	Feature Information
DS virtual splitting	Cisco 1x2 / Compact Shelf RPD Software 3.1	This feature was integrated into the Cisco Remote PHY Device.



CHAPTER 16

Cisco Remote PHY DS OFDM Channel Configuration

This document provides information on how to configure DOCSIS 3.1 DS OFDM channel on Remote PHY systems.

Finding Feature Information

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

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

- [Hardware Compatibility Matrix for Cisco Remote PHY Device, on page 105](#)
- [Information About R-PHY DOCSIS 3.1 DS OFDM Channel, on page 106](#)
- [Configure DS OFDM Channel, on page 106](#)
- [Configuration Example, on page 115](#)
- [Feature Information for RPHY DS OFDM Channel Configuration, on page 115](#)

Hardware Compatibility Matrix for Cisco Remote PHY Device



Note Unless otherwise specified, the hardware components introduced in a given Cisco Remote PHY Device Software Release are supported in all subsequent releases.

Table 29: Hardware Compatibility Matrix for the Cisco Remote PHY Device

Cisco HFC Platform	Remote PHY Device
Cisco GS7000 Super High Output Node	Cisco 1x2 / Compact Shelf RPD Software 2.1 and Later Releases

Cisco HFC Platform	Remote PHY Device
Cisco GS7000 Super High Output Intelligent Node (iNode)	Cisco 1x2 / Compact Shelf RPD Software 4.1 and Later Releases Cisco Intelligent Remote PHY Device 1x2 <ul style="list-style-type: none"> • PID—iRPD-1X2= • PID—iRPD-1X2-PKEY=



Note The -PKEY suffix in the PID indicates units that enable the SCTE-55-2 Out-of-Band protocol support.

Information About R-PHY DOCSIS 3.1 DS OFDM Channel

Cisco cBR routers support DS OFDM channels in an R-PHY system. The OFDM-channel-support includes two OFDM channels for each Remote PHY device (RPD) with a channel bandwidth up to 192 MHz and the modulation up to 4096 QAM.

RPD supports up to 128 SC-QAM channels in the presence of 2 OFDM channels. If more than 128 SC-QAM channels are already configured, then user needs to configure the RPD core to reduce the number of SC-QAM channel before the second OFDM can be configured.

Each OFDM channel supports a control profile, the NCP profile, and up to five data profiles. For a line card, a maximum of 32 DS OFDM channels are supported.

Configure DS OFDM Channel

Configure OFDM Channel Profile

To configure the OFDM channel profile, run the following commands:

```
enable
configure terminal

cable downstream ofdm-chan-profile id
  description System Profile id
  cyclic-prefix value
  interleaver-depth value
  pilot-scaling value
  roll-off value
  subcarrier-spacing value
  profile-control {modulation-default mod_prof_id | modulation-profile mod_prof_id}
  profile-ncp modulation-default <mod_prof_id>
  profile-data channel_data_prof_id {modulation-default mod_prof_id | modulation-profile mod_prof_id}
```

Configure RPD Port/Controller and Channel

To configure the port or controller and channel, use the following commands.

```
enable
configure terminal
cable rpd <rpd_name_string>
  identifier <xxxx.xxxx.xxxx>
  core-interface Te slot/subslot/port
  principal
  rpd-ds <port> downstream-cable slot/subslot/port profile <ID>
  rpd-us <port> upstream-cable slot/subslot/port profile <ID>

cable downstream controller-profile <ID>
max-ofdm-spectrum value

rf-chan [id]
type DOCSIS
frequency value
  rf-output NORMAL
  qam-profile id
  docsis-channel-id id
rf-chan [id]
  docsis-channel-id id
  ofdm channel-profile id start-frequency value width value [plc value]
```

The OFDM channel IDs range from 158 to 162.

In the following example, 2 OFDM channels 158 and 159 are configured:

```
Router# configure terminal
Router(config)# cable downstream controller-profile 6
Router(config-controller-profile)# max-carrier 128
Router(config-controller-profile)# max-ofdm-spectrum 384000000
Router(config-controller-profile)# rf-chan 0 23
Router(config-prof-rf-chan)# type DOCSIS
Router(config-prof-rf-chan)# qam-profile 1
Router(config-prof-rf-chan)# frequency 453000000
Router(config-prof-rf-chan)# rf-output NORMAL
Router(config-prof-rf-chan)# docsis-channel-id 1
Router(config-prof-rf-chan)# exit
Router(config-controller-profile)# rf-chan 158
Router(config-prof-rf-chan)# docsis-channel-id 159
Router(config-prof-rf-chan)# ofdm channel-profile 20 start-frequency 645000000 width 192000000
  plc 651000000
Router(config-prof-rf-chan)# exit
Router(config-controller-profile)# rf-chan 159
Router(config-prof-rf-chan)# docsis-channel-id 160
Router(config-prof-rf-chan)# ofdm channel-profile 20 start-frequency 837000000 width 192000000
  plc 930000000

Router(config)# cable rpd node0
Router(config-rpd)# identifier 0004.9f31.1234
Router(config-rpd)# core-interface Te9/1/0
Router(config-rpd-core)# principal
Router(config-rpd-core)# rpd-ds 0 downstream-cable 9/0/12 profile 6
Router(config-rpd-core)# rpd-us 0 upstream-cable 9/0/0 profile 3
Router(config-rpd-core)# exit
Router(config-rpd)# r-dti 8
Router(config-rpd)# rpd-event profile 0
Router(config-rpd)# rpd-55d1-us-event profile 0
```

Configure RF Channel Bandwidth in Wideband Interface

To add the RF channel to a wideband interface, and to specify the RF channel bandwidth allocated for the channel, use the following commands:



Note Cisco cBR router does not support Dynamic Bandwidth Sharing (DBS). Hence, the bandwidth-percentage value does not apply.

```
enable
configure terminal
interface Wideband-Cable{slot/subslot/port}:wideband-channel
cable bundle id
cable rf-channels channel-list grouplist bandwidth-percent percentage-bandwidth
```

Verify the Profile Ordering

To view the details of the profile downgrade ordering on a specific OFDM channel, run the following command:

```
Router#show controllers downstream-cable 7/0/0 rf-channel 158 prof-order
```

```
OFDM channel data profile order: [2/0/3:158]
```

```
-----
Data Profile:      Downgrade Profile:
Profile 1         ->   Profile 0
Profile 2         ->   Profile 1
Profile 3         ->   Profile 2
```

Verify OFDM Channel Profile

To view the details of an OFDM Channel Profile, run the following command:

```
Router# show controllers downstream-Cable 7/0/0 rf-channel 158 verbose
```

```
Chan State Admin Mod-Type Start      Width      PLC      Profile-ID dcid output
                Frequency
158  UP    UP    OFDM      807000000  192000000  963000000  20    162  NORMAL
Resource status: OK
License: granted <20:11:58 CST Jul 3 2017>
OFDM channel license spectrum width: 128200000
Config lock status: Open
OFDM config state: Configured
```

```
OFDM channel details: [7/0/0:158]
```

```
-----
OFDM channel frequency/subcarrier range : 807000000[ 128] - 998999999[3967]
OFDM spectrum frequency/subcarrier range : 800600000[  0] - 1005399999[4095]
Active spectrum frequency/subcarrier range : 808900000[ 166] - 997049999[3929]
OFDM channel center frequency/subcarrier : 903000000[2048]
PLC spectrum start frequency/subcarrier  : 963000000[3248]
PLC frequency/subcarrier                  : 965800000[3304]
Channel width                             : 192000000
Active Channel width                       : 128200000
OFDM Spectrum width                       : 204800000
Chan prof id                              : 20
Cyclic Prefix                             : 1024
```



```

Roll off : 128
Interleave depth : 16
Spacing : 50KHZ
Pilot Scaling : 48
Control modulation default : 1024
NCP modulation default : 16
Data modulation default : None
Data modulation profile : None
Lower guardband width in freq/subcarriers : 1900000[38]
Upper guardband width in freq/subcarriers : 1900000[38]

PLC spectrum frequencies [subcarriers] :
 963000000[3248] - 968999999[3367]

PLC channel frequencies [subcarriers] :
 965800000[3304] - 966199999[3311] Size: 8 subcarriers

Excluded frequencies [subcarriers] :
800600000[ 0] - 808899999[ 165] 865000000[1288] - 924999999[2487]
997100000[3930] - 1005399999[4095]
Count: 1532

Pilot frequencies [subcarriers] :
*:PLC pilots
810150000[ 191] 812700000[ 242] 815250000[ 293] 817800000[ 344]
820350000[ 395] 822900000[ 446] 825450000[ 497] 828000000[ 548]
830550000[ 599] 833100000[ 650] 835650000[ 701] 838200000[ 752]
840750000[ 803] 843300000[ 854] 845850000[ 905] 848400000[ 956]
Count: 4

Active frequencies [subcarriers] :
808900000[ 166] - 864999999[1287] 925000000[2488] - 997099999[3929]
Count: 2564

Data frequencies [subcarriers] :
808900000[ 166] - 810149999[ 190] 810200000[ 192] - 812699999[ 241]
812750000[ 243] - 815249999[ 292] 815300000[ 294] - 817799999[ 343]
817850000[ 345] - 820349999[ 394] 820400000[ 396] - 822899999[ 445]
822950000[ 447] - 825449999[ 496] 825500000[ 498] - 827999999[ 547]

..
Count: 2500

Profiles:
Number of profiles: 2
CTRL profile (Profile A): rate: 864000 kbps
Active frequencies [subcarriers]:
Modulation:Start-freq[start-subcarrier] - End-freq[end-subcarrier]
-----
1024 :808900000[ 166] - 810100000[ 190] 1024 :810200000[ 192] - 812650000[ 241]
1024 :812750000[ 243] - 815200000[ 292] 1024 :815300000[ 294] - 817750000[ 343]
1024 :817850000[ 345] - 820300000[ 394] 1024 :820400000[ 396] - 822850000[ 445]
1024 :822950000[ 447] - 825400000[ 496] 1024 :825500000[ 498] - 827950000[ 547]

...

Active subcarrier count: 2500, ZBL count: 0
Discontinuity time [days:hours:mins:secs]: 00:00:00:00

NCP profile:
Active frequencies [subcarriers]:
Modulation:Start-freq[start-subcarrier] - End-freq[end-subcarrier]
-----
16 :808900000[ 166] - 810100000[ 190] 16 :810200000[ 192] - 812650000[ 241]

```

Verify OFDM Channel

```

16 :812750000[ 243] - 815200000[ 292]    16 :815300000[ 294] - 817750000[ 343]
16 :817850000[ 345] - 820300000[ 394]    16 :820400000[ 396] - 822850000[ 445]
16 :822950000[ 447] - 825400000[ 496]    16 :825500000[ 498] - 827950000[ 547]
...
Active subcarrier count: 2500, ZBL count: 0

CCCs:
OCD CCC: 1
DPD CCCs:
Control profile (Profile A) CCC: 1
NCP profile CCC: 1
Resource config time taken: 29 msec
JIB channel number: 768
Chan Pr  EnqQ  Pipe  RAF  SyncTmr  DqQ  ChEn  RAF  Tun#  SessionId  Valid  P/S  XFI  0[TkbRt  MaxP]
1[TkbRt  MaxP]
768  0  384    0  308      0  384  1    5551  0    16778240  TRUE  0  0  479610000  4485120
383688000  4485120
768  1  384    0  4786     0  384  1    2190  0    16778240  TRUE  0  0  479610000  4485120
383688000  4485120
Encap Chan-id Data:0 PLC:5
Chan  Qos-Hi  Qos-Lo  Med-Hi  Med-Lo  Low-Hi  Low-Lo
768   24576  16384   24576  16384   40960   24576
Chan  Med  Low  TB-neg  Qos_Exc  Med_Xof  Low_Xof  Qdrops(H-M-L)  Pos  Qlen(Hi-Med-lo)  Fl  Tgl_cnt
Rdy_sts
768   0  0    0      0      0      0  0  0  0  0  Y  0  0  0  0
0 ff
Chan  Rate  Neg  Pos  LastTS  CurrCr  Pos  [PLC Rate Neg Pos]
768  10485750  65535  65535  123395759  268431360  Y  [MM 86 128 1024][EM 87 128 6144][TR 2
9 3072]

```

Verify OFDM Channel

To view the details of an OFDM channel, run the following command:

```
Router#show controllers downstream-Cable 7/0/0 counter ofdm-channel
```

Controller	Chan#	Profile/PLC	Packets	Bytes	MaxRate (Mbps)	Rate (Mbps)	Utilization (%)
7/0/0	158	Total	101694	9225522	-	0.015590	0.0
7/0/0	158	0	29216	2557604	864	0.004551	0.0
7/0/0	158	PLC-MMM	72474	6667608		0.011039	
7/0/0	158	PLC-EM	0	0		0.000000	
7/0/0	158	PLC-TR	0	0		0.000000	

Verify OCD and DPD of MAC Domain

To display the MAC domain's OFDM Channel Descriptor (OCD) and Downstream Profile Descriptor (DPD) messages, use the **show cable mac-domain dpd | ocd** command in privileged EXEC mode.

```
Router# show cable mac-domain cable 7/0/0 ocd
```

```
DCID: 162 OFDM Controller:channel 7/0/0:158
```

```
OCD Message
MAC Header
  Frame Control          : 0xC2 (MAC specific, MAC msg, EHDR Off)
  MAC Parameters        : 0x0
  Length                 : 190
  Header Check Sequence : 0x84A2 (33954)
```

```

MAC Management Header
?
  Destination MAC ADDR      : 01e0.2f00.0001
  Source MAC ADDR          : c414.3c17.3ead
  Length                    : 172
  Destination SAP          : 0
  Source SAP                : 0
  Control                   : 3
  Version                   : 5
  Type                      : 49
  Multipart                 : 0      (Sequence number 0, Fragments 0)
OCD fields
  DCID                      : 162
  CCC                       : 1
  TLV 0 Spacing             : 50 KHz
  TLV 1 Cyclic Prefix       : 1024 samples
  TLV 2 Rolloff             : 128 samples
  TLV 3 Spectrum Location   : 800600000 Hz
  TLV 4 Interleave Depth    : 16
  TLV 5 Subcarrier Assignment : Continuous Pilots (list)
    0191 0242 0293 0344 0395 0446 0497 0548 0599 0650
    0701 0752 0803 0854 0905 0956 1007 1058 1109 1160
    1211 1262 2513 2564 2615 2666 2717 2768 2819 2870
    2921 2972 3023 3074 3125 3176 3227 3257 3269 3280
    3289 3326 3335 3346 3358 3398 3449 3500 3551 3602
    3653 3704 3755 3806 3857 3908
  TLV 5 Subcarrier Assignment : Excluded Subcarriers (range)
    : 0000 - 0165
  TLV 5 Subcarrier Assignment : Excluded Subcarriers (range)
    : 1288 - 2487
  TLV 5 Subcarrier Assignment : Excluded Subcarriers (range)
    : 3930 - 4095
  TLV 5 Subcarrier Assignment : PLC Subcarriers (range)
    : 3304 - 3311
  TLV 6 Primary Capable     : 0 (No)
-----

```

Verify Profile Management Data

To view the detailed profile management data associated with each cable modem.

```
Router#show cable modem c0c6.87ff.dabc prof-mgmt
```

```
Downstream Profile Management Data:
MAC Address      : c0c6.87ff.dcea
IP Address       : 60.11.0.12
IPv6 Address     : ---
```

```
RxMer Exempt Percent : 2
RxMer Margin qdB     : 0
Automatic Prof Dwngrd : Active
```

```
DCID                : 162
Configured Profile(s) : 0
Profile(s) in REG-RSP-MP : 0
Profile(s) in DBC-REQ  : N/A
Current profile       : 0 [1024-QAM]
Percentages of ideal BL vs Curr Prof : 96 (better) 3 (equal)
Downgrade profile    : 0
Recommend profile     : 0
Unfit profile(s)     : N/A
Recommend profile (Expired) : N/A
```

```

Unfit profile(s) (Expired)           : N/A
Number of SubCarriers   : 4096
1st Active SubCarrier   : 166
# of Active SubCarriers: 3764
Tx Time                 : 0h:15m:15s ago
Rx Time                 : 0h:15m:15s ago
OFDM Profile Failure Rx: N/A
MER Poll Period (min): 60
Recommend Timeout (min): 120
Unfit Timeout (min): 60
Source                  : OPT
Sub-      RxMER
Carrier
0x0000  00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
0x0020  00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
0x0040  00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
0x0060  00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
0x0080  00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
0x00A0  00000000 0000A5A3 A4A1A2A1 A5A3A39E A5A3A6A4 A6A1A6A2 A3A69FA2 A1A4A4A2
0x00C0  A2A0A4A4 A49EA7A6 A4A29EA4 A2A2A1A4 A3A1A1A4 A4A3A0A6 A4A1A4A6 A4A4A2A5
0x00E0  A5A2A3A5 A8A3A3A3 A6A1A1A0 A2A3A4A4 A3A2A19E A4A89FA3 A4A4A3A4 A4A4A5A2
0x0100  A5A3A1A1 A0A4A59E 9FA2A3A3 9F9FAAA4 A5A09FA4 A4A1A2A6 9DA1A1A0 A4A2A4A3
0x0120  A3A0A3A8 A29FA5A5 A3A6A1A0 A69EA1A2 A1A2A3A2 A1A2A3A5 9FA6A4A5 A1A7A4A4
0x0140  A5A4A5A1 A3A4A2A4 A2A2A4A3 A1A2A5A4 A19FA4A5 A1A0A5A4 9FA4A1A1 A6A2A59F
0x0160  A1A2A4A5 A3A5A4A1 A4A3A5A1 A3A3A5A0 A0A3A3A0 A2A3A3A3 A2A2A2A5 A5A4A4A3
0x0180  9EA4A3A1 A4A5A2A3 A29FA39F A6A1A0A2 A4A59FA3 A4A2A4A1 A2A4A3A3 A6A39DA2
0x01A0  A3A1A1A2 A3A2A2A1 A2A0A39F A7A39FA5 A1A4A4A1 A2A4A2A0 A6A49F9F A6A39D9F
0x01C0  9FA2A5A2 9BA1A1A0 A3A2A1A3 A39FA3A1 A19EA3A5 9DA1A0A0 A3A0A39F A0A3A2A1
0x01E0  A5A4A0A1 A0A39F9E A09FA2A4 9FA2A39F A2A3A49C A3A29FA0 A0A3A2A5 A3A0A1A1
... ..
Upstream Profile Management Data:

```

Verify OCD and DPD Messages in RPD

To view OCD and DPD messages from RPD, run the following command. The output must be identical to the messages on Cisco cBR-8 routers.

```

RPD-config# show downstream ofdm configuration
OCD Message

OCD fields
DCID                               : 0
CCC                                 : 1
TLV 0 Spacing                       : 50 KHz
TLV 1 Cyclic Prefix                 : 1024 samples
TLV 2 Rolloff                       : 128 samples
TLV 3 Spectrum Location             : 800600000 Hz
TLV 4 Interleave Depth              : 16
TLV 5 Subcarrier Assignment         : Continuous Pilots (list)
  191  242  293  344  395  446  497  548  599  650
  701  752  803  854  905  956  1007 1058 1109 1160
 1211 1262 2513 2564 2615 2666 2717 2768 2819 2870
 2921 2972 3023 3074 3125 3176 3227 3257 3269 3280
 3289 3326 3335 3346 3358 3398 3449 3500 3551 3602
 3653 3704 3755 3806 3857 3908
TLV 5 Subcarrier Assignment         : Excluded Subcarriers (range)
                                     : 0 - 165
TLV 5 Subcarrier Assignment         : Excluded Subcarriers (range)
                                     : 1288 - 2487
TLV 5 Subcarrier Assignment         : Excluded Subcarriers (range)
                                     : 3930 - 4095
TLV 5 Subcarrier Assignment         : PLC Subcarriers (range)

```

```

                                : 3304 - 3311
    TLV 6 Primary Capable       : 1 (Yes)

DPD Message
  DPD fields
    DCID                       : 0
    Profile ID                 : 0
    CCC                        : 1
    TLV 5 Subcarrier Range/List : Range (continuous)
      Modulation               : 1024 (default value)
                                : 0 - 4095

DPD Message
  DPD fields
    DCID                       : 0
    Profile ID                 : 255
    CCC                        : 1
    TLV 5 Subcarrier Range/List : Range (continuous)
      Modulation               : 16 (default value)
                                : 0 - 4095

```

Verify per-Profile Counter on RPD

The following example shows how to verify the per-profile counter on RPD:

```
RPD-config# show downstream ofdm counter profile
```

Profile	Pkts	Sum-Pkts	Bytes	Sum-Bytes	Codewords	Sum-Codewords
0	7735	7735	677110	677110	4815	4815
1	0	0	0	0	0	0
2	0	0	0	0	0	0
3	0	0	0	0	0	0
4	0	0	0	0	0	0
5	0	0	0	0	0	0
6	0	0	0	0	0	0
7	0	0	0	0	0	0
8	0	0	0	0	0	0
9	0	0	0	0	0	0
10	0	0	0	0	0	0
11	0	0	0	0	0	0
12	0	0	0	0	0	0
13	0	0	0	0	0	0
14	0	0	0	0	0	0
15	0	0	0	0	0	0

Verify the Drop Counter in DPS

To verify the drop counter, especially in the DPS module, run the following command:

```

RPD-config#show downstream channel counter
----- Packets counter in TPMI -----

Level   Rx-pkts   Rx-sum-pkts
Node Rcv 32690704 32690704
Depi Pkt 32471383 32471383

Port Chan Rx-pkts   Rx-sum-pkts
DS_0 0 3599407 3599407
DS_0 1 3605066 3605066

```

Verify the Drop Counter in DPS

```

DS_0 5      3602293      3602293
DS_0 6      3596193      3596193
DS_0 7      3598393      3598393
DS_0 8        599        599
US_0 5      598656      598656

```

```

Port      Rx-pkts      Rx-sum-pkts Drop-pkts Drop-sum-pkts
DS_0      28998897    28998897    0          0
US_0      3602539     3602539     0          0
US_1      2244        2244        0          0

```

----- Packets counter in DPMI -----

```

Field      Pkts      Sum-pkts
Dpmi Ingress 28844845  28844845
Pkt Delete 0          0
Data Len Err 0          0

```

```

Chan Flow_id Octets      Sum-octs      SeqErr-pkts SeqErr-sum-pkts
0 0      374242      374242      1          1
0 1      710485      710485      1          1
0 2      218477141   218477141   1          1
0 3      0           0           0          0
1 0      379530      379530      1          1
1 1      700973      700973      1          1
1 2      218859695   218859695   1          1
1 3      0           0           0          0
2 0      372126      372126      1          1
2 1      695623      695623      1          1

```

```

31 2      0           0           0          0
31 3      0           0           0          0
158 0      0           0           0          0
158 1      682214      682214      1          1
158 2      0           0           0          0
158 3      0           0           1          1
163 0      0           0           0          0
163 1      0           0           1          1
163 2      0           0           0          0
163 3      1654620     1654620     1          1

```

----- Packets counter in DPS -----

```

Chan Tx-packets Tx-octets Drop-pkts Tx-sum-pkts Tx-sum-octs Drop-sum-pkts
0 3599803 219580072 0 3599803 219580072 0
1 3605466 219958582 0 3605466 219958582 0
2 3602414 219728291 0 3602414 219728291 0
3 3604543 219858566 0 3604543 219858566 0

31 599 20366 0 599 20366 0
158 7797 682524 0 7797 682524 0

```

Configuration Example

The following example shows how to configure OFDM channel:

```
cable downstream ofdm-chan-profile 0
  description System Profile 0
  cyclic-prefix 1024
  interleaver-depth 16
  pilot-scaling 48
  roll-off 128
  subcarrier-spacing 50KHZ
  profile-control modulation-default 256-QAM
  profile-ncp modulation-default 16-QAM
  profile-data 1 modulation-default 1024-QAM

cable downstream controller-profile 100
  max-ofdm-spectrum 192000000
  rf-chan 0 7
  type DOCSIS
  frequency 453000000
  rf-output NORMAL
  qam-profile 1
  docsis-channel-id 1
  rf-chan 158
  docsis-channel-id 159
  ofdm channel-profile 0 start-frequency 645000000 width 192000000 plc 651000000

cable rpd node_0873
  identifier 0004.9f00.0873
  core-interface Te7/1/0
  principal
  rpd-ds 0 downstream-cable 7/0/0 profile 100
  rpd-us 0 upstream-cable 7/0/0 profile 1
```

Feature Information for RPHY DS OFDM Channel Configuration

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



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

Table 30: Feature Information for RPHY DS OFDM Channel Configuration

Feature Name	Releases	Feature Information
Remote PHY DS OFDM Channel Configuration	Cisco 1x2 / Compact Shelf RPD Software 3.1	This feature was integrated into the Cisco Remote PHY Device.



CHAPTER 17

Virtual Combining of Upstream Channels on RPD

This chapter provides information on the support for virtual combining of upstream channels on Cisco Remote PHY Devices.

- [Hardware Compatibility Matrix for Cisco Remote PHY Device, on page 117](#)
- [Information About Virtual Combining of Upstream Channels, on page 118](#)
- [Configure Virtual Combining of Upstream Channels, on page 118](#)
- [Configuration Example, on page 120](#)
- [Feature Information for Virtual Combining of Upstream Channels, on page 121](#)

Hardware Compatibility Matrix for Cisco Remote PHY Device



Note Unless otherwise specified, the hardware components introduced in a given Cisco Remote PHY Device Software Release are supported in all subsequent releases.

Table 31: Hardware Compatibility Matrix for the Cisco Remote PHY Device

Cisco HFC Platform	Remote PHY Device
Cisco GS7000 Super High Output Node	Cisco 1x2 / Compact Shelf RPD Software 2.1 and Later Releases
Cisco GS7000 Super High Output Intelligent Node (iNode)	Cisco 1x2 / Compact Shelf RPD Software 4.1 and Later Releases Cisco Intelligent Remote PHY Device 1x2 <ul style="list-style-type: none">• PID—iRPD-1X2=• PID—iRPD-1X2-PKEY=



Note The -PKEY suffix in the PID indicates units that enable the SCTE-55-2 Out-of-Band protocol support.

Information About Virtual Combining of Upstream Channels

Virtual Combining helps in supporting more RPDs than the number of US SGs, similar to the way multiple physical cables are combined to the same upstream RF port in I-CMTS architecture.

In RPHY, a group of Upstream External PHY Interface (UEPI) sessions with different pseudowires are set up for a single upstream channel for both CCAP core and RPD. However, with virtual-combining, multiple UEPI sessions are mapped to one physical channel in Cisco cBR-8 Routers.

Through this feature, Cisco cBR-8 routers support the binding of multiple US ports on RPDs to the same US controller. The USPHY configuration on the combined RPDs is the same. All combined RPDs must use the same type of USPHY chip.

You are notified if an RPD USPHY is incompatible with the USPHY configuration when a new RPD comes online.

The combined US ports may be in the same RPD. The combined US ports may be in different RPDs. The maximum number of combined US ports to the same controller must not exceed 8. The combined USPHY channels share the bandwidth of the combined channel.

At any instance, only one USPHY channel can transmit. Cisco cBR Series routers support the modems under a specific RPD even in combined US channel cases. It also supports all member USPHY channel information in a combined channel.

When monitoring a physical channel, the cable monitor monitors all member UEPI channels. Spectrum surveillance collects and calculates the SNR and CNR for each USPHY channel.

The OFDMA channels supported for the Virtual Combining feature on Remote PHY start from 8192. The number of ATDMA channels supporting this feature are 256 physical channels for IPHY and 1024 for Remote PHY.

Configure Virtual Combining of Upstream Channels

Configure RPD for Virtual Combining

The virtual combining of upstream channels is initiated automatically when users configure the same US controller for more than one US ports. The ports may be in the same RPD or different RPDs, but should be on the same line card).

In the following example, the US port 0 on RPD node_1 and US port 0 and 1 on RPD node_2 are combined to upstream-cable 9/0/2.

```
cable rpd node <number>
  identifier badb.ad13.5d7e
  core-interface Te9/1/2
  principal
  rpd-ds 0 downstream-cable 9/0/2 profile 100
  rpd-us 0 upstream-cable 9/0/2 profile 221
  r-dti 1
!
cable rpd node_2
  identifier badb.ad13.5d96
  core-interface Te9/1/2
  principal
```

```

rpd-ds 0 downstream-cable 9/0/2 profile 100
rpd-us 0 upstream-cable 9/0/2 profile 221
rpd-us 1 upstream-cable 9/0/2 profile 221
r-dti 1
!
```

Verify Upstream Virtual Combining Details

To view the spectrum analysis measurements of the specified UEPI channels for virtual combining, use the following sample commands:

```

show cable spectrum-analysis Cable <slot/subslot/port> upstream <port> sid <Sid of modem
or noise> devID <0-7 Device ID>
Load for five secs: 5%/1%; one minute: 5%; five minutes: 5%
No time source, *11:16:00.436 CST Sat Feb 24 2018
```

```

Spectrum Analysis Measurements for Cable9/0/7: Upstream 0 Sid 1
Device ID: 1
Channel Center Frequency: 10000 kHz
Frequency Span:          3200 kHz
Number of Bins:         129
Bin Spacing:            25.0 kHz
Resolution Bandwidth:   42.750 kHz
Amplitude Data:
  Bin  1: -60.00 dBmV
  Bin  2: -60.00 dBmV
  Bin  3: -60.00 dBmV
  Bin  4: -32.00 dBmV
  Bin  5: -23.00 dBmV
  Bin  6: -22.00 dBmV
```

To view the signal quality of the specified channels supporting virtual combining, use the following sample commands:

```

show cable signal-quality cmts
I/F          DevID      CNiR          Expected Received
              (dB)          Signal Power (dBmV)
Cable1/0/0/U0  0          31.0          0.0
Cable1/0/0/U0  1          31.0          0.0
Cable1/0/0/U0  2          31.0          0.0
Cable1/0/0/U1  0          31.0          0.0
Cable1/0/0/U1  1          31.0          0.0
Cable1/0/0/U2  -----
Cable1/0/0/U3  -----
Cable1/0/0/U4  0          31.0          0.0
Cable1/0/0/U5  0          31.0          0.0
```

To view the status of upstream channel combining, use the following sample commands:

```

show controllers upstream-cable 7/0/62 us-channel 0

Load for five secs: 5%/1%; one minute: 6%; five minutes: 5%
Time source is NTP, 18:05:11.271 CST Tue Feb 27 2018

Controller RPD US Port List:

DevID  RPD ID          US Port  I/F      Name
-----
0      0004.9f03.0226  0        Te7/1/1  0004.9f03.0226
1      0004.9f03.0286  0        Te7/1/1  0004.9f03.0286
```

```

2    1004.9f30.1500    0    Te7/1/0    1004.9f30.1500
3    1004.9f30.1500    1    Te7/1/0    1004.9f30.1500

USPHY OFDMA support: NO

Controller 7/0/62 upstream 0  AdminState:UP OpState: UP
  atdma mode enabled
  Frequency 21.800 MHz, Channel Width 1.600 MHz, Symbol Rate 1.280 Msps
  Modulation Profile Group 221
  Modulations (64-QAM) - A-short 64-QAM, A-long 64-QAM, A-ugs 64-QAM

Mapped to connector 62 and receiver 0
Bind to Cable7/0/0 US0
US phy MER(SNR)_estimate for good packets - 42.410 dB
Spectrum Group is overridden
Nominal Input Power Level 0 dBmV
part_id=0x0000, rev_id=0x00, rev2_id=0x00
Range Load Reg Size=0x58
Request Load Reg Size=0x0E
Minislot Size in number of Timebase Ticks is = 4
Minislot Size in Symbols = 32
Minislot Size in Bytes = 24

UCD procedures on lch 0
UCD ucd-succeed          (3 ) invalid-req          (0 ) md-dispatch          (0 )
UCD mismatch-req        (0 ) start-sw             (0 ) start-state          (0 )
UCD ccc-time            (0 ) end-sw               (0 ) end-state            (0 )
UCD ucd-lch-tgc         (0 ) ucd-rcvr            (0 ) ucd-cdm-timeout     (0 )
UCD ucd-no-regtxn       (0 ) ucd-req-chn-mismatch(0 ) ucd-send-next-fail  (0 )
UCD ucd-rpd-np          (0 ) ucd-upd-gcp-msg     (0 ) ucd-cfg-gcp-msg     (0 )
UCD ucd-gcp-ack         (0 ) ucd-gcp-ack-timeout(0 ) ucd-gcp-nack        (0 )
UCD ucd-gcp-timout      (0 ) ucd-ack-err         (0 ) ucd-timer-null      (0 )
UCD ucd-proxy-timeout   (0 ) ucd-proxy-wrong-ack (0 )

PHY: us errors 0 us recoveries 0 (enp 0)
MAC PHY TSS: tss error start 0 tss error end 0
MAC PHY Status: mask 0 int_index 0
PHY: TSS late 0 discontinuous 0
PHY: TSS mis-match 0 not-aligned 0
PHY: TSS missed snapshots from phy 0
Map Counts:0
LCH_state RUN_STEADY , UCD_count 3, MD 0 chan 0

```

Configuration Example

This section provides example of how to configure the RPD for virtual combining of upstream channels.

Example for Configuring RPD for Virtual Combining

```

cable rpd node_1
  identifier badb.ad13.5d7e
  core-interface Te9/1/2
  principal
  rpd-ds 0 downstream-cable 9/0/2 profile 100
  rpd-us 0 upstream-cable 9/0/2 profile 221
  r-dti 1
!
cable rpd node_2
  identifier badb.ad13.5d96

```

```

core-interface Te9/1/2
principal
rpd-ds 0 downstream-cable 9/0/2 profile 100
rpd-us 0 upstream-cable 9/0/2 profile 221
rpd-us 1 upstream-cable 9/0/2 profile 221
r-dti 1
!
```

Feature Information for Virtual Combining of Upstream Channels

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



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

Table 32: Feature Information for Virtual Combining of Upstream Channels

Feature Name	Releases	Feature Information
Virtual Combining of Upstream Channels on Remote PHY	Cisco 1x2 RPD Software 4.1	This feature was introduced on the Cisco Remote PHY Devices.



CHAPTER 18

Redundant Multicast DEPI Pool

This document describes how to configure redundant multicast DEPI pool.

Finding Feature Information

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

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

- [Redundant Multicast DEPI Pool, on page 123](#)
- [Configure Redundant Multicast DEPI Pool, on page 124](#)
- [Feature Information for Redundant Multicast DEPI Pool, on page 125](#)

Redundant Multicast DEPI Pool

In DS sharing, the DS controller of the secondary line card uses the same multicast IP address as the primary line card DS controller. For a single RPD, the principal and standby Cores use different source IP addresses, but same group IP address in a multicast group. However, the NCS switch does not support one Group with multiple Sources in a multicast group. Hence, you must assign additional multicast IP addresses for standby cores.

Assign the additional multicast IP addresses to the DS controllers on the secondary line cards if the secondary line card is up.

When you enable the redundant multicast DEPI pool, the secondary line card is up in the redundancy line card group and the multicast IP addresses are assigned to secondary line card from the redundant multicast pool. All RPDs on standby cores are automatically cleared to be offline and later online again.

When you disable the redundant multicast pool, the IP addresses are removed from the redundant multicast pool, and all the RPD standby cores are cleared automatically. If you do not configure redundant pool, the secondary line card downstream controllers use the same IP as the downstream controllers in the primary line card.

You cannot use the redundant multicast pool in the downstream controller profile configuration.

Multicast IP address for the secondary line card is assigned based on the DS controller and the TenGE port. One DS controller can be assigned 8 IPv4/IPv6 addresses from Tx/1/0 to Tex/1/7, where x is the secondary line card slot number. Hence, the redundant multicast DEPI pool needs a minimum of 266 IP addresses (32 controller for 8 ports for DOCSIS, 10 for OOB). If 266 IP addresses are not available, you can assign 4 IPv4/IPv6 addresses to the ports 0,2,4,6 on a single DS controller for multicast DEPI IP addresses on the secondary line card.

Configure Redundant Multicast DEPI Pool

This section describes how to configure the redundant multicast DEPI pool on Cisco cBR-8 routers.



Note To know more about the commands referenced in this section, see the [Cisco IOS Command List](#).

Configuring Redundant Multicast DEPI Pool

When a secondary line card is configured, multicast IP addresses are assigned to its downstream controllers from the redundant multicast DEPI pool.

Step 1 Configure the multicast DEPI pool by using the following command:

```
configure terminal
cable depi multicast pool id{ip|ipv6} address ip mask
```

Step 2 Verify the multicast DEPI pool configuration.

```
show cable depi multicast pool
```

Example:

```
show cable depi multicast pool
Load for five secs: 7%/1%; one minute: 7%; five minutes: 7%
No time source, *15:57:05.512 CST Wed Aug 22 2018
POOL ID   Net IP           Net Mask         Redundant DESCRIPTION
1         227.0.0.0       255.255.255.0   FALSE
127      227.226.225.0   255.255.255.0   FALSE      to TE9/1/1+TE9/1/7
```

```
POOL ID   IPv6             Redundant DESCRIPTION
10        FF3A::9000:0/120 FALSE
```

Step 3 Configure the redundant multicast DEPI pool.

```
configure terminal
cable depi multicast pool id
redundant
```

Step 4 Verify the redundant multicast DEPI pool configuration.

```
show cable depi multicast pool
```

Example:

```
show cable depi multicast pool
Load for five secs: 7%/1%; one minute: 7%; five minutes: 7%
```



```

No time source, *16:27:05.552 CST Wed Aug 22 2018
POOL ID   Net IP           Net Mask           Redundant DESCRIPTION
1         227.0.0.0        255.255.255.0     FALSE
127      227.226.225.0    255.255.255.0     FALSE      to TE9/1/1+TE9/1/7

POOL ID   IPv6              Redundant DESCRIPTION
10       FF3A::9000:0/120  TRUE

```

Verify Assigned Multicast IP Addresses

Verify the multicast addresses that are assigned to the secondary linecard downstream controllers by running the `show cable depi multicast ip/ipv6 all` command, similar to the following example:

```

show cable depi multicast ipv6 all
Load for five secs: 6%/0%; one minute: 6%; five minutes: 7%
No time source, *14:23:14.522 CST Tue Aug 28 2018
IPv6          POOL ID   CONTROLLER
FF3E::8140:0  20        0/0/0 (1-Te0/1/0)
FF3E::8140:8  20        0/0/1 (2-Te0/1/0)
FF3E::8140:10 20        0/0/2 (3-Te0/1/0)
FF3E::8140:18 20        0/0/3 (4-Te0/1/0)
FF3E::8140:20 20        0/0/4 (5-Te0/1/0)
FF3E::8140:28 20        0/0/5 (6-Te0/1/0)
FF3E::8140:30 20        0/0/6 (7-Te0/1/0)
.....

```

Feature Information for Redundant Multicast DEPI Pool

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



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

Table 33: Feature Information for Redundant Multicast DEPI Pool

Feature Name	Releases	Feature Information
Redundant Multicast DEPI Pool	Cisco 1x2 / Compact Shelf RPD Software 4.1.2	This feature was introduced on the Cisco cBR Series Converged Broadband Routers.



CHAPTER 19

DOCSIS3.1 Downstream Resiliency for RPHY

This document describes how to configure the DOCSIS3.1 Downstream Resiliency on the Cisco Remote PHY Device.

Finding Feature Information

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

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

- [Hardware Compatibility Matrix for Cisco Remote PHY Device, on page 127](#)
- [Information about DOCSIS3.1 Downstream Resiliency for RPHY, on page 128](#)
- [Configure DOCSIS3.1 Downstream Resiliency for RPHY, on page 129](#)
- [Feature Information for DOCSIS3.1 Downstream Resiliency for RPHY, on page 130](#)

Hardware Compatibility Matrix for Cisco Remote PHY Device



Note Unless otherwise specified, the hardware components introduced in a given Cisco Remote PHY Device Software Release are supported in all subsequent releases.

Table 34: Hardware Compatibility Matrix for the Cisco Remote PHY Device

Cisco HFC Platform	Remote PHY Device
Cisco GS7000 Super High Output Node	Cisco 1x2 / Compact Shelf RPD Software 2.1 and Later Releases

Cisco HFC Platform	Remote PHY Device
Cisco GS7000 Super High Output Intelligent Node (iNode)	Cisco 1x2 / Compact Shelf RPD Software 4.1 and Later Releases Cisco Intelligent Remote PHY Device 1x2 <ul style="list-style-type: none"> • PID—iRPD-1X2= • PID—iRPD-1X2-PKEY=



Note The -PKEY suffix in the PID indicates units that enable the SCTE-55-2 Out-of-Band protocol support.

Information about DOCSIS3.1 Downstream Resiliency for RPHY

When DOCSIS3.1 cable modem reports non-primary RF channel failure for SCQAM or OFDM channel, actions performed by downstream resiliency is the same as DOCSIS3.0 cable modem. In other words, if RF channel impairment is below the resiliency threshold, CM's service flows are moved to Resiliency Bonding Group (RBG) or Narrow Band (NB) interface. If RF channel impairment is above the resiliency threshold, the impaired RF channel is temporarily removed from the bonding group.

The following table summarizes the CM-STATUS events for OFDM channel, and the action taken by the downstream resiliency module:

Table 35: CM-STATUS events for OFDM channel

Event Type Code	Event Description	DS Resiliency Action
1	MDD timeout	Move CM's service flows to RBG/NB or suspend RF from BG.
2	FEC lock failure	Move CM's service flows to RBG/NB or suspend RF from BG.
4	MDD recovery	Move CM's service flows back to original BG.
5	FEC lock recovery	Move CM's service flows back to original BG.
16	DS OFDM profile failure. A loss of FEC lock on one of the assigned downstream OFDM profiles of a channel.	DS OFDM Profile Manager will handle this event and take action.
20	NCP profile failure. Loss of FEC lock on NCP.	Move CM's service flows to RBG/NB or suspend RF from BG.
21	Loss of FEC lock on the PLC.	Move CM's service flows to RBG/NB or suspend RF from BG.

Event Type Code	Event Description	DS Resiliency Action
22	NCP profile recovery.	Move CM's service flows back to original BG.
23	FEC recovery on PLC channel.	Move CM's service flows back to original BG.
24	FEC recovery on OFDM profile.	Recovery of impairment reported by event 16. DS OFDM Profile Manager will handle this event and take action.

Configure DOCSIS3.1 Downstream Resiliency for RPHY

Configure DOCSIS3.1 Downstream Resiliency for RPHY

User must configure the command **cable rf-change-trigger percent value count number** to enable the downstream resiliency functionality.

To configure the trigger thresholds specific to OFDM RF impairment, follow the steps below:

enable

configure terminal

cable ofdm-rf-change-trigger percent value counter number [no-ncp-plc]

Trigger thresholds *value* and *number* apply globally to the non-primary OFDM RF channels. If this command is not configured, the trigger thresholds configured by the command **cable rf-change-trigger percent value count number** will be used for the non-primary OFDM channels.

With **no-ncp-plc** configured in the command, this feature will not take any action when CM reports CM-STATUS-EVENT 20 or 21.



Note The **cable rf-change-trigger percent value count number** command is optional and the configured trigger thresholds apply to non-primary OFDM channels only.

Display OFDM Specific CM-STATUS Events

To display the statistics of the OFDM specific CM-STATUS events, use the **show cable modem wideband rcs-status** command as shown in the example below:

```
router#show cable modem 4800.33ea.7072 wideband rcs-status verbose
CM : 4800.33ea.7072
RF : 3/0/0 0
  Status                : UP
  FEC/QAM Failure       : 0
  Dup FEC/QAM Failure   : 0
  FEC/QAM Recovery      : 0
  Dup FEC/QAM Recovery  : 0
  MDD Failure           : 0
```

```

Dup MDD Failure           : 0
MDD Recovery             : 0
Dup MDD Recovery         : 0
Flaps                    : 0
Flap Duration            : 00:00
RF : 3/0/0 159
Status                   : UP
FEC/QAM Failure          : 0
Dup FEC/QAM Failure      : 0
FEC/QAM Recovery        : 0
Dup FEC/QAM Recovery     : 0
MDD Failure              : 0
Dup MDD Failure          : 0
MDD Recovery             : 0
Dup MDD Recovery         : 0
NCP PROF Failure        : 2      May 8 15:14:24
Dup NCP PROF Failure     : 0
NCP PROF Recovery       : 1      May 8 15:15:18
Dup NCP PROF Recovery    : 0
PLC Lock Recovery       : 1      May 8 15:15:46
Dup PLC Lock Recovery    : 0
Flaps                    : 0
Flap Duration            : 00:00
OFDM Profile Id : 2
Status                   : UP
Profile Failure          : 1      May 8 15:16:18
DUP Profile Failure      : 0
Profile Recovery         : 1      May 8 15:16:44
DUP Profile Recovery     : 0

```

Feature Information for DOCSIS3.1 Downstream Resiliency for RPHY

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



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

Table 36: Feature Information for DOCSIS3.1 Downstream Resiliency for RPHY

Feature Name	Releases	Feature Information
DOCSIS3.1 Downstream Resiliency for RPHY	Cisco 1x2 / Compact Shelf RPD Software 4.1	This feature was introduced on the Cisco Remote PHY Device.



CHAPTER 20

Dynamic Bonding Group for RPHY

The Dynamic Bonding Group (DBG) feature enables the system to automatically create bonding groups of different sizes based on the cable modems' capacity. It helps to manage the resources of all downstream bonding groups. When the number of available bonding groups reaches the lower limit, it reclaims the bonding groups that match the reclaim threshold set by the user. The modems used on these bonding groups are then moved to other bonding groups without primary channel change. This move makes space for new bonding group allocations. This automated way of creating and reclaiming bonding groups greatly reduces the management effort of RCC configuration. DBG also automatically accommodates primary channel and CM capacity distributions.

The load balancing feature leverages DBG to balance traffic among all channels. With DBG, the modem is assigned to the downstream bonding group without any static RCC configuration.

DBG supports the following:

- DOCSIS 3.0 and DOCSIS 3.1 channel types.
- DOCSIS 3.0 and DOCSIS 3.1 load balance.
- Interoperation with modem registration, load balancing, and high availability.
- Enhanced dynamic load balance to allow movement of modem without a change in the primary channel.
- Enhanced FPGA to allow channel utilization fairness.

This chapter describes how to configure the DBG feature on the Cisco Remote PHY Device.

Finding Feature Information

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

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

- [Hardware Compatibility Matrix for Cisco Remote PHY Device, on page 132](#)
- [Configure Dynamic Bonding Group, on page 132](#)
- [Configure Load Balancing with Dynamic Bonding Group Enabled, on page 135](#)
- [Feature Information for Dynamic Bonding Group, on page 140](#)

Hardware Compatibility Matrix for Cisco Remote PHY Device



Note Unless otherwise specified, the hardware components introduced in a given Cisco Remote PHY Device Software Release are supported in all subsequent releases.

Table 37: Hardware Compatibility Matrix for the Cisco Remote PHY Device

Cisco HFC Platform	Remote PHY Device
Cisco GS7000 Super High Output Node	Cisco 1x2 / Compact Shelf RPD Software 2.1 and Later Releases
Cisco GS7000 Super High Output Intelligent Node (iNode)	Cisco 1x2 / Compact Shelf RPD Software 4.1 and Later Releases Cisco Intelligent Remote PHY Device 1x2 <ul style="list-style-type: none"> • PID—iRPD-1X2= • PID—iRPD-1X2-PKEY=



Note The -PKEY suffix in the PID indicates units that enable the SCTE-55-2 Out-of-Band protocol support.

Configure Dynamic Bonding Group

Before configuring DBG, it is assumed that interface Mac domain and fiber node are already configured on the Cisco cbr-8 router. The recommended primary channel distribution is one primary channel for contiguous four channels, such as 0, 4, 8, 12, 16, 20, 24, 28 and so on. For more information, see DOCSIS Interface and Fiber Node Configuration in the Cisco cBR Converged Broadband Routers DOCSIS Software Configuration Guide.

Enable Dynamic Bonding Group

DBG is disabled by default. Use **cable dynamic-bonding-group** command to enable DBG as shown in the following example:

```
ROUTER# configure terminal
ROUTER(config)# cable dynamic-bonding-group
ROUTER(config)# end
```

To configure the bonding group reclaim threshold, use **cable dynamic-bonding-group reclaim-threshold** command as shown in the following example:

```
ROUTER# configure terminal
```



```
ROUTER(config)# cable dynamic-bonding-group reclaim-threshold percent 5% modems 6
ROUTER(config)# end
```

5% is the default bonding group throughput percentage threshold, and 6 is the default cable modem count threshold. If the throughput of a bonding group is lower than 5% of all bonding groups' throughput, and this bonding group has less than 6 cable modems assigned to it, then this bonding group is reclaimed when the available bonding groups reach the lower limit (20%).

By default, cable modem registration and load balance trigger DBG creation when needed. If you want to disable the interoperation with cable modem registration and load balance, use the commands in the following example:

```
ROUTER# configure terminal
ROUTER(config)# no cable dynamic-bonding-group registration

ROUTER# configure terminal
ROUTER(config)# no cable dynamic-bonding-group load-balance
```

When DBG is enabled, we recommend you to complete the following configurations.

Enable DS-Resiliency and Configure Resiliency Bonding Group

To make sure that the modem is still in w-online state with maximum downstream capability when several RF channels are impaired, enable the ds-resiliency feature by running the following commands:

```
Router# configure terminal
Router(config)# cable resiliency ds-bonding
Router(config)# end

Router# configure terminal
Router(config)# interface wideband-Cable 3/0/1:30
Router(config-if)# cable ds-resiliency
Wideband-Cable3/0/1:30 is set to WB resiliency bonding group.
Remove any existing bundle and rf-channel configuration.
Router(config-if)# end
```

Enable ACFE

Enable ACFE feature to make sure that modem registration is not blocked because of QoS failures:

```
Router# configure terminal
Router(config)# cable acfe enable
Router(config)# end
```

Verify Dynamic Bonding Group Configuration

This section describes how to use certain **show** commands to verify if the dynamic bonding groups are created.

Check the modem's primary wideband interface using the **show cable modem wideband channel** command as shown in this example:

```
Router# show cable modem 4800.33ee.ebee wideband channel
```

MAC Address	IP Address	I/F	MAC State	DSxUS	Primary WB
4800.33ee.ebee	30.132.15.246	C3/0/1/UB	w-online	32x2	Wi3/0/1:3

Check the modem's downstream tuner capability using the **show cable modem verbose | in DS Tuner** command as shown in the following example:

```
Router# show cable modem 4800.33ee.ebee verbose | in DS Tuner
DS Tuner Capability : 32
```

Check the related RCC using the **show cable mac-domain rcc** command as shown in the following example:

```
Router# show cable mac-domain c3/0/1 rcc
RCC-ID  RCP          RCs  MD-DS-SG  CMs  WB/RCC-TMPL  D3.0  D3.1
32      00 00 00 00 00 8    0          11  WB (Wi3/0/1:1)  Y      Y
33      00 00 00 00 00 32   0          6   WB (Wi3/0/1:3)  Y      Y
34      00 00 00 00 00 8    0          7   WB (Wi3/0/1:2)  Y      Y
35      00 00 00 00 00 8    0          7   WB (Wi3/0/1:4)  Y      Y
36      00 00 00 00 00 8    0          7   WB (Wi3/0/1:5)  Y      Y
```

Check the dynamically created bonding groups using the **show cable dynamic-bonding-group summary** command as shown in the following example:

```
Router# show cable dynamic-bonding-group summary
Dynamic bonding group: Enable
BG ID BG Name  BG Size CMs ServFlows Create Time          Create Client      BG State
RFid list
24834 Wi3/0/1:1 8          11  11          Sep 14 14:36:35.194 MODEM_ONLINE      OPERATIONAL
24832-24839
24836 Wi3/0/1:3 32         6    6          Sep 14 14:43:24.144 MODEM_ONLINE      OPERATIONAL
24832-24863
24835 Wi3/0/1:2 8          7    7          Sep 14 17:20:37.115 MODEM_ONLINE      OPERATIONAL
24840-24847
24837 Wi3/0/1:4 8          7    7          Sep 14 17:21:37.723 STATIC_LOAD_BALANCE OPERATIONAL
24856-24863
24838 Wi3/0/1:5 8          7    7          Sep 14 17:21:39.761 STATIC_LOAD_BALANCE OPERATIONAL
24848-24855
```

This example shows the DBG with D31 modems:

```
Router# show cable mac-domain c1/0/4 rcc
RCC-ID  RCP          RCs  MD-DS-SG  CMs  WB/RCC-TMPL  D3.0  D3.1
7       00 00 00 00 00 33   0          51  WB (Wi1/0/4:2)  N      Y
8       00 00 00 00 00 8    0          2   WB (Wi1/0/4:3)  Y      Y
9       00 00 00 00 00 8    0          1   WB (Wi1/0/4:4)  Y      Y
```

```
Router# show cable dynamic-bonding-group summary
Dynamic bonding group: Enable
BG ID BG Name  BG Size CMs ServFlows Create Time          Create Client      BG
State      RFid list
9219 Wi1/0/4:2 33         51  51          Sep 26 13:56:00.337 MODEM_ONLINE
OPERATIONAL 9216-9247, 9375
9220 Wi1/0/4:3 8          2    2          Sep 26 13:56:19.011 MODEM_ONLINE
OPERATIONAL 9216-9223
9221 Wi1/0/4:4 8          1    1          Sep 26 13:56:36.090 MODEM_ONLINE
OPERATIONAL 9240-9247
```

Table 38: Dynamic Bonding Group States

DBG State	Description
CREATE_WAITING_SUP	Line card sends a request to create DBG and waits for SUP to create the bonding group.

DBG State	Description
HOLD	DBG is created from SUP, or bonding group reverts from reclaim to ready-for-use state.
OPERATIONAL	If a modem is used on the bonding group after the HOLD state times out, the DBG state changes to OPERATIONAL.
RECLAIM_HOLD	Ready for reclaim. If no modem is used on the bonding group or match the reclaim in two minutes, the bonding group is reclaimed. The DBG state changes to RECLAIM_HOLD.
RECLAIM_MODEM_MOVING	Ready for reclaim. The modem is moved out of the bonding group.
RECLAIM_WAITING_SUP	Line card sends a DBG reclaim request and waits for SUP to reclaim the BG.

To display the detailed channel list information of dynamic bonding group, use the **show derived-config interface wideband** command as shown in the following example:

```
Router# show derived-config interface wideband-Cable 3/0/1:1
Building configuration...
Derived configuration: 113 bytes
!
interface Wideband-Cable3/0/1:1
  cable bundle 255
  cable rf-channels channel-list 0-7 bandwidth-percent 1
end
```

Check the usage of bonding group resource using the **show cable dynamic-bonding-group quota** command.

```
Router# show cable dynamic-bonding-group quota controller 3/0/1
slot/subslot/ctrlr: 3/0/1
Total BG number: 128
Used BG number (static/dynamic): 6(1/5) Available BG number: 122
Available BG list port: 0, 6-29, 31-127
```

Check the reclaimed bonding group using the **show cable dynamic-bonding-group reclaim-history summary** command:

```
Router# show cable dynamic-bonding-group reclaim-history summary
BG ID BG Name   BG Size Create Time      Create Client Reclaim Time   Reclaim Client RFid
list
24835 Wi3/0/1:2 16      Sep 14 14:40:27 MODEM_ONLINE  Sep 14 14:44:27 DBG_INTERNAL
24832-2484
```

Configure Load Balancing with Dynamic Bonding Group Enabled

If you want to use load balancing with the DBG enabled, we recommend that you configure the load balancing as shown here.

Enable Load Balancing for DOCSIS 3.0 and DOCSIS 3.1

To enable DOCSIS load balancing, run the following commands:

```
Router# config terminal
Router(config)# cable load-balance docsis-enable
Router(config)# end
```

When DOCSIS load balancing is enabled, run the following commands to enable load balancing for DOCSIS 3.0 and DOCSIS 3.1.

```
Router# config terminal
Router(config)# cable load-balance docsis30-enable
Router(config)# end
```

Enable DOCSIS 3.0 and DOCSIS 3.1 Static Load Balance

To balance the load of primary channels, enable static load balance using the following commands:

```
Router# configure terminal
Router(config)# cable load-balance docsis30-enable static
Router(config)# end
```

Enable DOCSIS 3.0 and DOCSIS 3.1 General Load Balance Group

To enable general load balance group, use cable load-balance docsis-group command as shown here:

```
Router# configure terminal
Router(config)# cable load-balance docsis-group fn 1 md c3/0/1
Router(config-lb-group)# no disable
Router(config-lb-group)# end
```

Enable Dynamic Load Balance and Fixed-Primary Channel Movement

To balance the load of all downstream channels based on utilization, enable dynamic load balance by running the following commands:

```
Router# configure terminal
Router(config)# cable load-balance docsis30-enable dynamic downstream
Router(config)# end
```

Fixed primary channel movement is disabled by default. With dynamic load balancing enabled, we recommend that you enable fixed primary channel movement to reduce service outage by running the following commands:

```
Router# configure terminal
Router(config)# cable load-balance fixed-primary-channel
Router(config)# end
```

Verify Static Load Balancing Configuration

This section describes how to use **show** commands to verify the configuration of the static load balancing.

Check the load of all primary channels using the **show cable load-balance docsis-group load** command as shown here:

```
Router# show cable load-balance docsis-group fn 1 md c3/0/1 load | in In
Interface          State      Group      Utilization Rsvd NBCM WB/UB Weight
In3/0/1:0 (573 MHz) initial  2147557888 0%(0%/0%)  0%  0   17   37
In3/0/1:4 (597 MHz) initial  2147557888 0%(0%/0%)  0%  0   17   37
In3/0/1:8 (621 MHz) initial  2147557888 0%(0%/0%)  0%  0   13   37
In3/0/1:12 (645 MHz) initial  2147557888 0%(0%/0%)  0%  0   13   37
In3/0/1:16 (669 MHz) initial  2147557888 0%(0%/0%)  0%  0   13   37
In3/0/1:20 (693 MHz) initial  2147557888 0%(0%/0%)  0%  0   13   37
In3/0/1:24 (717 MHz) initial  2147557888 0%(0%/0%)  0%  0   13   37
In3/0/1:28 (741 MHz) initial  2147557888 0%(0%/0%)  0%  0   13   37
```

This command output lists all primary channels and shows the number of cable modems used with these channels. NBCM is the number of narrowband modems used with a channel while WBCM (WB/UB) is the number of wideband modems used with a channel. The total number of WBCMs must be balanced among all channels.

The difference between the total number of WBCMs used with any two channels is smaller or equal to the minimum threshold load. The default value of the minimum threshold load is 5.

This example shows the load in DOCSIS 3.1 static load balancing configuration:

```
Router# show cable load-balance docsis-group fn 33 md c3/0/0 load | i In
Interface          State      Group      Utilization Rsvd NBCM WB/UB Weight
In3/0/0:0 (453 MHz) initial  2147557408 1%(0%/1%)  0%  0   16   37
In3/0/0:8 (501 MHz) initial  2147557408 1%(0%/1%)  0%  0   16   37
In3/0/0:30 (633 MHz) initial  2147557408 1%(0%/1%)  0%  0   12   37
In3/0/0:40 (693 MHz) initial  2147557408 1%(0%/1%)  0%  0   15   37
In3/0/0:55 (783 MHz) initial  2147557408 1%(0%/1%)  0%  0   12   37
In3/0/0:158 (258 MHz) initial  2147557408 1%(0%/1%)  0%  0   21  224
```

- Above example, the modem count balanced with a configured threshold of 5

- Count based load balancing is done only on sc-qam channels of equal weight. OFDM channel is of much higher weight and is excluded from the modem count calculations.

Check the load of all RF channels using the **show cable load-balance docsis-group rfch-util** command as shown in this example:

```
Router# show cable load-balance docsis-group fn 1 md c3/0/1 rfch-util
Interface Pstate Pending-In Pending-Out Throughput(Kbps) Util NBCM WBCM
In3/0/1:0 up      No           No           0                0%  0   17
In3/0/1:1 NA      No           No           0                0%  0   17
In3/0/1:2 NA      No           No           0                0%  0   17
In3/0/1:3 NA      No           No           0                0%  0   17
In3/0/1:4 up      No           No           0                0%  0   17
In3/0/1:5 NA      No           No           0                0%  0   17
In3/0/1:6 NA      No           No           0                0%  0   17
In3/0/1:7 NA      No           No           0                0%  0   17
In3/0/1:8 up      No           No           0                0%  0   13
In3/0/1:9 NA      No           No           0                0%  0   13
In3/0/1:10 NA     No           No           0                0%  0   13
In3/0/1:11 NA     No           No           0                0%  0   13
In3/0/1:12 up      No           No           0                0%  0   13
In3/0/1:13 NA     No           No           0                0%  0   13
In3/0/1:14 NA     No           No           0                0%  0   13
In3/0/1:15 NA     No           No           0                0%  0   13
.....
Average: 0.0
Variance: 0.0
```

This command lists the load information of the primary and secondary channels. WBCM is the number of wideband modems used with a channel.

Check the cable modem's internal state in load balancing using the **show cable load-balance docsis-group modem-list wideband** command as shown in this example:

```
Router# show cable load-balance docsis-group fn 1 md c3/0/1 modem-list wideband
Codes: M - Multicast, U - UGS, P - PCMM, F - Max-Failures, X - eXcluded
      L - L2vpn, R - RSVP, S - DS-Resiliency
Primary WB   MAC Address   Primary DS  RCC-ID Priority MUPFXLRS State
Wi3/0/1:0    (3)
             c8fb.2631.0e56 In3/0/1:20 41      0      ----- LB_CM_HOLD_EXPIRE_IN 36
             c8fb.26a6.c3dc In3/0/1:16 41      0      ----- LB_CM_HOLD_EXPIRE_IN 37
             c8fb.2631.0d7e In3/0/1:16 41      0      ----- LB_CM_HOLD_EXPIRE_IN 43
Wi3/0/1:1    (9)
             c8fb.2631.0c80 In3/0/1:0  32      0      ----- LB_CM_STATIC_MOVING
             c8fb.2631.0cae In3/0/1:0  32      0      ----- LB_CM_STATIC_READY
             c8fb.2631.0db0 In3/0/1:24 42      0      ----- LB_CM_STATIC_MOVING
             c8fb.2631.0c10 In3/0/1:28 42      0      ----- LB_CM_STATIC_MOVING
             c8fb.2631.0d80 In3/0/1:16 41      0      ----- LB_CM_STATIC_MOVING
             c8fb.2631.0d26 In3/0/1:24 41      0      ----- LB_CM_STATIC_MOVING
             a4a2.4a2d.b4aa In3/0/1:20 41      0      ----- LB_CM_STATIC_MOVING
             c8fb.2631.0e5c In3/0/1:0  32      0      ----- LB_CM_STATIC_MOVING
             c8fb.2631.0cb0 In3/0/1:0  32      0      ----- LB_CM_STATIC_MOVING
Wi3/0/1:2    (3)
             c8fb.2631.0d2a In3/0/1:12 34      0      ----- LB_CM_HOLD_EXPIRE_IN 27
             c8fb.2631.0e5a In3/0/1:12 34      0      ----- LB_CM_STATIC_MOVING
             c8fb.2631.0bfe In3/0/1:8  34      0      ----- LB_CM_STATIC_MOVING
Wi3/0/1:3    (2)
             4800.33ea.54be In3/0/1:28 33      0      ----- LB_CM_DYANMIC_READY
             4800.33ee.ebe6 In3/0/1:20 33      0      ----- LB_CM_HOLD_EXPIRE_IN 1
Wi3/0/1:4    (2)
             c8fb.2631.0e44 In3/0/1:24 42      0      ----- LB_CM_HOLD_EXPIRE_IN 40
             c8fb.2631.0a44 In3/0/1:28 42      0      ----- LB_CM_HOLD_EXPIRE_IN 42
```

Table 39: Cable Modem States

CM State	Description
LB_CM_STATIC_READY	Modem is ready for static load balance movement.
LB_CM_STATIC_MOVING	Modem is in movement triggered by static load balance.
LB_CM_HOLD_EXPIRE_IN	Modem is in hold for the next movement. The default hold time, in seconds, is 600.
LB_CM_DYANMIC_READY	Modem is ready for dynamic load balance movement.
LB_CM_DYANMIC_MOVING	Modem is in movement triggered by dynamic load balance.
LB_CM_DISABLED	Modem is not ready for movement. If the modem failure movement count reaches maximum failure threshold, then set the modem in LB_CM_DISABLED to avoid further movement.

Verify Dynamic Load Balancing Configuration

This section describes how to use the **show** commands to verify the configuration of the dynamic load balancing.

Check the utilization of all RF channels using **show cable load-balance docsis-group rfch-util** command as shown in this example:

```
Router# show cable load-balance docsis-group fn 320 md c3/0/0 rfch-util
Interface  Pstate Pending-In Pending-Out Throughput(Kbps) Util NBCM WBCM
Do3/0/0:0  up      No           No           11754          31% 0    308
Do3/0/0:1  up      No           No           11754          31% 0    296
Do3/0/0:2  up      No           No           11754          31% 0    333
Do3/0/0:3  up      No           No           11754          31% 0    296
Do3/0/0:4  up      No           No           11754          31% 0    297
Do3/0/0:5  up      No           No           11754          31% 0    331
Do3/0/0:6  up      No           No           11754          31% 0    299
Do3/0/0:7  up      No           No           11753          31% 0    268
Do3/0/0:8  up      No           No           11754          31% 0    302
Do3/0/0:9  up      No           No           11754          31% 0    331
Do3/0/0:10 up      No           No           11753          31% 0    308
Do3/0/0:11 up      No           No           11754          31% 0    305
Do3/0/0:12 NA      No           No           12862          34% 0    258
Do3/0/0:13 NA      No           No           12862          34% 0    258
Do3/0/0:14 NA      No           No           12862          34% 0    258
.....
Average: 30.416
Variance: 1.701
```

The traffic among all RF channels is considered balanced when the difference between any two RF channel utilization is under the threshold load. The default percentage of threshold load is 10%.

To check the potential target bonding group for each of the source bonding group, use the **show cable load-balance docsis-group target dbg** and the **show cable load-balance docsis-group target wide** commands as shown in this example:

```
Router# show cable load-balance docsis-group fn 320 md c3/0/0 target dbg
Interface  Bg-Id      Size      Group          Target
Wi3/0/0:0  24577      4         2147557695
Wi3/0/0:3  24580      4         2147557695
Wi3/0/0:4  24581      8         2147557695
Wi3/0/0:5  24582      8         2147557695
Wi3/0/0:6  24583      24        2147557695    33% [24576, 24584-24587, 24589-24607]
Wi3/0/0:7  24584      16        2147557695    30% [24576, 24586-24587, 24595-24607]
Wi3/0/0:8  24585      16        2147557695
Wi3/0/0:9  24586      32        2147557695
Wi3/0/0:10 24587      24        2147557695    33% [24576, 24584-24587, 24589-24607]
Wi3/0/0:11 24588      8         2147557695
Wi3/0/0:12 24589      8         2147557695    27% [24596-24603]
Wi3/0/0:13 24590      8         2147557695
Wi3/0/0:14 24591      4         2147557695

Router# show cable load-balance docsis-group fn 5 md c1/0/4 target wide
Interface  Bg-Id      State      Group          Target
Wi1/0/4:2  9219      up         2147510276    Wi1/0/4:4
Wi1/0/4:3  9220      up         2147510276
Wi1/0/4:4  9221      up         2147510276
```

If there is no target bonding group in the output, it means that no bonding groups are created to balance traffic among RF channels.

A sample output for DOCSIS 3.1 modems with a configured threshold of 14% is shown. For utilization based load balancing to start on DOCSIS 3.1 modems, the OFDM channel must be utilized 100% and SC-QAM must have traffic. The utilization-based load balancing balances the traffic on the SC-QAM channels in a DOCSIS 3.1 modem.

```
Router# show cable load-balance docsis-group fn 5 md c1/0/4 rfch-util
Interface      Pstate Pending-In Pending-Out Throughput (Kbps) Util NBCM WBCM
In1/0/4:0      up      No          No          10632          28%  0    45
In1/0/4:1      NA      No          No          11226          29%  0    41
In1/0/4:2      NA      No          No          11225          29%  0    41
In1/0/4:3      NA      No          No          11225          29%  0    41
In1/0/4:4      down    No          No          11225          29%  0    41
In1/0/4:5      down    No          No          11225          29%  0    41
In1/0/4:6      down    No          No          11225          29%  0    41
In1/0/4:7      down    No          No          11225          29%  0    41
In1/0/4:8      up      No          No          10620          28%  0    43
.....
.....
In1/0/4:35     NA      No          No          6646           17%  0    6
In1/0/4:36     NA      No          No          6646           17%  0    6
In1/0/4:37     NA      No          No          6647           17%  0    6
In1/0/4:38     NA      No          No          6646           17%  0    6
In1/0/4:39     NA      No          No          6647           17%  0    6
In1/0/4:40     up      No          No          6088           16%  0    6
In1/0/4:41     NA      No          No          6648           17%  0    6
In1/0/4:42     NA      No          No          6647           17%  0    6
In1/0/4:43     NA      No          No          6647           17%  0    6
In1/0/4:44     NA      No          No          6646           17%  0    6
In1/0/4:45     NA      No          No          6646           17%  0    6
In1/0/4:46     No      No          No          6647           17%  0    6
In1/0/4:47     NA      No          No          6648           17%  0    6
In1/0/4:48     NA      No          No          6648           17%  0    6
In1/0/4:49     NA      No          No          6648           17%  0    6
In1/0/4:50     NA      No          No          6646           17%  0    6
In1/0/4:51     NA      No          No          6648           17%  0    6
In1/0/4:52     NA      No          No          6647           17%  0    6
In1/0/4:53     NA      No          No          6648           17%  0    6
In1/0/4:54     No      No          No          6647           17%  0    6
In1/0/4:55     NA      No          No          6648           17%  0    6
In1/0/4:56     NA      No          No          6647           17%  0    6
In1/0/4:57     NA      No          No          6647           17%  0    6
In1/0/4:58     NA      No          No          6646           17%  0    6
In1/0/4:59     NA      No          No          6645           17%  0    6
In1/0/4:60     NA      No          No          6646           17%  0    6
In1/0/4:61     NA      No          No          6646           17%  0    6
In1/0/4:62     NA      No          No          6647           17%  0    6
In1/0/4:63     NA      No          No          6647           17%  0    6
In1/0/4:159   NA      No          No          1819685        100% 0    47
```

Feature Information for Dynamic Bonding Group

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



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

Table 40: Feature Information for Dynamic Bonding Group

Feature Name	Releases	Feature Information
Dynamic Bonding Group	Cisco 1x2 / Compact Shelf RPD Software 4.1	This feature was introduced on the Cisco Remote PHY Device.



CHAPTER 21

Cisco Remote PHY Device IPv6

Finding Feature Information

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

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

- [Hardware Compatibility Matrix for Cisco Remote PHY Device, on page 143](#)
- [Information about RPD IPv6, on page 144](#)
- [Configure RPD IPv6 Unicast Online, on page 144](#)
- [Configure IPv6 DS Splitting, on page 147](#)
- [Feature Information for Remote-PHY Device IPv6, on page 151](#)

Hardware Compatibility Matrix for Cisco Remote PHY Device



Note Unless otherwise specified, the hardware components introduced in a given Cisco Remote PHY Device Software Release are supported in all subsequent releases.

Table 41: Hardware Compatibility Matrix for the Cisco Remote PHY Device

Cisco HFC Platform	Remote PHY Device
Cisco GS7000 Super High Output Node	Cisco 1x2 / Compact Shelf RPD Software 2.1 and Later Releases

Cisco HFC Platform	Remote PHY Device
Cisco GS7000 Super High Output Intelligent Node (iNode)	Cisco 1x2 / Compact Shelf RPD Software 4.1 and Later Releases Cisco Intelligent Remote PHY Device 1x2 <ul style="list-style-type: none"> • PID—iRPD-1X2= • PID—iRPD-1X2-PKEY=



Note The -PKEY suffix in the PID indicates units that enable the SCTE-55-2 Out-of-Band protocol support.

Information about RPD IPv6

The CableLabs' MHA v2 standards requires CCAP Core and RPD must support both IPv4 and IPv6, which means the Remote PHY Signaling between the CCAP Core and RPD is able to run on both IPv4 and IPv6 networks.



- Note**
- CCAP Core can support IPv4/IPv6 dual stack.
 - RPD can support either IPv4 or IPv6 network.
 - RPD does not support IPv4/IPv6 Dual Stack at the same time.
 - RPD will try IPv6 connection first. When DHCPv6 failed, RPD will try DHCPv4.
 - For single RPD, all the server addresses, protocols to communicate with it must be in the same IP version.

Configure RPD IPv6 Unicast Online

This section describes how to configure RPD IPv6 Unicast Online on Cisco cBR-8.

Configure Unicast IPv6

To configure Unicast IPv6, complete the following procedure:

1. Enable IPv6 unicast routing.

```
configure terminal
ipv6 unicast-routing
```

2. Configure IPv6 Address on DPIC interface.

```
configure terminal
interface TenGigabitEthernet slot/1/port
```

```

ipv6 enable
ipv6 address ipv6_address

```

Configure RPD core interface

To configure RPD core interface, complete the following procedure:

```

configure terminal
cable rpd name
identifier rpdc_mac
core-interface tenG_interface
principal
rpdc-ds id downstream-cable controller profile id
rpdc-us id upstream-cable controller profile id

```

Configure IPv6 PTP Clock Option

To configure the IPv6 PTP Clock Option, complete the following procedure:

1. Configure CBR as secondary PTP, see the configuration example below:

```

configure terminal
  interface Loopback1588
    ip address 158.158.158.5 255.255.255.255
  ptp clock ordinary domain 0
  servo tracking-type R-DTI
  clock-port slave-from-903 slave
  delay-req interval -4
  sync interval -5
  sync one-step
  transport ipv4 unicast interface Lo15888 negotiation
  clock source 10.90.3.93

```



Note CCAP-Core as secondary PTP can only support IPv4.

2. Configure R-DTI for RPD PTP IPv6.

```

configure terminal
ptp r-dti number
ptp-domain domain
clock-port number
ethernet number
transport ipv6
clock source ipv6 address gateway ipv6 gateway

```



- Note**
- PTP domain and 1588 primary have same domain number.
 - Clock source IPv6 address is 1588 primary IPv6 address.
 - Gateway is next hop to 1588 primary, and it is optional.
 - For RPD, ethernet 1=vbh0, ethernet 2=vbh1, ethernet 0 will choose either vbh0 or vbh1 which is functional as clock-port.

3. Associate R-DTI with RPD configuration.

```
configure terminal
cable rpd id
r-dti number
```

Verify IPv6 PTP Clock Option Configuration

To display the CBR PTP Status, use the **show ptp clock running** command as shown in the example below:

```
Router# show ptp clock running
Load for five secs: 6%/2%; one minute: 7%; five minutes: 8%
No time source, *05:11:13.610 UTC Sun Oct 22 2017
PTP Ordinary Clock [Domain 0]
      State          Ports          Pkts sent      Pkts rcvd      Redundancy Mode
      PHASE_ALIGNED 1              2478203        7512533        Hot standby

                                PORT SUMMARY

Name          Tx Mode      Role          Transport      State          Sessions      PTP Master
              Port Addr
slave-from-903 unicast     slave         Lo15888       Slave          1             10.90.3.93
```

To display the RPD PTP Status, use the **show ptp clock** command as shown in the example below:

```
Router# show ptp clock 0 config
Domain/Mode      : 0/OC_SLAVE
Priority 1/2/local : 128/255/128
Profile          : 001b19000100-000000 E2E
Total Ports/Streams : 1 /1
--PTP Port 23, Enet Port 1 ----
Port local Address :2001:120:102:70:7:1b71:476c:70ba
Unicast Duration :300 Sync Interval : -4
Announce Interval : 0 Timeout : 11
Delay-Req Intreval : -4 Pdelay-req : -4
Priority local :128 COS: 6 DSCP: 47
==Stream 0 : Port 23 Master IP: 2001:10:90:3::93
```

```
Router# show ptp clock 0 state
apr state       : PHASE_LOCK
clock state     : SUB_SYNC
current tod     : 1508640223 Sun Oct 22 02:43:43 2017
active stream   : 0
==stream 0 :
port id        : 0
master ip      : 2001:10:90:3::93
stream state   : PHASE_LOCK
Master offset  : 3490
Path delay    : -27209
```

```

Forward delay :          -27333
Reverse delay :          -27085
Freq offset   :          6544364
1Hz offset   :              49

```

Router# show ptp clock 0 statistics

```

AprState 4 :
    2@0-00:06:25.027          1@0-00:06:15.382          0@0-00:03:51.377
    4@0-00:03:32.176
ClockState 5 :
    5@0-00:06:36.141          4@0-00:06:33.684          3@0-00:06:30.510
    2@0-00:06:25.512          1@0-00:06:24.982
BstPktStrm 1 :
    0@0-00:06:15.987
StepTime 1 :
    908222863@0-00:05:42.199
AdjustTime 2589 :
    -339@1-20:18:42.949      -321@1-20:17:41.949      49@1-20:16:40.949
    145@1-20:15:39.949      6@1-20:14:38.949      261@1-20:13:37.949
    327@1-20:12:36.949      76@1-20:11:35.949      157@1-20:10:34.949
streamId  msgType          rx          rxProcessed      lost          tx
0          SYNC             2549177      2549177          4292476931   0
0          DELAY REQUEST      0            0                0            2549150
0          P-DELAY REQUEST    0            0                0            0
0          P-DELAY RESPONSE    0            0                0            0
0          FOLLOW UP         0            0                0            0
0          DELAY RESPONSE    2549144      2549144          4292476934   0
0          P-DELAY FOLLOWUP    0            0                0            0
0          ANNOUNCE          159330       159330           4294836225   0
0          SIGNALING         1662         1662             0            1663
0          MANAGEMENT        0            0                0            0
TOTAL          5259313      5259313          12879790090   2550813

```

Verify RPD IPv6 Configuration

To display the RPD IPv6 Status, use the **show cable rpd ipv6** command as shown in the example below:

```

Router# show cable rpd ipv6
Load for five secs: 7%/2%; one minute: 9%; five minutes: 8%
No time source, *14:03:13.622 UTC Sun Oct 22 2017
MAC Address  I/F          State          Role HA  Auth IP Address
0004.9f03.0226 Te0/1/6  online        Pri  Act N/A  2001:120:102:70:7:1B71:476C:70BA
0004.9f03.0232 Te0/1/7  online        Pri  Act N/A  ---
0004.9f03.0256 Te0/1/2  online        Pri  Act N/A  2001:120:102:70:3:830A:FAEA:CF7E
0004.9f03.0268 Te0/1/6  online        Pri  Act N/A  2001:120:102:70:7:41F1:7CCD:4475
0004.9f03.0268 Te6/1/6  online        Aux  Act N/A  2001:120:102:70:7:41F1:7CCD:4475
badb.ad13.5d7e Te0/1/2  online        Pri  Act N/A  2001:120:102:70:3:FF46:1FF9:29FE

```

Configure IPv6 DS Splitting

This section describes how to configure RPD IPv6 DS splitting on Cisco cBR-8. In this configuration, different RPDs share the same DS SG traffic. For each DS sharing controller, one unique IPv6 multicast IP is assigned according to multicast pool. When RPD is IPv6 online, all DS sharing Controller associated multicast IPs are IPv6 type. Multiple DS controllers used by one RPD core must be either IPv4 or IPv6 and cannot be mixed. RPD sharing same DS Controller must only be IPv4 or IPv6 online and cannot be mixed. Multiple RPD cores in one RPD must only be IPv4 or IPv6 online and cannot be mixed.

Configure the multicast IPv6 DEPI pool

To configure multicast IPv6 DEPI pool, complete the following procedure:

```
configure terminal
cable depi multicast pool id
ipv6 address ip/prefix
```

Enable Multicast Sharing under Downstream Controller Profile

To configure Unicast IPV6, complete the following procedure (same as IPv4 downstream splitting):

```
configure terminal
cable downstream controller-profile id
multicast-pool id
```

Configure the RPD with the Same Downstream Controller and Profile

To configure the RPDs with the same downstream controller and profile, complete the procedure as shown in the example below (same as IPv4 downstream splitting):

```
configure terminal
cable rpd node_1
  core-interface tenGigabitEthernet 9/1/0
    rpd-ds 0 controller downstream-cable 9/0/0 profile 0
    rpd-us 0 controller upstream-cable 9/0/0 profile 221
cable rpd node_2
  core-interface tenGigabitEthernet 9/1/0
    rpd-ds 0 controller downstream-cable 9/0/0 profile 0
    rpd-us 0 controller upstream-cable 9/0/0 profile 221
```

Configure the RPDs to different fiber-nodes

To configure the RPDs to different fiber-nodes, complete the procedure as shown in the example below (same as IPv4 downstream splitting):

```
configure terminal
cable fiber-node 100
  downstream Downstream-Cable 9/0/0
  upstream Upstream-Cable 9/0/0
cable fiber-node 101
  downstream Downstream-Cable 9/0/0
  upstream Upstream-Cable 9/0/1
```

Configure the RPDs to MAC Domain

To configure the RPDs to the MAC domain, complete the procedure as shown in the example below (same as IPv4 downstream splitting):

```
configure terminal
interface Cable9/0/0
  downstream Downstream-Cable 9/0/0 rf-channel 0
  downstream Downstream-Cable 9/0/0 rf-channel 8
  upstream 0 Upstream-Cable 9/0/0 us-channel 0
  upstream 1 Upstream-Cable 9/0/0 us-channel 1
  upstream 2 Upstream-Cable 9/0/0 us-channel 2
```



```

upstream 3 Upstream-Cable 9/0/0 us-channel 3
upstream 4 Upstream-Cable 9/0/1 us-channel 0
upstream 5 Upstream-Cable 9/0/1 us-channel 1
upstream 6 Upstream-Cable 9/0/1 us-channel 2
upstream 7 Upstream-Cable 9/0/1 us-channel 3
cable upstream bonding-group 1
  upstream 0
  upstream 1
  upstream 2
  upstream 3
  attributes 800000F0
cable upstream bonding-group 2
  upstream 4
  upstream 5
  upstream 6
  upstream 7
  attributes 8000000F

```

Or use the following example (same as IPv4 downstream splitting):

```

configure terminal
  interface Cable9/0/0
    downstream Downstream-Cable 9/0/0 rf-channel 0
    upstream 0 Upstream-Cable 9/0/0 us-channel 0
    upstream 1 Upstream-Cable 9/0/0 us-channel 1
    upstream 2 Upstream-Cable 9/0/0 us-channel 2
    upstream 3 Upstream-Cable 9/0/0 us-channel 3
    cable upstream bonding-group 1
      upstream 0
      upstream 1
      upstream 2
      upstream 3
      attributes 800000F0
configure terminal
  interface Cable9/0/1
    downstream Downstream-Cable 9/0/0 rf-channel 8
    upstream 0 Upstream-Cable 9/0/1 us-channel 0
    upstream 1 Upstream-Cable 9/0/1 us-channel 1
    upstream 2 Upstream-Cable 9/0/1 us-channel 2
    upstream 3 Upstream-Cable 9/0/1 us-channel 3
    cable upstream bonding-group 1
      upstream 0
      upstream 1
      upstream 2
      upstream 3
      attributes 800000F0

```

Enable IPv6 multicast on Cisco cBR-8 Router

To enable the IPv6 multicast on cBR-8, complete the following procedure:

```

configure terminal
ipv6 multicast-routing

```

If cBR-8 and RPD are connected in L2 network, we recommend to enable MLD Snooping in L2 switches.

Verify the IPv6 DS Splitting Configuration

To display the IPv6 multicast DEPI pool, use the **show cable depi multicast pool ipv6** command as shown in the example below:

```

Router# show cable depi multicast pool ipv6
Load for five secs: 8%/2%; one minute: 7%; five minutes: 8%
No time source, *06:57:11.898 UTC Sun Oct 22 2017
POOL ID   IPv6                               DESCRIPTION
22        FF3B::8000:0/100
50        FF3A::8000:0/126                    zyq
100       FF39::8000:0/120                    zyq
Infra_C05#show cable depi multicast pool ipv6 id 22
Load for five secs: 8%/2%; one minute: 8%; five minutes: 8%
No time source, *07:00:03.577 UTC Sun Oct 22 2017
POOL ID   IPv6                               DESCRIPTION
22        FF3B::8000:0/100

```

To display the assigned IPv6 multicast address, use the **show cable depi multicast ipv6** command as shown in the example below:

```

Router# show cable depi multicast ipv6 all
Load for five secs: 10%/3%; one minute: 8%; five minutes: 8%
No time source, *07:01:33.659 UTC Sun Oct 22 2017
IPv6      POOL ID   CONTROLLER
FF3A::8000:0    50        9/0/2 (291)
FF3A::8000:1    50        9/0/28 (317)
FF39::8000:0    100       9/0/29 (318)
FF3A::8000:2    50        9/0/30 (319)
Infra_C05#show cable depi multicast ipv6 FF3A::8000:0
Load for five secs: 7%/2%; one minute: 8%; five minutes: 8%
No time source, *07:01:44.020 UTC Sun Oct 22 2017
IPv6      POOL ID   CONTROLLER
FF3A::8000:0    50        9/0/2 (291)

```

To display the relationship between the downstream controller profile and IPv6 multicast Pool, use the **show cable downstream controller-profile** command as shown in the example below:

```

Router# show cable downstream controller-profile 100
Load for five secs: 24%/3%; one minute: 10%; five minutes: 8%
No time source, *07:10:28.074 UTC Sun Oct 22 2017

Downstream controller-profile 100, type RPHY
Description:
Downstream controller-profile 100 is being used by controller Downstream-Cable:
  0/0/30,
  Admin: UP
  MaxOfdmSpectrum: 192000000
  MaxCarrier: 158
  Mode: normal
  Free freq block list has 3 blocks:
    45000000 - 449999999
    594000000 - 602999999
    795000000 - 1217999999
DS Splitting: Yes
Multicast Pool ID: 50
  OFDM frequency exclusion bands: None

Configured RF Channels:
Chan Admin Frequency Type Annex Mod srate Qam-profile dcid output
0 UP 453000000 DOCSIS B 256 5361 1 1 NORMAL
1 UP 459000000 DOCSIS B 256 5361 1 2 NORMAL
2 UP 465000000 DOCSIS B 256 5361 1 3 NORMAL

```

To display the RPD associated with the downstream controller, use the **show controllers downstream-Cable** command as shown in the example below:

```

Router# show controllers downstream-Cable 9/0/2 rpd
Load for five secs: 8%/2%; one minute: 9%; five minutes: 8%

```

```
No time source, *07:14:20.326 UTC Sun Oct 22 2017
Controller RPD DS Port List:(2 of 2)
  RPD ID          I/F          Name
-----
```

```
badb.ad13.5d7e  Te9/1/2  node_3
0004.9f03.0256  Te9/1/2  node_5
```

When the DS Controller IPv4/IPv6 type and the RPD IPv4/IPv6 online type conflicts, the RPD log prompts the conflict as shown in the example below:

```
Router# show cable rpd 0004.9f00.0979 Te3/1/0 log reverse
RPD ID I/F Severity Time LOG INFORMATION
```

```
-----
0004.9f00.0979 Te3/1/0 ERROR
2017-09-23 21:44:52.851 RPD 0004.9f00.0979 CoreTe 3/1/0 reset connection due to unmatched
IPv4/IPv6 between GCP connection(IPv6) and Downstream Sharing Controllers 3/1/0(IPv4)
0004.9f00.0979 Te3/1/0 ERROR
2017-09-23 21:44:50.817 RPD 0004.9f00.0979 CoreTe 3/1/0 reset connection due to unmatched
IPv4/IPv6 between GCP connection(IPv6) and Downstream Sharing Controllers 3/1/0(IPv4)
```

Feature Information for Remote-PHY Device IPv6

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



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

Table 42: Feature Information for Remote-PHY Device IPv6

Feature Name	Releases	Feature Information
Remote-PHY Device IPv6	Cisco 1x2 / Compact Shelf RPD Software 3.1	This feature was introduced on the Cisco Remote PHY Device.



CHAPTER 22

DOCSIS 3.1 OFDMA Channel Configuration

This document describes the Remote PHY device DOCSIS 3.1 OFDMA channel configuration on the Cisco cBR Series Converged Broadband Router.

Finding Feature Information

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

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

- [Hardware Compatibility Matrix for Cisco Remote PHY Device, on page 153](#)
- [Information about OFDMA Channel Configuration, on page 154](#)
- [Configure OFDMA Channel, on page 155](#)
- [Support for Line Card High Availability, on page 164](#)
- [Support for Line Card Process Restart, on page 164](#)
- [Feature Information for DOCSIS 3.1 OFDMA Channel Configuration, on page 165](#)

Hardware Compatibility Matrix for Cisco Remote PHY Device



Note Unless otherwise specified, the hardware components introduced in a given Cisco Remote PHY Device Software Release are supported in all subsequent releases.

Table 43: Hardware Compatibility Matrix for the Cisco Remote PHY Device

Cisco HFC Platform	Remote PHY Device
Cisco GS7000 Super High Output Node	Cisco 1x2 / Compact Shelf RPD Software 2.1 and Later Releases

Cisco HFC Platform	Remote PHY Device
Cisco GS7000 Super High Output Intelligent Node (iNode)	Cisco 1x2 / Compact Shelf RPD Software 4.1 and Later Releases Cisco Intelligent Remote PHY Device 1x2 <ul style="list-style-type: none"> • PID—iRPD-1X2= • PID—iRPD-1X2-PKEY=



Note The -PKEY suffix in the PID indicates units that enable the SCTE-55-2 Out-of-Band protocol support.

Information about OFDMA Channel Configuration

DOCSIS 3.1 introduces modes for higher throughput and higher spectral efficiency while still allowing backward compatibility to DOCSIS 3.0. Orthogonal Frequency Division Multiple Access (OFDMA) channel has following features:

- Frequency-range up to 96 MHz
- Upstream spectrum 5 – 204 MHz
- 25 KHz and 50 KHz subcarrier spacing

Modulation Profile

A globally configured OFDMA modulation profile defines modulation orders and pilot patterns for different interval usage codes (IUC). It is also used to assign parameters for initial ranging and fine ranging.

OFDMA Channel Exclusion Band

Ranges of frequencies can be excluded from all OFDMA channels on a port using the **ofdma-frequency-exclusion-band** command.

Exclusion and unused bands apply to OFDMA channels only. OFDMA channel never use frequencies in the exclusion band. So the legacy SC-QAM channel can be placed in this band. OFDMA channel does not use frequencies in the unused band set by **ofdma-frequency-unused-band** command for data traffic, but can send probes in them.

Configure OFDMA Channel

Configure OFDMA Modulation Profile

The OFDMA modulation profile is used to configure initial ranging, fine ranging and data IUC parameters. To define the ofdma modulation profile to be applied to OFDMA channels, follow the steps below:

```
enable
configure terminal
cable mod-profile-ofdma id
subcarrier-spacing value
initial-rng-subcarrier value
fine-rng-subcarrier value
data-iuc id modulation value pilot-pattern value
```

Here is a configuration example:

```
Router# enable
Router# configure terminal
Router(config)# cable mod-profile-ofdma 451
Router(config-ofdma-mod-profile)# subcarrier-spacing 50KHz
Router(config-ofdma-mod-profile)# initial-rng-subcarrier 64
Router(config-ofdma-mod-profile)# fine-rng-subcarrier 128
Router(config-ofdma-mod-profile)# data-iuc 13 modulation 1024-QAM pilot-pattern 2
Router(config-ofdma-mod-profile)# exit
Router(config)# cable mod-profile-ofdma 472
Router(config-ofdma-mod-profile)# subcarrier-spacing 25KHz
Router(config-ofdma-mod-profile)# initial-rng-subcarrier 64
Router(config-ofdma-mod-profile)# fine-rng-subcarrier 128
Router(config-ofdma-mod-profile)# data-iuc 6 modulation 1024-QAM pilot-pattern 8
Router(config-ofdma-mod-profile)# data-iuc 9 modulation 1024-QAM pilot-pattern 8
Router(config-ofdma-mod-profile)# data-iuc 10 modulation 512-QAM pilot-pattern 8
Router(config-ofdma-mod-profile)# data-iuc 11 modulation 256-QAM pilot-pattern 8
Router(config-ofdma-mod-profile)# data-iuc 12 modulation 128-QAM pilot-pattern 9
Router(config-ofdma-mod-profile)# data-iuc 13 modulation 64-QAM pilot-pattern 9
```



Note

- Subcarrier spacing must match the subcarrier spacing of each channel profile in which it is configured.
- Modulation profiles 421 and 461 are the default modulation profiles for 25 KHz and 50 KHz subcarrier spacing respectively. You can add additional modulation profiles. The modulation profile range is between 401-500.
- You must configure subcarrier spacing, ranging, and data IUC 13 before applying modulation profile to a upstream channel.
- Regular pilot patterns (1-4/8-11) and boosted pilot patterns (5-7/12-14) cannot co-exist on the same upstream channel.
- We recommend to not change subcarrier spacing, ranging, and data IUC configuration of a modulation profile that is applied to a channel.

Verify OFDMA Modulation Profile Configuration

To display the OFDMA modulation profile details, use the **show cable modulation-profile ofdma** command as shown in the following example:

```
Router# show cable modulation-profile ofdma
Mod Subc IUC type Act Preamble Bit Pilot
      Spacing      subc Symbols Loading Pattern
421 25KHz 3 (IR) 64 4
      4 (FR) 192 1
      13 (data) 16-QAM 8
423 25KHz 3 (IR) 64 4
      4 (FR) 128 1
      6 (data) 1024-QAM 8
      10 (data) 512-QAM 8
      11 (data) 256-QAM 8
      12 (data) 128-QAM 9
      13 (data) 64-QAM 9
461 50KHz 3 (IR) 32 4
      4 (FR) 192 1
      13 (data) 16-QAM 1
466 50KHz 3 (IR) 64 4
      4 (FR) 128 1
      13 (data) 1024-QAM 2
```

Configure OFDMA Channel

To configure the OFDMA channel, follow these steps:

```
enable
configure terminal
cable upstream controller-profile id
us-channel id docsis-mode ofdma
us-channel id subcarrier-spacing value
us-channel id modulation-profile id
us-channel id frequency-range start-value end-value
us-channel id initial-rng-frequency-start value
us-channel id cyclic-prefix value roll-off-period value
us-channel id symbols-per-frame value
us-channel id data-iuc id band start-value end-value modulation value pilot-pattern
value
```

To use QAM modulation in between specific bandwidth, use the **us-channel id data-iuc id band start-value end-value modulation value pilot-pattern value** command.

Here is a configuration example:

```
Router# enable
Router# configure terminal
Router(config)# cable upstream controller-profile 1
Router(config-controller-profile)# us-channel 12 docsis-mode ofdma
Router(config-controller-profile)# us-channel 12 subcarrier-spacing 25KHz
Router(config-controller-profile)# us-channel 12 frequency-range 40000000 85000000
Router(config-controller-profile)# us-channel 12 modulation-profile 423
Router(config-controller-profile)# us-channel 12 cyclic-prefix 640 roll-off-period 224
```



```
Router(config-controller-profile)# us-channel 12 symbols-per-frame 9
Router(config-controller-profile)# us-channel 12 data-iuc 9 band 50000000 60000000 modulation
512-QAM pilot-pattern 8
Router(config-controller-profile)# no us-channel 12 shutdown
```

**Note**

- A maximum of one OFDMA channel can be configured per controller. For this OFDMA channel, the us-channel index must be set to 12. This corresponds with OFDMA channel 0 on an RPD port.
- Change docsis-mode to **OFDMA** to enable OFDMA configuration options. These options are enabled by default on us-channel 12.
- We recommend that you configure no more than 4 active SC-QAMs while an OFDMA channel is present.
- OFDMA channel can be placed between 5 Mhz and 204 Mhz.
- Values of the options are often interdependent, changing one value may change other values or make them invalid.
- We recommend that you set subcarrier spacing and frequency range first. To achieve a higher OFDMA channel traffic throughput, configure OFDMA channel with 25kHz subcarrier spacing.
- Maximum of 4:1 upstream combining for OFDMA channels is supported.

Bind Upstream Controllers With RPHY Ports

If the upstream channel profile contains OFDMA channel, you can bind up to four RPD ports with the upstream controller.

```
cable rpd node1
  identifier badb.ad15.1288
  core-interface Te7/1/4
  principal
  rpd-ds 0 downstream-cable 7/0/30 profile 10
  rpd-us 0 upstream-cable 7/0/63 profile 1
  rpd-us 1 upstream-cable 7/0/63 profile 1

cable rpd node2
  identifier badb.ad15.1290
  core-interface Te7/1/4
  principal
  rpd-ds 0 downstream-cable 7/0/31 profile 10
  rpd-us 0 upstream-cable 7/0/63 profile 1
  rpd-us 1 upstream-cable 7/0/63 profile 1
```

Verify OFDMA Channel Configuration

To display the OFDMA channel configuration, use the **show controllers upstream-Cable us-channel** command as shown in the example below:

```
Router# show controllers upstream-Cable 1/0/4 us-channel 12
Controller RPD US Port List:
DevID RPD ID US Port I/F Name
-----
0 badb.ad13.acfe 0 Te1/1/2 necker-5
```

Verify OFDMA Channel Configuration

USPHY OFDMA support: FULL

Controller 1/0/4 upstream 12 AdminState:UP OpState: UP
ofdma mode enabled

Channel Freq Range 35.500 MHz to 79.500 MHz

Channel Subcarrier Index Range Cfg: 74, 953 Op: 74, 953

Channel SC0 Freq Cfg: 31.800 MHz Op: 31.800 MHz

#Excl bands: 2

(0, 73), (954, 2047),

#Unused bands: 0

Cyclic Prefix Size 96, Rolloff Period Size 64

Subcarrier Spacing 50KHz, Symbols Per Frame 18 Subcarrier Per Minislot: 8

Modulation Profile (ID 466, Subcarrier Spacing 50KHz)

IUC type	Cfg	Act	Preamble	Bit	Pilot
	subc	subc	Symbols	Loading	Pattern
3 (IR)	64	64	4	-	-
4 (FR)	128	128	1	-	-
13 (data)	-	-	-	1024-QAM	2

Calculated Data burst profile:

IUC	Group	Bit	Pilot	Start	Consec
		Loading	Pattern	Mslot	Mslot
13	0	1024-QAM	2	0	109

#Total mslots:110 #Fine Rng capable:95 #Initial Rng capable:103

Initial Rng - Freq 50.000MHz mslotOffset:36 #mslot in frame:8

Minislot mapping: mslot#(start_sc start_freq(Mhz) end_sc end_freq(Mhz))

mslot type(E-Edge; B-Body; S-Share with SCQAM;

I-Initial rng capable; F-Fine rng capable)

(next Fine Rng capable minislot if current is not capable))

```

0 ( 74, 35.500, 81, 35.850, EIF ( - ) ), 1 ( 82, 35.900, 89, 36.250, BIF ( - ) ),
2 ( 90, 36.300, 97, 36.650, BIF ( - ) ), 3 ( 98, 36.700, 105, 37.050, BIF ( - ) ),
4 ( 106, 37.100, 113, 37.450, BIF ( - ) ), 5 ( 114, 37.500, 121, 37.850, BIF ( - ) ),
6 ( 122, 37.900, 129, 38.250, BIF ( - ) ), 7 ( 130, 38.300, 137, 38.650, BIF ( - ) ),
8 ( 138, 38.700, 145, 39.050, BIF ( - ) ), 9 ( 146, 39.100, 153, 39.450, BIF ( - ) ),
10 ( 154, 39.500, 161, 39.850, BIF ( - ) ), 11 ( 162, 39.900, 169, 40.250, BIF ( - ) ),
12 ( 170, 40.300, 177, 40.650, BIF ( - ) ), 13 ( 178, 40.700, 185, 41.050, BIF ( - ) ),
14 ( 186, 41.100, 193, 41.450, BIF ( - ) ), 15 ( 194, 41.500, 201, 41.850, BIF ( - ) ),
16 ( 202, 41.900, 209, 42.250, BIF ( - ) ), 17 ( 210, 42.300, 217, 42.650, BIF ( - ) ),
18 ( 218, 42.700, 225, 43.050, BIF ( - ) ), 19 ( 226, 43.100, 233, 43.450, BIF ( - ) ),
20 ( 234, 43.500, 241, 43.850, BIF ( - ) ), 21 ( 242, 43.900, 249, 44.250, BIF ( - ) ),
22 ( 250, 44.300, 257, 44.650, BIF ( - ) ), 23 ( 258, 44.700, 265, 45.050, BIF ( - ) ),
24 ( 266, 45.100, 273, 45.450, BIF ( - ) ), 25 ( 274, 45.500, 281, 45.850, BIF ( - ) ),

26 ( 282, 45.900, 289, 46.250, BIF ( - ) ), 27 ( 290, 46.300, 297, 46.650, BIF ( - ) ),
28 ( 298, 46.700, 305, 47.050, BIF ( - ) ), 29 ( 306, 47.100, 313, 47.450, BIF ( - ) ),
30 ( 314, 47.500, 321, 47.850, BIF ( - ) ), 31 ( 322, 47.900, 329, 48.250, BIF ( - ) ),
32 ( 330, 48.300, 337, 48.650, BIF ( - ) ), 33 ( 338, 48.700, 345, 49.050, BIF ( - ) ),
34 ( 346, 49.100, 353, 49.450, BIF ( - ) ), 35 ( 354, 49.500, 361, 49.850, BIF ( - ) ),
36 ( 362, 49.900, 369, 50.250, BIF ( - ) ), 37 ( 370, 50.300, 377, 50.650, BIF ( - ) ),
38 ( 378, 50.700, 385, 51.050, BIF ( - ) ), 39 ( 386, 51.100, 393, 51.450, BIF ( - ) ),
40 ( 394, 51.500, 401, 51.850, BIF ( - ) ), 41 ( 402, 51.900, 409, 52.250, BIF ( - ) ),
42 ( 410, 52.300, 417, 52.650, BIF ( - ) ), 43 ( 418, 52.700, 425, 53.050, BIF ( - ) ),
44 ( 426, 53.100, 433, 53.450, BIF ( - ) ), 45 ( 434, 53.500, 441, 53.850, BIF ( - ) ),
46 ( 442, 53.900, 449, 54.250, BIF ( - ) ), 47 ( 450, 54.300, 457, 54.650, BIF ( - ) ),
48 ( 458, 54.700, 465, 55.050, BIF ( - ) ), 49 ( 466, 55.100, 473, 55.450, BIF ( - ) ),
50 ( 474, 55.500, 481, 55.850, BIF ( - ) ), 51 ( 482, 55.900, 489, 56.250, BIF ( - ) ),
52 ( 490, 56.300, 497, 56.650, BIF ( - ) ), 53 ( 498, 56.700, 505, 57.050, BIF ( - ) ),
54 ( 506, 57.100, 513, 57.450, BIF ( - ) ), 55 ( 514, 57.500, 521, 57.850, BIF ( - ) ),
56 ( 522, 57.900, 529, 58.250, BIF ( - ) ), 57 ( 530, 58.300, 537, 58.650, BIF ( - ) ),
58 ( 538, 58.700, 545, 59.050, BIF ( - ) ), 59 ( 546, 59.100, 553, 59.450, BIF ( - ) ),
60 ( 554, 59.500, 561, 59.850, BIF ( - ) ), 61 ( 562, 59.900, 569, 60.250, BIF ( - ) ),
62 ( 570, 60.300, 577, 60.650, BIF ( - ) ), 63 ( 578, 60.700, 585, 61.050, BIF ( - ) ),

```

```

64 ( 586, 61.100, 593, 61.450, BIF ( - ) ), 65 ( 594, 61.500, 601, 61.850, BIF ( - ) ),
66 ( 602, 61.900, 609, 62.250, BIF ( - ) ), 67 ( 610, 62.300, 617, 62.650, BIF ( - ) ),
68 ( 618, 62.700, 625, 63.050, BIF ( - ) ), 69 ( 626, 63.100, 633, 63.450, BIF ( - ) ),
70 ( 634, 63.500, 641, 63.850, BIF ( - ) ), 71 ( 642, 63.900, 649, 64.250, BIF ( - ) ),
72 ( 650, 64.300, 657, 64.650, BIF ( - ) ), 73 ( 658, 64.700, 665, 65.050, BIF ( - ) ),
74 ( 666, 65.100, 673, 65.450, BIF ( - ) ), 75 ( 674, 65.500, 681, 65.850, BIF ( - ) ),
76 ( 682, 65.900, 689, 66.250, BIF ( - ) ), 77 ( 690, 66.300, 697, 66.650, BIF ( - ) ),
78 ( 698, 66.700, 705, 67.050, BIF ( - ) ), 79 ( 706, 67.100, 713, 67.450, BIF ( - ) ),
80 ( 714, 67.500, 721, 67.850, BIF ( - ) ), 81 ( 722, 67.900, 729, 68.250, BIF ( - ) ),
82 ( 730, 68.300, 737, 68.650, BIF ( - ) ), 83 ( 738, 68.700, 745, 69.050, BIF ( - ) ),
84 ( 746, 69.100, 753, 69.450, BIF ( - ) ), 85 ( 754, 69.500, 761, 69.850, BIF ( - ) ),
86 ( 762, 69.900, 769, 70.250, BIF ( - ) ), 87 ( 770, 70.300, 777, 70.650, BIF ( - ) ),
88 ( 778, 70.700, 785, 71.050, BIF ( - ) ), 89 ( 786, 71.100, 793, 71.450, BIF ( - ) ),
90 ( 794, 71.500, 801, 71.850, BIF ( - ) ), 91 ( 802, 71.900, 809, 72.250, BIF ( - ) ),
92 ( 810, 72.300, 817, 72.650, BIF ( - ) ), 93 ( 818, 72.700, 825, 73.050, BIF ( - ) ),
94 ( 826, 73.100, 833, 73.450, BIF ( - ) ), 95 ( 834, 73.500, 841, 73.850, BI ( 0 ) ),
96 ( 842, 73.900, 849, 74.250, BI ( 0 ) ), 97 ( 850, 74.300, 857, 74.650, BI ( 0 ) ),
98 ( 858, 74.700, 865, 75.050, BI ( 0 ) ), 99 ( 866, 75.100, 873, 75.450, BI ( 0 ) ),
100 ( 874, 75.500, 881, 75.850, BI ( 0 ) ), 101 ( 882, 75.900, 889, 76.250, BI ( 0 ) ),
102 ( 890, 76.300, 897, 76.650, BI ( 0 ) ), 103 ( 898, 76.700, 905, 77.050, B ( 0 ) ),
104 ( 906, 77.100, 913, 77.450, B ( 0 ) ), 105 ( 914, 77.500, 921, 77.850, B ( 0 ) ),
106 ( 922, 77.900, 929, 78.250, B ( 0 ) ), 107 ( 930, 78.300, 937, 78.650, B ( 0 ) ),
108 ( 938, 78.700, 945, 79.050, B ( 0 ) ), 109 ( 946, 79.100, 953, 79.450, B ( 0 ) ),

```

Mapped to connector 4 and receiver 108

```

Bind to Cable1/0/4 US4
MER(SNR) - Unknown - no modems online.
Spectrum Group is unassigned
Nominal Input Power Level 0 dBmV

```

```

UCD procedures on lch 0
UCD ucd-proxy-timeout ( 0 ) ucd-proxy-wrong-ack ( 0 )

```

Configure Exclusion / Unused Bands

An OFDMA channel never uses frequencies that are located in exclusion bands. OFDMA probes are sent on frequencies that are located in the unused bands. Therefore exclusion bands must be used to prevent interference with SC-QAM channels. To configure the Exclusion / Unused Bands, follow these steps:

```

enable
configure terminal
cable upstream controller-profile id
cable ofdma-frequency-exclusion-band start-value end-value
cable ofdma-frequency-unused-band start-value end-value

```

Here is a configuration example:

```

Router# enable
Router# configure terminal
Router(config)# cable upstream controller-profile 33
Router(config-controller-profile)# cable ofdma-frequency-exclusion-band 48000000 54200000
Router(config-controller-profile)# cable ofdma-frequency-unused-band 50000000 52000000
Router(config-controller-profile)# us-channel 12 docsis-mode ofdma
Router(config-controller-profile)# us-channel 12 subcarrier-spacing 25KHz
Router(config-controller-profile)# us-channel 12 modulation-profile 423
Router(config-controller-profile)# us-channel 12 frequency-range 45000000 70000000
Router(config-controller-profile)# us-channel 12 cyclic-prefix 96 roll-off-period 64
Router(config-controller-profile)# us-channel 12 symbols-per-frame 18

```

Verify Exclusion / Unused Bands

To display the Exclusion / Unused Band configuration, use the **show controllers upstream-Cable us-channel** command as shown in the following example:

```
Router# show controllers upstream-Cable 1/0/2 us-channel 12
USPHY OFDMA support: FULL

Controller Exclusion Freq List:
( 40.000 MHz, 44.200 MHz),
Controller Unused Freq List:
( 50.000 MHz, 52.000 MHz),

Controller 1/0/9 upstream 12 AdminState:UP OpState: UP
ofdma mode enabled
Channel Freq Range 28.500 MHz to 69.500 MHz
Channel Subcarrier Index Range Cfg: 148, 1787 Op: 148, 1787
Channel SCO Freq Cfg: 24.800 MHz Op: 24.800 MHz
#Excl bands: 3
( 0, 147), ( 608, 776), (1788, 4095),
#Unused bands: 3
( 596, 607), (1001, 1088), (1777, 1787),
```

Override OFDMA Modulation Profile Per Channel

It is possible to override the modulation and pilot pattern that is used by a particular IUC on a given OFDMA channel as shown with the following command.

```
enable
configure terminal
cable upstream controller profile id
us-channel id data-iuc id band start-value end-value modulation value pilot-pattern
value
```

Here is a configuration example:

```
Router# enable
Router# configure terminal
Router(config)# cable upstream controller profile 33
Router(config-controller-profile)# us-channel 12 docsis-mode ofdma
Router(config-controller-profile)# us-channel 12 subcarrier-spacing 25KHz
Router(config-controller-profile)# us-channel 12 modulation-profile 423
Router(config-controller-profile)# us-channel 12 frequency-range 28000000 70000000
Router(config-controller-profile)# us-channel 12 cyclic-prefix 96 roll-off-period 64
Router(config-controller-profile)# us-channel 12 symbols-per-frame 18
Router(config-controller-profile)# us-channel 12 data-iuc 6 band 60000000 65000000 modulation
128-QAM pilot-pattern 9
Router(config-controller-profile)# no us-channel 12 shutdown
```



Note Override values are removed from the US channel when changing modulation profile, including when the profile changes due to changes in subcarrier spacing.

Verify Override Configuration

To display the override configuration, use the `show controllers upstream-Cable us-channel` command as shown in the following example:

```
Router# show controllers upstream-Cable 1/0/2 us-channel 12
```

```
.....
Modulation Profile (ID 423, Subcarrier Spacing 25KHz)
  IUC type   Cfg   Act   Preamble Bit   Pilot
            subc subc Symbols Loading Pattern
  3 (IR)    64   64    4             -     -
  4 (FR)   128  128    1             -     -
  6 (data)  -    -     -            1024-QAM 8
 10 (data) -    -     -             512-QAM 8
 11 (data) -    -     -             256-QAM 8
 12 (data) -    -     -             128-QAM 9
 13 (data) -    -     -              64-QAM 9
Overwrite Data Profile:
IUC Start End Start End Bit Pilot
 Freq(MHz) Freq(MHz) Subc Subc Loading Pattern
6 60.0 65.0 1408 1608 128-QAM 9

Calculated Data burst profile:
IUC Group Bit Pilot Start Consec
      Loading Pattern Mslot Mslot
6 0 1024-QAM 8 0 61
6 1 128-QAM 9 62 11
6 2 1024-QAM 8 74 10
10 0 512-QAM 8 0 84
11 0 256-QAM 8 0 84
12 0 128-QAM 9 0 84
13 0 64-QAM 9 0 84
.....
```

Bind OFDMA Channel Profile to Controller

To bind OFDMA channel profile to a controller, follow this example:

```
cable virtual-service-group sg-upstream-7-0-63 upstream-cable 7/0/63 profile 1

cable rpd node1
  identifier badb.ad15.1288
  core-interface Te7/1/4
    principal
      rpd-ds 0 downstream-cable 7/0/30 profile 10
      rpd-us 1 upstream-cable 7/0/63 profile 1
```



Note We recommend using separate channel profiles to debug issues on specific RPD port.

Bind OFDMA Upstream to Cable Interface

To associate upstream channels with a MAC domain and configure upstream bonding, follow these steps:

```
enable
configure terminal
```

```

interface Cable slot/subslot/interface
upstream id Upstream-Cable slot/subslot/interface us-channel id
cable upstream bonding-group id
upstream id
attributes value
cable bundle id

```

Here is a configuration example:

```

Router# enable
Router# configure terminal
Router(config)# interface Cable 1/0/4
Router(config-if)# downstream Integrated-Cable 1/0/4 rf-channel 0
Router(config-if)# downstream Integrated-Cable 1/0/4 rf-channel 16
Router(config-if)# upstream 0 Upstream-Cable 1/0/0 us-channel 0
Router(config-if)# upstream 1 Upstream-Cable 1/0/0 us-channel 1
Router(config-if)# upstream 2 Upstream-Cable 1/0/0 us-channel 2
Router(config-if)# upstream 3 Upstream-Cable 1/0/0 us-channel 3
Router(config-if)# upstream 6 Upstream-Cable 1/0/0 us-channel 12
Router(config-if)# cable upstream bonding-group 1
Router(config-upstream-bonding)# upstream 0
Router(config-upstream-bonding)# upstream 1
Router(config-upstream-bonding)# upstream 2
Router(config-upstream-bonding)# upstream 3
Router(config-upstream-bonding)# attributes 80000000
Router(config-upstream-bonding)# exit
Router(config-if)# cable upstream bonding-group 2
Router(config-upstream-bonding)# upstream 0
Router(config-upstream-bonding)# upstream 1
Router(config-upstream-bonding)# upstream 2
Router(config-upstream-bonding)# upstream 3
Router(config-upstream-bonding)# upstream 6
Router(config-upstream-bonding)# attributes 80000000
Router(config-upstream-bonding)# exit
Router(config-if)# cable bundle 1

```

Determine DOCSIS 3.1 Cable Modems and the Cable Modems Using OFDMA Upstreams

To display the DOCSIS 3.1 cable modem, use the **show cable modem docsis version d31-capable** command as shown in the following example:

```

Router# show cable modem docsis version d31-capable
MAC Address      I/F          MAC              Reg Oper DSxUS DS   RCC   US
                  State        Ver Ver          OFDM ID          OFDMA
4800.33ea.7012 C1/0/0/UB   w-online (pt)   3.1 3.1   33x4  1    5     1
203d.66ae.4169 C1/0/0/UB   w-online (pt)   3.1 3.1   33x4  1    5     1

```

To display DOCSIS PHY layer information for the cable modem, use the **show cable modem phy** command as shown in the following example:

```

Router# show cable modem 5039.5584.5bbe phy
MAC Address      I/F          Sid  USPwr  USMER  Timing  DSPwr  DSMER  Mode  DOCSIS
                  (dBmV)      (SNR) Offset (dBmV) (SNR)  (dB)  (dB)  Prov
5039.5584.5bbe C1/0/0/U0   15   38.75  ----- 2282   0.00  ----- ofdma  1.1

```

To display the cable modem using OFDMA upstream, use the **show cable modem phy** command as shown in the following example:

```
Router# show cable modem phy | include ofdma
5039.5584.5bbe C1/0/0/U0 15 38.75 ----- 2282 0.00 ----- ofdma 1.1
0895.2a9b.26f1 C1/0/0/U0 16 28.00 ----- 2146 0.00 ----- ofdma 1.1
```

To display the OFDMA channel capacity and utilization, use the **show interface cable mac-scheduler** command as shown in the following example:

```
Router# show interfaces cable 1/0/2 mac-scheduler 6
DOCSIS 1.1 MAC scheduler for Cable1/0/2/U6 : rate 279807192
Max potential performance for each configured IUC type
IUC: 6 rate: 279807192
IUC: 10 rate: 263104848
IUC: 11 rate: 233779840
IUC: 12 rate: 203019328
IUC: 13 rate: 173899376
wfq:None
us_balance:OFF
dpon_mode:OFF
fairness:OFF
Queue[Rng Polls] flows 0
Queue[CIR Grants] flows 0
Queue[BE(07) Grants] flows 0
Queue[BE(06) Grants] flows 0
Queue[BE(05) Grants] flows 0
Queue[BE(04) Grants] flows 0
Queue[BE(03) Grants] flows 0
Queue[BE(02) Grants] flows 0
Queue[BE(01) Grants] flows 0
Queue[BE(00) Grants] flows 0
Req Slots 38510548
Req/Data Slots 1275
Init Mtn Slots 47832
Stn Mtn Slots 0
IUC 5 Slots 0
IUC 6 Slots 6378
IUC 9 Slots 0
IUC 10 Slots 254923830
IUC 11 Slots 220
IUC 12 Slots 4006
IUC 13 Slots 251213508
Avg upstream channel utilization : 0%
Avg upstream channel utilization in 30 sec : 0%
Avg percent contention slots : 96%
Avg percent initial ranging slots : 0%
Avg percent minislots lost on late MAPs : 0%

MAP TSS: lch_state 10, init_retries 0
         late_initial_maps 0, late_ucd_maps 0
         mac-phy tss errors 0, missed ccc 0
```

Verify DOCSIS 3.1 Upstream OFDMA Channel Bonding Across DOCSIS 3.0 ATDMA Channels

DOCSIS 3.1 Upstream OFDMA channel can be bonded with DOCSIS 3.0 ATDMA channel. If the user wants to utilize non-best effort flows, it is recommended to bond the OFDMA channel with one or more ATDMA channels. A maximum of 1 OFDMA channel and 4 ATDMA channels can be bonded together.

Below is an output example showing the bonding group 8 has both OFDMA (channel 12) and ATDMA channels (channel 0, 1, 2, 3).

```
interface Cable6/0/0
  downstream Integrated-Cable 6/0/0 rf-channel 1
  downstream Integrated-Cable 6/0/0 rf-channel 158
  upstream 0 Upstream-Cable 6/0/0 us-channel 0
  upstream 1 Upstream-Cable 6/0/0 us-channel 1
  upstream 2 Upstream-Cable 6/0/0 us-channel 2
  upstream 3 Upstream-Cable 6/0/0 us-channel 3
  upstream 6 Upstream-Cable 6/0/0 us-channel 12
  cable upstream bonding-group 1
    upstream 0
    upstream 1
    upstream 2
    upstream 3
    attributes 80000000
  cable upstream bonding-group 8
    upstream 0
    upstream 1
    upstream 2
    upstream 3
    upstream 6
    attributes 80000000
  cable bundle 1
  cable privacy accept-self-signed-certificate
end
```

Support for Line Card High Availability

N+1 line card high availability (LCHA) is supported for modems that are assigned OFDMA upstream channels. If LCHA is enabled, the modems remain active after switchover and revert.

Configure Line Card High Availability

For information on configuring for Line Card High Availability, go through the *Cable Line Card Process Restart* content in the topic *Consolidated Packages and SubPackages Management* in the document [Cisco cBR Converged Broadband Routers Basic Configuration Guide for Cisco IOS XE](#).

Support for Line Card Process Restart

Linecard IOSd and linecard US-Scheduler (CDMAN) process restart (LCPR) is supported for modems that are assigned OFDMA upstream channels. If LCPR is enabled, remote phy devices remain active after process restarts.

Configure Line Card Process Restart

For information on configuring for Line Card Process Restart, go through the *Cable Line Card Process Restart* content in the topic *Consolidated Packages and SubPackages Management* in the document [Cisco cBR Converged Broadband Routers Basic Configuration Guide for Cisco IOS XE](#).

Feature Information for DOCSIS 3.1 OFDMA Channel Configuration

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



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

Table 44: Feature Information for DOCSIS 3.1 OFDMA Channel Configuration

Feature Name	Releases	Feature Information
Remote PHY DOCSIS 3.1 OFDMA Channel Configuration	Cisco 1x2 / Compact Shelf RPD Software 5.1 Cisco IOS XE Fuji 16.9.1	This feature was introduced on the Cisco Remote PHY Device and Cisco cBR Series Converged Broadband Routers.
Support for Line Card High Availability	Cisco 1x2 / Compact Shelf RPD Software 6.1 Cisco IOS XE Gibraltar 16.10.1	This feature was introduced on the Cisco Remote PHY Device and Cisco cBR Series Converged Broadband Routers.
Support for Line Card Process Restart	Cisco 1x2 / Compact Shelf RPD Software 6.1 Cisco IOS XE Gibraltar 16.10.1	This feature was introduced on the Cisco Remote PHY Device and Cisco cBR Series Converged Broadband Routers.



CHAPTER 23

Spectrum Capture

- [Hardware Compatibility Matrix for Cisco Remote PHY Device, on page 167](#)
- [Spectrum Capture, on page 168](#)
- [Verifying Spectrum Capture Configuration, on page 168](#)
- [Feature Information for Spectrum Capture, on page 169](#)

Hardware Compatibility Matrix for Cisco Remote PHY Device



Note Unless otherwise specified, the hardware components introduced in a given Cisco Remote PHY Device Software Release are supported in all subsequent releases.

Table 45: Hardware Compatibility Matrix for the Cisco Remote PHY Device

Cisco HFC Platform	Remote PHY Device
Cisco GS7000 Super High Output Node	Cisco 1x2 / Compact Shelf RPD Software 2.1 and Later Releases
Cisco GS7000 Super High Output Intelligent Node (iNode)	Cisco 1x2 / Compact Shelf RPD Software 4.1 and Later Releases Cisco Intelligent Remote PHY Device 1x2 <ul style="list-style-type: none">• PID—iRPD-1X2=• PID—iRPD-1X2-PKEY=

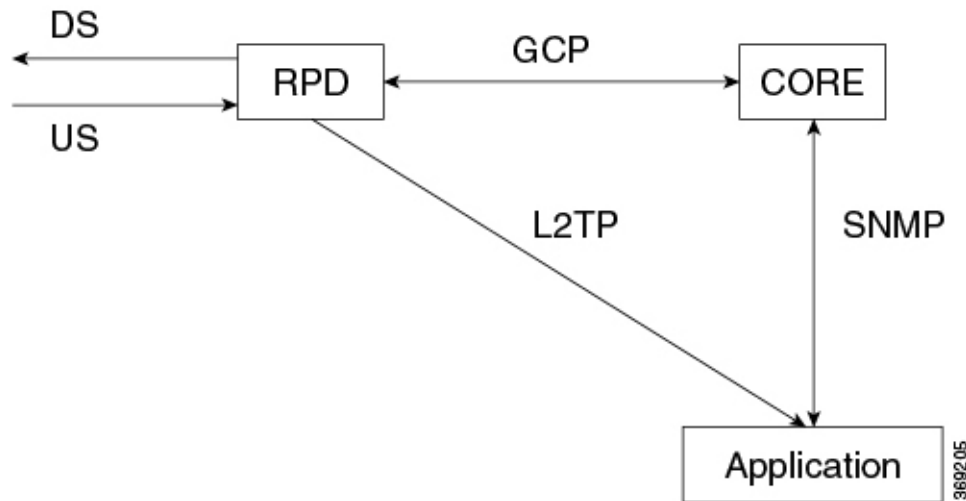


Note The -PKEY suffix in the PID indicates units that enable the SCTE-55-2 Out-of-Band protocol support.

Spectrum Capture

The upstream triggered spectrum analysis measurement provides a wideband spectrum analyzer function in the CCAP which can be triggered to examine desired upstream transmissions as well as underlying noise or interference during a quiet period. WBFFT stands for Wide Band Fast Fourier Transform. This feature allows all RPD US ports to enable an upstream spectrum analyzer built into the RPD's front end. RPD supports FreeRunning trigger mode.

Figure 8: Spectrum capture workflow



Note US FFT data is computed and sent directly from US PHY. RPD firmware does not handle these data. The firmware configures US PHY to send L2TP stream based on GCP TLV messages.

Please refer to below link for cBR8 configuration about this feature:

https://www.cisco.com/c/en/us/td/docs/cable/cbr/configuration/guide/b_cbr_docsis_full_book_xe16_10/b_cbr_docsis_full_book_xe16_10_chapter_0100110.html



- Note**
1. This feature provides a stream of raw spectrum data only.
 2. The application that interprets and presents the data in human readable format is not part of this feature.

Verifying Spectrum Capture Configuration

To verify if the spectrum capture is enabled, use **show bcm-register wbfft config** command as shown in the following example. The WBFFT Trigger Mode should be FreeRunning if this feature is enabled.

```
R-PHY#show bcm-register wbfft config
WBFFT Trigger Mode : FreeRunning
```

```

Enable UTSC           : TRUE
Sample Num            : 4096
Session ID            : 44201020
PNM Dest IP           : 2001:30:84:0:1:0:66:1
PNM Dest Mac          : c414.3c16.d682

R-PHY#show bcm-register wfft all 0
WBFFT Start Ctrl     [cc000000] : 00000001
In Control            [cc000004] : 00472F04
Out Control           [cc00000c] : 0000009B
Timing Ctrl          [cc000010] : 00000003
WBFFT FIRST WDW CF   [cc000024] : 00000920
WBFFT SCND WDW CF    [cc000028] : 0000C660
WBFFT MIDL WDW CF    [cc00002c] : 000061E0
WBFFT MAX CTL        [d0000048] : 33800000
WBFFT Status         [cc000034] : 00000000

WBFFTS In Ctrl       [d0000044] : 00000100
WBFFT PKT BYTE       : 004A0000
WBFFT PKT COUNT      : 00004A00

```

Feature Information for Spectrum Capture

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

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

Table 46: Feature Information for Spectrum Capture

Feature Name	Releases	Feature Information
Spectrum Capture	Cisco 1x2 / Compact Shelf RPD Software 6.4	This feature was integrated into the Cisco Remote PHY Device.



CHAPTER 24

Viavi Integration

- [Hardware Compatibility Matrix for Cisco Remote PHY Device, on page 171](#)
- [Viavi Integration, on page 172](#)
- [Verifying Spectrum Capture Configuration, on page 172](#)
- [Feature Information for Viavi Integration, on page 173](#)

Hardware Compatibility Matrix for Cisco Remote PHY Device



Note Unless otherwise specified, the hardware components introduced in a given Cisco Remote PHY Device Software Release are supported in all subsequent releases.

Table 47: Hardware Compatibility Matrix for the Cisco Remote PHY Device

Cisco HFC Platform	Remote PHY Device
Cisco GS7000 Super High Output Node	Cisco 1x2 / Compact Shelf RPD Software 2.1 and Later Releases
Cisco GS7000 Super High Output Intelligent Node (iNode)	Cisco 1x2 / Compact Shelf RPD Software 4.1 and Later Releases Cisco Intelligent Remote PHY Device 1x2 <ul style="list-style-type: none">• PID—iRPD-1X2=• PID—iRPD-1X2-PKEY=

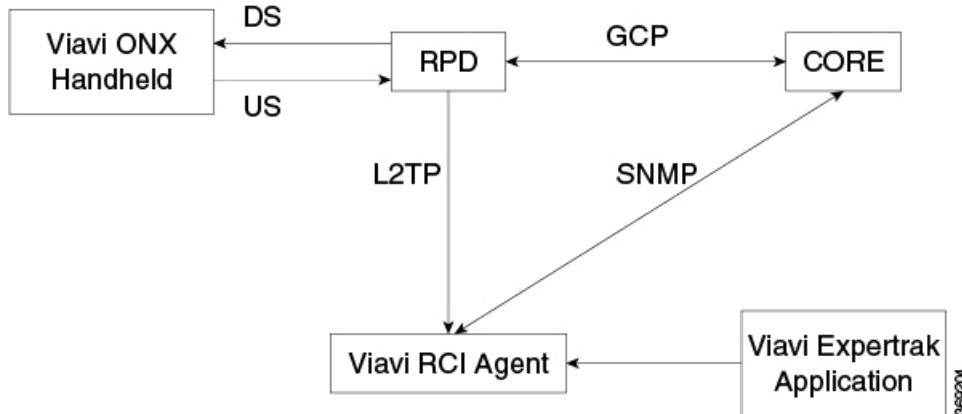


Note The -PKEY suffix in the PID indicates units that enable the SCTE-55-2 Out-of-Band protocol support.

Viavi Integration

In this feature, RPD supports non-CCAP defined MAX-HOLD mode for spectrum capture that work with Viavi RCI Agent.

Figure 9: Viavi integration workflow



- Note**
1. Communications with core is implemented using SNMP.
 2. Before using this feature, the NDF/NDR feature must be configured on cBR-8.
 3. Viavi RCI Agent needs to be installed and configured on the system with Linux/Ubuntu operating system.

Verifying Spectrum Capture Configuration

To verify if the spectrum capture is enabled, use `show bcm-register wbbft config` command as shown in the following example. The WBFFT Trigger Mode should be FreeRunning if this feature is enabled.

```

R-PHY#show bcm-register wbbft config
WBFFT Trigger Mode : FreeRunning
Enable UTSC       : TRUE
Sample Num        : 4096
Session ID        : 44201020
PNM Dest IP       : 2001:30:84:0:1:0:66:1
PNM Dest Mac      : c414.3c16.d682

R-PHY#show bcm-register wbbft all 0
WBFFT Start Ctrl  [cc000000] : 00000001
In Control        [cc000004] : 00472F04
Out Control       [cc00000c] : 0000009B
Timing Ctrl      [cc000010] : 00000003
WBFFT FIRST WDW CF [cc000024] : 00000920
WBFFT SCND WDW CF [cc000028] : 0000C660
WBFFT MIDL WDW CF [cc00002c] : 000061E0
WBFFT MAX CTL     [d0000048] : 33800000
WBFFT Status      [cc000034] : 00000000
  
```



```
WBFFTS In Ctrl      [d0000044]      : 00000100
WBFFT PKT BYTE      : 004A0000
WBFFT PKT COUNT     : 00004A00
```

Feature Information for Viavi Integration

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

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

Table 48: Feature Information for Viavi Integration

Feature Name	Releases	Feature Information
Viavi Integration	Cisco 1x2 / Compact Shelf RPD Software 6.4	This feature was integrated into the Cisco Remote PHY Device.



PART **IV**

Remote PHY System Video Configuration

- [Cisco Remote PHY Video Configuration, on page 177](#)
- [Remote PHY DVB Video on Demand, on page 185](#)
- [Cisco Remote PHY PowerKEY VOD, on page 197](#)
- [Cisco Remote PHY Pre-encrypted Broadcast Video, on page 205](#)
- [Remote PHY BFS QAM Configuration, on page 211](#)
- [Remote PHY Switched Digital Video, on page 223](#)
- [Remote PHY QAM Profile Configuration, on page 235](#)
- [Cisco Remote PHY Out of Band, on page 239](#)



CHAPTER 25

Cisco Remote PHY Video Configuration

Finding Feature Information

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

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

- [Hardware Compatibility Matrix for Cisco Remote PHY Device, on page 177](#)
- [Hardware Compatibility Matrix for Cisco Remote PHY Device, on page 178](#)
- [Information About R-PHY Video Configuration, on page 178](#)
- [How to Configure R-PHY Video, on page 179](#)
- [Example: R-PHY Video Configuration, on page 182](#)
- [Feature Information for Remote PHY Video, on page 184](#)

Hardware Compatibility Matrix for Cisco Remote PHY Device



Note Unless otherwise specified, the hardware components introduced in a given Cisco Remote PHY Device Software Release are supported in all subsequent releases.

Table 49: Hardware Compatibility Matrix for the Cisco Remote PHY Device

Cisco HFC Platform	Remote PHY Device
Cisco GS7000 Super High Output Node	Cisco 1x2 / Compact Shelf RPD Software 2.1 and Later Releases

Cisco HFC Platform	Remote PHY Device
Cisco GS7000 Super High Output Intelligent Node (iNode)	Cisco 1x2 / Compact Shelf RPD Software 4.1 and Later Releases Cisco Intelligent Remote PHY Device 1x2 <ul style="list-style-type: none"> • PID—iRPD-1X2= • PID—iRPD-1X2-PKEY=



Note The -PKEY suffix in the PID indicates units that enable the SCTE-55-2 Out-of-Band protocol support.

Hardware Compatibility Matrix for Cisco Remote PHY Device



Note Unless otherwise specified, the hardware components introduced in a given Cisco Remote PHY Device Software Release are supported in all subsequent releases.

Table 50: Hardware Compatibility Matrix for the Cisco Remote PHY Device

Cisco HFC Platform	Remote PHY Device
Cisco GS7000 Super High Output Node	Cisco 1x2 / Compact Shelf RPD Software 2.1 and Later Releases
Cisco GS7000 Super High Output Intelligent Node (iNode)	Cisco 1x2 / Compact Shelf RPD Software 4.1 and Later Releases Cisco Intelligent Remote PHY Device 1x2 <ul style="list-style-type: none"> • PID—iRPD-1X2= • PID—iRPD-1X2-PKEY=



Note The -PKEY suffix in the PID indicates units that enable the SCTE-55-2 Out-of-Band protocol support.

Information About R-PHY Video Configuration

The controller profile specifies the RF channels that belong to this profile and their RF parameters. Profile can either be unicast or multicast.

Multicast profile is used for downstream sharing. Multiple Remote PHY Devices (RPDs) can be configured to receive the same downstream controller. The traffic is multicast to all RPDs configured to receive the

downstream controller. Applications include Video on Demand (VOD), Switched Digital Video (SDV) and Broadcast Video.

There is one principal core interface, and up to four auxiliary core interfaces in the RPD configuration. Principal core specifies the DPIC interface with which RPD connects. Auxiliary cores specify external DPIC interfaces that can be used for downstream sharing. Auxiliary core is currently used for narrowcast video, broadcast video and out-of-band data signaling path (OOB) only.

The Cisco RPD 2x2 supports the Extended US Frequency Range, as described in the DOCSIS Physical Layer Specification. The extended US frequency range of 5-85 MHz is an optional range for a CM to transmit.

How to Configure R-PHY Video

This section describes how to configure R-PHY video on Cisco cBR-8.

Configuring Downstream Controller Profile

To configure the downstream controller profile, use the example below:

```
Router# configure terminal
Router(config)# cable depi multicast pool 20
Router(config-multicast-pool)# ip address 225.28.0.0 255.255.0.0
Router(config-multicast-pool)# exit
Router(config)# cable downstream controller-profile 1
Router(config-controller-profile)# multicast-pool 20
Router(config-controller-profile)# rf-chan 0 15
Router(config-prof-rf-chan)# type docsis
Router(config-prof-rf-chan)# frequency 111000000
Router(config-prof-rf-chan)# rf-output normal
Router(config-prof-rf-chan)# qam-profile 1
Router(config-prof-rf-chan)# docsis-channel-id 1
Router(config-prof-rf-chan)# exit
Router(config-controller-profile)# rf-chan 16 19
Router(config-prof-rf-chan)# type video sync
Router(config-prof-rf-chan)# frequency 699000000
Router(config-prof-rf-chan)# rf-output normal
Router(config-prof-rf-chan)# qam-profile 1
Router(config-prof-rf-chan)# exit
Router(config-controller-profile)# exit
Router(config)# cable downstream controller-profile 2
Router(config-controller-profile)# multicast-pool 1
Router(config-controller-profile)# rf-chan 20 47
Router(config-prof-rf-chan)# type video sync
Router(config-prof-rf-chan)# frequency 231000000
Router(config-prof-rf-chan)# rf-output normal
Router(config-prof-rf-chan)# qam-profile 4
```

In the above example, two profiles are configured, profile 1 is a mixed profile, profile 2 is a video only profile.

Configuring RPD

To configure the RPD to include the controller profile, follow the example below:

```
Router# configure terminal
Router(config)# cable rpd RPD01
Router(config-rpd)# identifier 0004.9f31.0455
```

```

Router(config-rpd)# core-interface Te3/1/0
Router(config-rpd-core)# principal
Router(config-rpd-core)# rpd-ds 0 downstream-cable 3/0/0 profile 1
Router(config-rpd-core)# rpd-ds 0 downstream-cable 3/0/1 profile 2
Router(config-rpd-core)# rpd-us 0 upstream-cable 3/0/0 profile 1
Router(config-rpd-core)# exit
Router(config-rpd)# core-interface te6/1/0
Router(config-rpd-core)# rpd-ds 0 downstream-cable 6/0/0 profile 2
Router(config-rpd-core)# exit
Router(config-rpd)# r-dti 1
Router(config-rpd)# rpd-event profile 0
Router(config-rpd)# rpd-55d1-us-event profile 0

```

**Note**

- All channels within the profiles of a RPD must be unique, frequencies must not overlap each other.
- There must be at least one DOCSIS downstream profile in the principal core.
- Auxiliary core must only contain video and out-of-band profiles.
- A downstream controller can only be associated to one profile.

Configuring Downstream Sharing

Downstream sharing is used for multicast (MC) traffic. To configure downstream sharing, follow the example below:

```

Router# configure terminal
Router(config)# cable rpd RPD01
Router(config-rpd)# core-interface Te3/1/0
Router(config-rpd-core)# principal
Router(config-rpd-core)# rpd-ds 0 downstream-cable 3/0/1 profile 2
Router(config-rpd-core)# exit
Router(config-rpd)# exit
Router(config)# cable rpd RPD02
Router(config-rpd)# core-interface te3/1/0
Router(config-rpd-core)# principal
Router(config-rpd-core)# rpd-ds 0 downstream-cable 3/0/1 profile 2
Router(config-rpd-core)# exit
Router(config-rpd)# exit
Router(config)# cable rpd RPD03
Router(config-rpd)# core-interface te6/1/0
Router(config-rpd-core)# principal
Router(config-rpd-core)# rpd-ds 0 downstream-cable 6/0/1 profile 3
Router(config-rpd-core)# exit
Router(config-rpd)# core-interface te3/1/0
Router(config-rpd-core)# rpd-ds 0 downstream-cable 3/0/1 profile 2

```

**Note**

All RPDs in the same multicast group have the same controller and profile association.

Configuring Video

To configure Video, see [Cisco Converged Broadband Routers Video Configuration Guide for Cisco IOS XE Everest 16.5.1](#).

Configuring Virtual Service Group

Virtual Service Group is supported to allow the controller configuration and removal of an RPD using that controller without removing the video configuration. To configure virtual service group, follow the example below:

1. Add controller profile:

```
Router(config)# cable downstream controller-profile 2
Router(config-controller-profile)# multicast-pool 20
Router(config-controller-profile)# rf-channel 20 47
Router(config-prof-rf-chan)# type video sync
Router(config-prof-rf-chan)# frequency 231000000
Router(config-prof-rf-chan)# rf-output NORMAL
Router(config-prof-rf-chan)# qam-profile 7
Router(config-prof-rf-chan)# exit
Router(config-controller-profile)# exit
```

2. Assign controller profile to a downstream cable for a virtual service group:

```
Router(config)# cable virtual-service-group VOD_SG1801 downstream-cable 9/0/1 profile 2
Router(config)# cable virtual-service-group VOD_SG1802 downstream-cable 9/0/3 profile 2
Router(config)# cable virtual-service-group BC_Chicago downstream-cable 9/0/31 profile 3
```

3. Create VCG, SDG, RPD downstream cable, bind VCG to SDG, assign VCG to LED, set LED active, and create sessions:

```
Router(config)# cable video
Router(config-video)# multicast-uplink Port-channel22 access-list all-multicasts
Router(config-video)# mgmt-intf VirtualPortGroup 0
Router(config-video)# service-distribution-group sdg91 id 91
Router(config-video-sdg)# rpd downstream-cable 9/0/1
Router(config-video-sdg)# exit
Router(config-video)# virtual-carrier-group vcg91 id 91
Router(config-video-vcg)# encrypt
Router(config-video-vcg)# service-type narrowcast
Router(config-video-vcg)# rf-channel 40-63 tsid 38001-38024 output-port-number 1-24
Router(config-video-vcg)# exit
Router(config-video)# bind-vcg
Router(config-video-bd)# vcg vcg91 sdg sdg91
Router(config-video-bd)# exit
Router(config-video)# logical-edge-device led-1 id 1
Router(config-video-led)# protocol table-based
Router(config-video-led-protocol)# virtual-edge-input-ip 174.102.1.1 input-port-number 1
Router(config-video-led-protocol)# vcg vcg91
Router(config-video-led-protocol)# active
Router(config-video-led-protocol)# table-based
Router(config-video-tb)# vcg vcg91
Router(config-video-tb-vcg)# rf-channel 40
Router(config-video-tb-vcg-sess)# session ss group 232.2.1.251 source 175.2.3.2
processing-type remap
```

4. Assign controller to RPD, then physical QAM id is allocated and video sessions are online:

```

Router(config)# cable rpd RPD01
Router(config-rpd)# identifier 0004.9f32.1573
Router(config-rpd)# core-interface Te9/1/0
Router(config-rpd-core)# principal
Router(config-rpd-core)# rpd-ds 0 downstream-cable 9/0/1 profile 2
Router(config-rpd-core)# rpd-ds 0 downstream-cable 9/0/3 profile 2
Router(config-rpd-core)# rpd-us 0 upstream-cable 9/0/0 profile 1
Router(config-rpd-core)# exit
Router(config-rpd)# core-interface Te9/1/6
Router(config-rpd-core)# rpd-ds 0 BC_Chicago
Router(config-rpd-core)# exit
Router(config-rpd)# r-dti 1
Router(config-rpd)# rpd-event profile 0
Router(config-rpd)# rpd-55d1-us-event profile 0

```

- It is allowed to remove or replace the controller from the RPD configuration as show below, without touching any video configuration, then the video sessions are in off state which is similar to the scenario that the video QAM is shut down.

```

Router(config)# cable rpd RPD01
Router(config-rpd)# core-interface Te9/1/0
Router(config-rpd-core)# no rpd-ds 0 downstream-cable 9/0/1 profile 2

```

**Note**

If virtual service group doesn't exist while adding controller downstream to RPD configuration, virtual service group is automatically generated when the controller profile has one or more rf-channels of the video type. If the user changes RPD downstream configuration to use another controller profile different from the one in virtual service group and in the meantime video configuration exists, the user also needs to update the controller profile in the virtual service group for that downstream as well, otherwise all the video sessions will be down.

Example: R-PHY Video Configuration

The following example shows how to configure Remote-PHY video:

```

Router# configure terminal
Router(config)# cable downstream qam-profile 7
Router(config-qam-prof)# annex B modulation 256
Router(config-qam-prof)# interleaver-depth I32-J4
Router(config-qam-prof)# symbol-rate 5361
Router(config-qam-prof)# spectrum-inversion off
Router(config-qam-prof)# description default-annex-b-256-qam
Router(config-qam-prof)# exit
Router(config)# cable depi multicast pool 20
Router(config-multicast-pool)# ip address 225.28.0.0 255.255.0.0
Router(config-multicast-pool)# exit
Router(config)# cable downstream controller-profile 1
Router(config-controller-profile)# multicast-pool 20
Router(config-controller-profile)# rf-channel 0 15
Router(config-prof-rf-chan)# type docsis
Router(config-prof-rf-chan)# frequency 111000000
Router(config-prof-rf-chan)# rf-output NORMAL
Router(config-prof-rf-chan)# qam-profile 7
Router(config-prof-rf-chan)# docsis-channel-id 1
Router(config-prof-rf-chan)# exit
Router(config-controller-profile)# exit

```

```
Router(config)# cable downstream controller-profile 2
Router(config-controller-profile)# multicast-pool 20
Router(config-controller-profile)# rf-channel 20 47
Router(config-prof-rf-chan)# type video sync
Router(config-prof-rf-chan)# frequency 231000000
Router(config-prof-rf-chan)# rf-output NORMAL
Router(config-prof-rf-chan)# qam-profile 7
Router(config-prof-rf-chan)# exit
Router(config-controller-profile)# exit
Router(config)# cable rpd RPD01
Router(config-rpd)# identifier 0004.9f31.0979
Router(config-rpd)# core-interface te6/1/0
Router(config-rpd-core)# principal
Router(config-rpd-core)# rpd-ds 0 downstream-cable 6/0/0 profile 1
Router(config-rpd-core)# rpd-ds 0 downstream-cable 6/0/1 profile 2
Router(config-rpd-core)# rpd-us 0 upstream-cable 6/0/0 profile 1
Router(config-rpd-core)# exit
Router(config-rpd)# r-dti 6
Router(config-rpd)# rpd-event profile 0
Router(config-rpd)# rpd-55dl-us-event profile 0
Router(config-rpd)# exit
Router(config)# cable rpd RPD2
Router(config-rpd)# identifier 0004.9f31.1437
Router(config-rpd)# core-interface Te3/1/0
Router(config-rpd-core)# principal
Router(config-rpd-core)# rpd-ds 0 downstream-cable 3/0/0 profile 1
Router(config-rpd-core)# rpd-us 0 upstream-cable 3/0/0 profile 1
Router(config-rpd-core)# exit
Router(config-rpd)# core-interface Te6/1/0
Router(config-rpd-core)# rpd-ds 0 downstream-cable 6/0/1 profile 2
Router(config-rpd-core)# exit
Router(config-rpd)# r-dti 3
Router(config-rpd)# rpd-event profile 0
Router(config-rpd)# rpd-55dl-us-event profile 0
Router(config-rpd)# exit
Router(config)# cable video
Router(config-video)# service-distribution-group RPD_SDG
Router(config-video-sdg)# rpd downstream-cable 6/0/1
Router(config-video-sdg)# exit
Router(config-video)# virtual-carrier-group RPC_VCG
Router(config-video-vcg)# rf-channel 20-47 tsid 20-47 output-port-number 20-47
Router(config-video-vcg)# exit
Router(config-video)# bind-vcg
Router(config-video-bd)# vcg RPC_VCG sdg RPD_SDG
Router(config-video-bd)# exit
Router(config-video)# logical-edge-device RPD_LED
Router(config-video-led)# protocol table-based
Router(config-video-led-protocol)# virtual-edge-input-ip 174.102.1.1 input-port-number 1
Router(config-video-led-protocol)# vcg RPD_VCG
Router(config-video-led-protocol)# active
Router(config-video-led-protocol)# table-based
Router(config-video-tb)# vcg RPD_VCG
Router(config-video-tb-vcg)# rf-channel 20-47
Router(config-video-tb-vcg-sess)# session tb-session-1 input-port 1 start-udp-port 49152
num-sessions-per-qam 20 processing-type remap start-program 1 bit-rate 1800000
```

Feature Information for Remote PHY Video

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



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

Table 51: Feature Information for Remote PHY Video

Feature Name	Releases	Feature Information
RPHY Video PME VOD	Cisco 1x2 / Compact Shelf RPD Software 3.1	This feature was integrated into the Cisco Remote PHY Device.
RPHY Video Pre-Encrypted MPTS Pass-Thru Support	Cisco 1x2 / Compact Shelf RPD Software 3.1	This feature was integrated into the Cisco Remote PHY Device.
RPHY Pre-encrypted Broadcast Video Support	Cisco 1x2 / Compact Shelf RPD Software 3.1	This feature was integrated into the Cisco Remote PHY Device.



CHAPTER 26

Remote PHY DVB Video on Demand

The Digital Video Broadcasting (DVB) protocol for encrypting video services as defined in the ETSI TS 103 197 DVB Simulcrypt specification has been implemented on the line card for DVB R-PHY on Cisco cBR-8. This document contains an overview of the commands for configuring DVB and the commands for viewing the status of the encryption of services.

Finding Feature Information

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

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

- [Information About DVB VOD, on page 185](#)
- [How to Configure DVB, on page 187](#)
- [Configuration Examples, on page 191](#)
- [Additional References, on page 194](#)
- [Feature Information for RPHY DVB VoD Support, on page 194](#)

Information About DVB VOD

Overview of DVB VOD

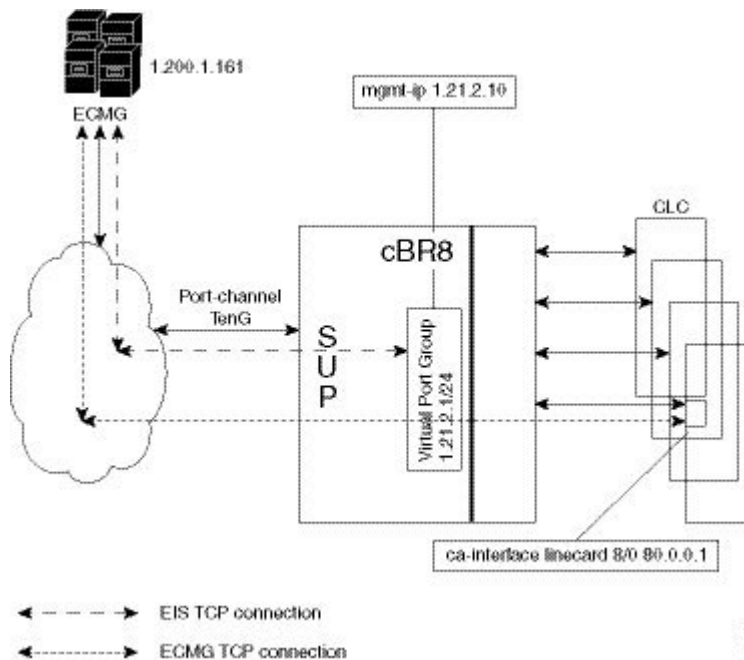
This feature enables the operator to scramble the video sessions on the chassis. It involves the configuration to establish a connection with the Entitlement Control Message Generator (ECMG) and the Event Information Scheduler (EIS).

The two primary modes of scrambling are: session based scrambling and tier-based scrambling. The basic difference between the two modes is that the manner in which the Entitlement Control Messages (ECM) are requested from the ECMG. For session based scrambling, a control word (CW) is generated once every Crypto Period (CP) and the ECM is requested for each session. For tier-based scrambling, the control word is generated once every CP and the ECM generated by the ECMG for the CW is used by all the sessions in the chassis.

Session based Scrambling Setup

The connection with the external EIS Server is established via the Virtual Port Group in the Supervisor. The connection with the external ECMG server is established via the linecard.

Figure 10: Session based Setup



Fail-to-Clear

The fail-to-clear-duration feature is supported on DVB sessions and DualCrypt encryption modes. Based on the session encryption, the following two features are supported on the Cisco cBR Series Converged Broadband Routers.

Fail-to-Clear Duration for DVB Session-based Encryption

This feature is used along with DVB or DualCrypt encryption with external Event Information Scheduler (EIS) configuration. When encryption for a session fails in the Cisco cBR-8, this feature enables the operator to control the configured DVB-encrypted sessions to function without encryption for a configured duration. If the encryption still fails, the DVB session is marked as `Fail-to-black` after the fail-to-clear duration timeout.

Fail-to-Clear for DVB Tier-based Encryption

This feature is used along with Tier-based configuration. When encryption for a session fails in Cisco cBR-8, this feature enables the operator to control the configured DVB-encrypted sessions to function without encryption.

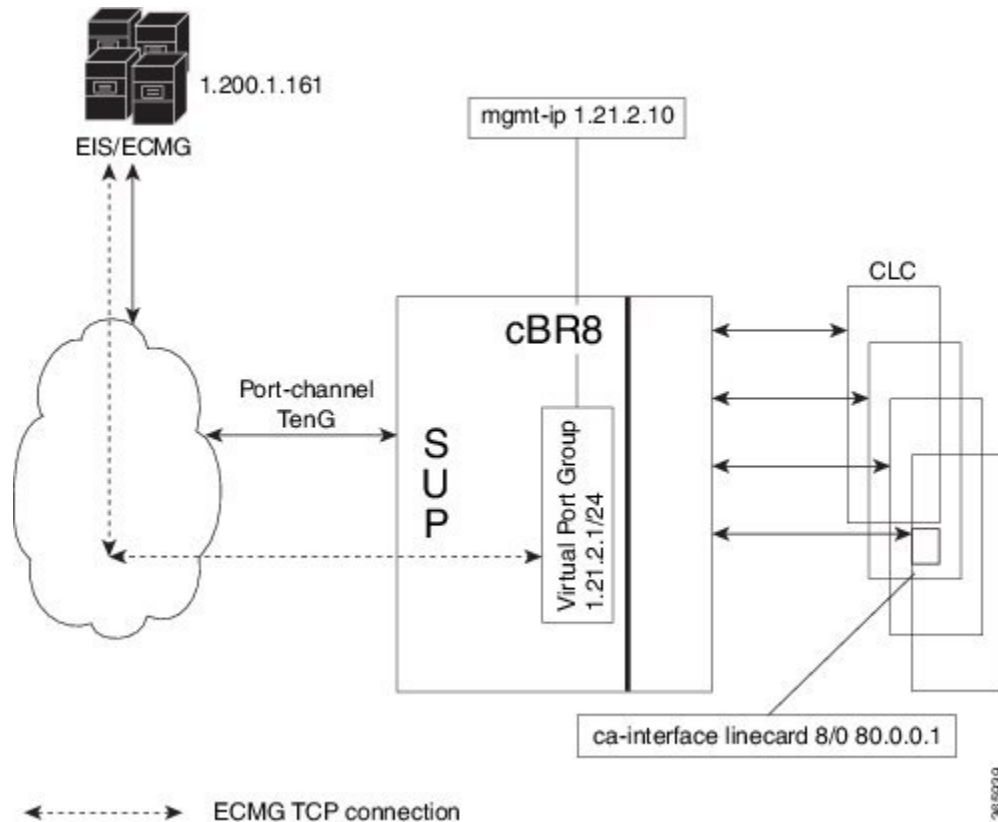
If fail-to-clear is configured, tier-based configuration is enabled, and then if the encryption fails, the DVB session's `Encrypt Status` is marked as `clear`. The status changes to `Encrypted` when the encryption starts.

This feature is not enabled by default.

Tier based Scrambling Setup

The connection with the external ECMG server is established via the Virtual Port Group in the Supervisor.

Figure 11: Tier based Setup



Restrictions for DVB

- This feature is applicable only for remapped table based sessions.
- Fail-to-clear-duration feature is applicable only to session-based scrambling for DVB CAS encryption.
- Fail-to-clear feature is applicable only to DVB tier-based scrambling sessions.

How to Configure DVB

Configuring RPHY DVB VoD

Before You Begin

- Virtual Port Group interface must be configured and the management IP for DVB must be identified.
- Management interface is set to this Virtual Port Group interface under cable video configuration.

- Logical Edge Device is configured with the table based protocol.
- The encryption algorithm of the linecard is set to DVB-CSA.
- For session based scrambling, the CA interface on the linecard and the route for reaching the ECMG server must be specified.

To configure session based scrambling, follow the steps below:

```
enable
config terminal
interface int_id
  vrf forwarding vrf_script_red_1
  ip address ip-address subnet-mask
  no mop enabled
  no mop sysid
  exit
cable video
  mgmt-intf VirtualPortGroup group_id
  encryption
    linecard slot/bay ca-system dvb scrambler dvb-csa
    dvb
      route-ecmg ECMG_Server_IP_Address Netmask Interface Forwarding_Router_IP_Address
      mgmt-ip management ip address
      eis EIS_name id EIS_id
        listening-port <1-65535> bind led id <led id | led name>
      ca-interface linecard slot/bay IP_Address
      ecmg ECMG_Name id ECMG_ID
        mode vod linecard slot/bay
        type standard
        ca-system-id CA_System_ID CA_Subsystem_ID
        auto-channel-id
        ecm-pid-source sid
        connection id ID priority connection_priority IP_Address Port
      service-distribution-group sdg name id SDG_ID onid onid number
      rpd downstream-cable slot/subslot/bay
      virtual-carrier-group vcg-name id vcg_id
      encrypt
        service-type narrowcast
        rf-channel channel tsid tsid_number output-port-number number
      bind-vcg
        vcg vcg-name sdg sdg-name
      logical-edge-device led-name id led_id
        protocol gqi
        mgmt-ip IP_Address
        mac-address MAC address
        server server_ip_address
        keepalive retry 3 interval 10
        reset interval 8
        virtual-edge-input-ip IP address input-port-number 1
        vcg vcg-name
        active
```

The fail-to-clear-duration is measured in seconds. The valid values are in the range from 0 to 10800 seconds. The default value is 0.

To configure tier based scrambling, follow the steps below:

```
enable
config terminal
interface VirtualPortGroup group_id
  vrf forwarding Mgmt-intf
  ip address ip-address subnet-mask
```



```

no mop enabled
no mop sysid
exit

cable video
mgmt-intf VirtualPortGroup group_id
encryption
  linecard slot/bay ca-system dvb scrambler dvb-csa
  dvb
    route-ecmg ECMG_Server_IP_Address Netmask Interface Forwarding_Router_IP_Address
    ecmg ECMG_Name id ECMG_ID
    mode tier-based
    type standard
    ca-system-id CA_System_ID CA_Subsystem_ID
    auto-channel-id
    ecm-pid-source sid
    connection id ID priority connection_priority IP_Address Port
    tier-based
    ecmg id ECMG_ID access- criteria access_criteria_in_hex
    fail-to-clear
    enable
  service-distribution-group sdg name id SDG ID onid onid number
  rpd downstream-cable slot/subslot/port
  virtual-carrier-group vcg-name id vcg_id
  encrypt
  service-type narrowcast
  rf-channel channel tsid tsid_number output-port-number number
  bind-vcg
  vcg vcg-name sdg sdg-name
  logical-edge-device led-name id led_id
  protocol table-based
  virtual-edge-input-ip IP address input-port-number 1
  vcg vcg-name
  active
  table-based
  vcg vcg-name
  rf-channel channel
  session session_name input-port id start-udp-port udp port number processing-type
  remap start-program 1 cbr

```



Note If the tier-based configuration is already enabled, you must first disable the tier-based configuration using the **no enable**, before you configure fail-to-clear feature.

Verifying the DVB Configuration

To verify the configuration of the encryption algorithm on the linecard, use the **show cable video encryption linecard** command as shown in the example below:

```

Router# show cable video encryption linecard 7/0
Line card: 7/0
CA System      Scrambler      DVB-Conformance
=====
dvb            dvb-csa        Enabled

```

To verify the ECMG connection, use the **show cable video encryption dvb ecmg id id connection** command as shown in the example below:

```
Router# show cable video encryption dvb ecmg id 1 connection
```

ECMG ID	ECMG Name	ECMG Slot	ECMG Type	ECMG Connections	CA Sys ID	CA Subsys ID	PID Source	Lower limit	Upper limit	Streams/ECMG	Open Streams/ECMG	ID
1	polaris_ecmg01		standard		0x4748	0x0	sid	0	0	1	1	
Enabled RP 1 Tier-Based												

```
ECMG Connections for ECMG ID = 1
```

Conn -ID	Conn Priority	IP Address	Port Number	Channel ID	Conn Status	Open Streams
1	1	10.10.1.1	8888	1	Open	1

The sample output of the session based scrambling configuration verification command is shown below:

```
Router# show cable video encryption dvb ecmg id 7 connection
```

ECMG ID	ECMG Name	ECMG Slot	ECMG Type	ECMG Connections	CA Sys ID	CA Subsys ID	PID Source	Lower limit	Upper limit	Streams/ECMG	Open Streams/ECMG	ID
7	ecmg-7		standard		0x950	0x1234	sid	0	0	1680	1680	
Enabled 7 1 VOD												

```
ECMG Connections for ECMG ID = 1
```

Conn -ID	Conn Priority	IP Address	Port Number	Channel ID	Conn Status	Open Streams
1	1	10.10.1.10	8888	1	Open	1

The status of the connection with the ECMG Server is indicated by the Conn Status. The Open Streams field indicates the number of Active ECM Streams.

To verify the EIS connection, use the **show cable video encryption dvb eis id id** command as shown in the example below:

```
Router# show cable video encryption dvb eis id 1
```

EIS ID	EIS Name	Peer IP	Management IP	TCP Port	CP Overrule	CP Duration	Overwrite SCG	Fail-To-Clear Duration	Connection Status
1	test	10.10.1.11	10.10.1.1	9898	DISABLED	0	DISABLED	400	Connected

To verify the CA Interface configuration in the case of session based scrambling, use the **show cable video encryption dvb ca-interface brief** command as shown in the example below:

```
Router# show cable video encryption dvb ca-interface brief
CA Interface configuration
```

Linecard	IP Address	VRF
7	10.10.1.1	N/A

```
ECMG Route configuration
```

```

IP Address      NetMast          Interface
-----
10.10.1.10     255.255.255.224 TenGigabitEthernet4/1/2

```

To verify the encryption status of the sessions, use the **show cable video session logical-edge-device id** command as shown in the example below:

```

Router# show cable video session logical-edge-device id 1
Total Sessions = 1

Session Output Streaming Session Session Source          UDP   Output  Input
Output Input  Output Encrypt Encrypt  Low   Session
Id      Port   Type   Type   Ucast Dest IP/Mcast IP (S, G) Port  Program State
State  Bitrate Bitrate Type   Status Latency Name
-----
1048576 1      Remap  UDP    10.10.1.1          49167 20    ACTIVE-PSI
      1695161 1689747 DVB    Encrypted N      dvbsess.1.0.1.0.23167

```

To verify the ECM PID and whether the CA Descriptor is added to the PMT, use the **show cable video session logical-edge-device id session-id** command as shown in the example below:

```

Router# show cable video session logical-edge-device id 1 session-id 1048576
Output PMT Info:
=====
Program 20, Version 3, PCR 49, Info len 18, (CA SYS-ID 4748, PID 79)
PID 49: Type 2, Info len 0
PID 50: Type 3, Info len 6, (lang eng)

```

Troubleshooting Tips

If some configuration errors occur, see the following troubleshooting tips:

- The Management IP must be unique and in the subnet of virtual port group.
- Ensure that the ECMG Server is pingable with source interface as the virtual port group from the Cisco cBR-8 console. This indicates that the ECMG Server is reachable and route is valid.
- Ensure that the TCP port number configured for the ECMG Server in the Cisco cBR-8 is the same as that of the ECMG Server listening port.
- Ensure that the management IP is pingable from the EIS Server. Otherwise, check the routing between the cBR-8 chassis and the EIS server.
- Ensure that the listening port that is configured for the EIS is used for establishing the connection from the EIS Server.
- Ensure that the Virtual Port Group interface is active.
- Ensure that the TenGigabitEthernet interface using which the management traffic reaches the Cisco cBR-8 and the interface through which the CA interface route is configured are active.

Configuration Examples

This section provides examples for the DVB configuration.

Example: Basic Session-based Scrambling Configuration

```

enable
config terminal
interface VirtualPortGroup0
  vrf forwarding vrf_script_red_1
  ip address 10.10.1.1 255.255.255.224
  no mop enabled
  no mop sysid
  exit
cable video
  mgmt-intf VirtualPortGroup 0
  encryption
    linecard 7/0 ca-system dvb scrambler dvb-csa
    dvb
      route-ecmg 10.20.1.1 255.255.255.224 TenGigabitEthernet4/1/2 10.20.1.1
      mgmt-ip 10.10.1.2
      eis eis-1 id 1
        listening-port 8890 bind led id 1
      ca-interface linecard 7/0 10.30.1.1
      ecmg ecmg-7 id 7
        mode vod linecard 7/0
        type standard
        ca-system-id 950 1234
        auto-channel-id
        ecm-pid-source sid
        connection id 1 priority 1 10.20.1.3 8888
      service-distribution-group sdg-1 id 1 onid 1
        rpd downstream-cable 7/0/1
      virtual-carrier-group vcg-1 id 1
        encrypt
          service-type narrowcast
          rf-channel 0 tsid 1 output-port-number 1
        bind-vcg
          vcg vcg-1 sdg sdg-1
        logical-edge-device led-1 id 1
          protocol table-based
          virtual-edge-input-ip 192.0.2.0 input-port-number 1
          vcg vcg-1
            active
            table-based
              vcg vcg-1
                rf-channel 0
                  session dvb-1 input-port 1 start-udp-port 49152 processing-type
remap start-program 1 cbr

```

Example: Basic Tier-based Scrambling Configuration

```

enable
config terminal
interface VirtualPortGroup0
  vrf forwarding vrf_script_red_1
  ip address 10.10.1.1 255.255.255.224
  no mop enabled
  no mop sysid
  exit
cable video
  mgmt-intf VirtualPortGroup 0
  encryption
    linecard 7/0 ca-system dvb scrambler dvb-csa
    dvb

```

```

route-ecmg 10.20.1.0 255.255.255.224 TenGigabitEthernet4/1/2 10.20.1.1
ecmg ecmg-7 id 7
  mode tier-based
  type standard
  ca-system-id 950 1234
  auto-channel-id
  ecm-pid-source sid
  connection id 1 priority 1 10.20.1.3 8888
tier-based
  ecmg id 7 access-criteria 1122334455
  fail-to-clear
  enable
service-distribution-group sdg-1 id 1 onid 1
  rpd downstream-cable 7/0/1
virtual-carrier-group vcg-1 id 1
  encrypt
  service-type narrowcast
  rf-channel 0 tsid 1 output-port-number 1
bind-vcg
  vcg vcg-1 sdg sdg-1
logical-edge-device led-1 id 1
  protocol table-based
  virtual-edge-input-ip 192.0.2.0 input-port-number 1
  vcg vcg-1
  active
table-based
  vcg vcg-1
  rf-channel 0
  session dvb-1 input-port 1 start-udp-port 49152 processing-type remap start-program
1 cbr

```

Example: Basic Session-based Dualcrypt Scrambling Configuration

```

enable
config terminal
interface VirtualPortGroup0
  vrf forwarding vrf_script_red_1
  ip address 10.10.1.1 255.255.255.224
  no mop enabled
  no mop sysid
  exit
cable video
mgmt-intf VirtualPortGroup 0
encryption
  linecard 7/0 ca-system dvb scrambler dvb-csa
  dvb
    route-ecmg 10.20.1.0 255.255.255.224 TenGigabitEthernet4/1/2 10.20.1.1
    mgmt-ip 10.10.1.2
    eis eis-1 id 1
      listening-port 8890 bind led id 1
    ca-interface linecard 7/0 10.30.1.1
  ecmg ecmg-7 id 7
    mode vod linecard 7/0
    type standard
    ca-system-id 950 1234
    auto-channel-id
    ecm-pid-source sid
    connection id 1 priority 1 10.20.1.3 8888
  service-distribution-group sdg-1 id 1 onid 1
    rpd downstream-cable 7/0/1
  virtual-carrier-group vcg-1 id 1
    encrypt
    service-type narrowcast
    rf-channel 0 tsid 1 output-port-number 1

```

```

bind-vcg
vcg vcg-1 sdg sdg-1
logical-edge-device led-1 id 1
protocol gqi
  mgmt-ip 10.10.1.3
  mac-address xxxx.yyyy.zzzz
  server 10.20.1.2
  keepalive retry 3 interval 10
  reset interval 8
  virtual-edge-input-ip 192.0.2.0 input-port-number 1
vcg vcg-1
active

```

Additional References

Related Documents

Related Topic	Document Title
Configuring Tier-Based Scrambling	<i>Cisco RF Gateway 10 Software Configuration Guide</i>

Technical Assistance

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

Feature Information for RPHY DVB VoD Support

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



Note

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

Table 52: Feature Information for RPHY DVB VoD Support

Feature Name	Releases	Feature Information
RPHY DVB VoD Support	Cisco 1x2 / Compact Shelf RPD Software 3.1	This feature was introduced on the Cisco Remote PHY Device.



CHAPTER 27

Cisco Remote PHY PowerKEY VOD

PowerKEY Video-on-Demand refers to video content that is chosen by the subscriber and streamed specifically to the subscriber. The content is encrypted using PowerKEY conditional access through a video session that is created on the line card in R-PHY mode on Cisco cBR-8, specifically for each request.

Finding Feature Information

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

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

- [Hardware Compatibility Matrix for Cisco Remote PHY Device](#), on page 197
- [Information About PowerKEY VOD](#), on page 198
- [How to Configure RPHY PowerKey VOD](#), on page 198
- [Configuration Examples](#), on page 203
- [Feature Information for Rmote PHY PowerKEY VoD](#), on page 204

Hardware Compatibility Matrix for Cisco Remote PHY Device



Note Unless otherwise specified, the hardware components introduced in a given Cisco Remote PHY Device Software Release are supported in all subsequent releases.

Table 53: Hardware Compatibility Matrix for the Cisco Remote PHY Device

Cisco HFC Platform	Remote PHY Device
Cisco GS7000 Super High Output Node	Cisco 1x2 / Compact Shelf RPD Software 2.1 and Later Releases

Cisco HFC Platform	Remote PHY Device
Cisco GS7000 Super High Output Intelligent Node (iNode)	Cisco 1x2 / Compact Shelf RPD Software 4.1 and Later Releases Cisco Intelligent Remote PHY Device 1x2 <ul style="list-style-type: none"> • PID—iRPD-1X2= • PID—iRPD-1X2-PKEY=



Note The -PKEY suffix in the PID indicates units that enable the SCTE-55-2 Out-of-Band protocol support.

Information About PowerKEY VOD

The line cards in R-PHY mode on Cisco cBR-8 supports session-based PowerKey VOD. In both RPHY and integrated modes, the Cisco cBR-8 router establishes a GQI Remote Procedure Call (RPC) connection to the Edge Resource Manager (SRM), which may be an Explorer Controller (EC), USRM, or any other session manager. The Cisco cBR-8 supports 40G-R line cards, which can be configured for RPHY.

Configure the PowerKey VOD carriers in a GQI protocol LED. The Virtual Carrier Groups (VCG) in the LED, must be bound to a Service Distribution Group (SDG) with downstream-cable ports (instead of the integrated-cable ports).

Overview of PowerKEY VoD

PowerKEY VOD allows the operator to provide secure, encrypted video streams to a particular subscriber over the RF plant. PowerKEY video-on-demand is used in a Cisco cable environment to provide edge-encrypted video-on-demand movies and other content to subscribers. A subscriber can select the content through an on-screen selection and the set-top box (STB) notifies the head-end of the request.

The head-end equipment receives the request from the STB and triggers the Session Resource Manager (SRM) to create an encrypted video session on the Cisco cBR-8. At the same time, the video streamer is triggered to begin streaming the content in a UDP stream to the Cisco cBR-8. The Cisco cBR-8 receives an unscrambled video content, encrypts it using PowerKEY, combines the scrambled stream with other content intended for the RF carrier into a Multi-Program Transport Stream (MPTS), encapsulates it using R-DEPI protocol, and sends it out on Ethernet port to the Converged Interconnect Network (CIN) between the cBR-8 RPHY core and the RPHY Device (RPD).

How to Configure RPHY PowerKey VOD

Configuring the Encryption Type on the Line Card

The Cisco IOS-XE supports PowerKey encryption CA systems, but allows only one encryption type to be installed on the line card. There are two levels in the CA system. The lower level scrambler, which encrypts

the actual data streams and the upper level conditional access system, which handles how the control words are transferred from the encrypting device to the decrypting device.

To specify the type of encryption used to scramble the data streams, complete the following procedure:

```
configure terminal cable video encryption
linecard slot/bay ca-system [powerkey] scrambler scrambler-type
exit
```

PowerKey currently supports DES type of encryption.

Verifying the Encryption Configuration

To verify the encryption type of a line card, use the `show cable video encryption linecard` command as shown in the following example:

```
show cable video encryption linecard 7/0
Line card: 7/0
CA System Scrambler
=====
powerkey des
```

Configuring the Encrypted Virtual Carrier Groups

For the sessions to be encrypted on the Cisco cBR-8, the Virtual Carrier Groups (VCGs) must be specified as `encrypt` and the line card must be configured as encrypted. In this way, the operator can choose the carriers on the line card that support encryption and other carriers that support only clear or pre-encrypted sessions. Each encrypted carrier consumes an encrypted carrier license.

For the VCG to be used in a Logical Edge Device (LED) that is configured with the GQI protocol, each RF carrier must be assigned with an output port number. The LED must be configured with the Generic QAM Interface (GQI) protocol in order to support session-based operation.



Note For PowerKEY VOD, you have to specify the session-based operation.

To configure the VCG, complete the following procedure:

```
configure terminal cable video
virtual-carrier-group vcg-name
encrypt
rf-channel channel range tsid tsid range output-port-number port num range
exit
```

Configuring the Encrypted Virtual Carrier Groups

For the sessions to be encrypted on the Cisco cBR-8, the Virtual Carrier Groups (VCGs) must be specified as **encrypt** and the line card must be configured as encrypted. In this way, the operator can choose the carriers on the line card that support encryption and other carriers that support only clear or pre-encrypted sessions. Each encrypted carrier consumes an encrypted carrier license.

For the VCG to be used in a Logical Edge Device (LED) that is configured with the GQI protocol, each RF carrier must be assigned with an output port number. The LED must be configured with the Generic QAM Interface (GQI) protocol in order to support session-based operation.



Note For PowerKEY VOD, you have to specify the session-based operation.

To configure the VCG, complete the following procedure:

```
configure terminal
cable video
virtual-carrier-group vcg-name
rf-channel channel range tsid tsid range output-port-number port num range
virtual-edge-input ip-address [vrf] vrf name input-port-number number
encrypt
exit
```

Verifying the Encrypted Virtual Carrier Groups Configuration

To verify the encrypted VCGs configuration, use the **show cable video virtual-carrier-group name** command as shown in the example below:

```
show cable video virtual-carrier-group name vod-grp
```

Configuring the Service Distribution Groups and Binding

The Service Distribution Group (SDG) is a collection of one or more RF ports and defines the physical slot/bay/port to be used in a video service. After you configure an SDG, you can bind a VCG to an SDG. The binding connects the carriers defined in the VCG to the physical port listed in the SDG. After binding, a path from the Virtual Edge Input (VEI) is mapped to the RF channels.

The following example shows how to configure the SDGs and binding:

```
configure terminal cable video
  mgmt-intf VirtualPortGroup 0

service-distribution-group sdg1 id 1
  rpd downstream-cable 7/0/0
virtual-carrier-group vcg1 id 1
  service-type narrowcast
  encrypt
  rf-channel 0-10 tsid 1-11 output-port-number 1-11

bind-vcg
  vcg vcg1 sdg sdg1
```

Configuring the Logical Edge Device and GQI Protocol

The PowerKEY VOD feature on the Cisco cBR-8 is directed by an external Session Resource Manager (SRM) that creates video sessions in response to a subscriber selecting VOD content to watch on the set top box. You must configure a Logical Edge Device (LED) supporting the GQI protocol on the Cisco cBR-8 to support the PowerKEY VOD.

The LED is configured with the GQI protocol as the LED communicates with an external SRM using the GQI protocol. The GQI protocol supports the creation and deletion of sessions on the carriers owned by this LED.



Note Use the following command to get the chassis MAC address:

```
Router#show diag all eeprom detail | include MAC
Chassis MAC Address : 54a2.740e.2000
MAC Address block size : 1024
```

Using the Chassis MAC as a basis, increment the least significant number to give a unique identifier (mac-address) for each LED. This number needs to be unique with respect to the GQI server and does not really relate to a true MAC address. Thus, the number is irrelevant, but needs to be unique.

To configure the Logical Edge Device and GQI Protocol, complete the following procedure:

```
cable video
logical-edge-device led1 id 1
  protocol gqi
    mgmt-ip management ip address
    mac-address mac address from this chassis range
    server ip address of srm
    keepalive retry 3 interval 10
    reset interval 8
    virtual-edge-input-ip ip addr for content input-port-number num
    vcg virtual edge qam name (may be multiple vcgs in an LED)
  active
```

Verifying the PowerKEY VoD Configuration

The PowerKEY encrypted VOD LED is active and communicates with the external SRM device after configuring the encryption type on the line card, VCGs, binding of SDGs, and LED with GQI protocol are completed.

To verify the Logical Edge Device configuration, use the show cable video logical-edge-device name led name command or the show cable video logical-edge-device id led number command as shown in the example below:

```
show cable video logical-edge-device name pkvodled
Logical Edge Device: pkvodled
Id: 1
Protocol: gqi
Service State: Active
Discovery State: Disable
Management IP: 1.23.2.10
MAC Address: 54a2.740d.dc99
Number of Servers: 1
Server 1: 1.200.3.75
Reset Interval: 8
Keepalive Interval: 10
Retry Count:3
Number of Virtual Carrier Groups: 1
Number of Share Virtual Edge Input: 1
Number of Physical Qams: 20
Number of Sessions: 0
No Reserve PID Range
Virtual Edge Input:
Input Port  VEI          Slot/Bay  Bundle  Gateway
ID    IP        ID    IP
-----
1          174.10.2.1  7/0  -  -
```

Verify the following:

- The service state of the LED should be active and the other fields must be same as the configured values.
- The connection to the remote SRM should be displayed to ensure that there is a valid network connection to the SRM.
- Execute the `show cable video gqi connections` command. The following is the sample output when the connection is not established to the SRM:

```
LED Management Server      Connection      Version Event      Reset      Encryption
ID  IP    IP  Status        Pending Indication Discovery
-----
1   1.23.2.10  1.200.3.75 Not Connected  0 0          Not Sent    Not Sent
```

The following is the sample output when the connection is established to the SRM:

```
LED Management Server      Connection      Version Event      Reset      Encryption
ID  IP    IP  Status        Pending Indication Discovery
-----
1   1.23.2.10  1.200.3.75 Not Connected  2 0    ACKED ACKED
```

After the connection is established, the SRM may create encrypted sessions on the carriers of the LED.

- To view the encrypted sessions, use the `show cable video session logical-edge-device id led name summary` command as shown in the example below:

```
show cable video session logical-edge-device id lsummary
Video Session Summary:

Active      : 1  Init      : 0  Idle      : 0
Off         : 0  Blocked : 0  PSI-Ready : 1
UDP         : 1  ASM       : 0  SSM       : 0
Remap       : 1  Data      : 0  Passthru  : 0
Total Sessions: 1
```

- The individual session information can be displayed for the entire LED, for a particular port or line card. The details of a single session may be displayed by specifying a session-id or session-name. To display all the sessions on the LED, use the `show cable video session logical-edge-device name led name` command as shown in the example below:

```
show cable video session logical-edge-device name pkvodled
Total Sessions = 1

Session Output Streaming Session Destination UDP   Output  Input  Output Input
Id  Port  Type      Type      Port  Program State  State  Bitrate
-----
1048576 1      Remap     UDP       174.101.1.1 4915  1 ACTIVE-PSI ON    732788

Output Encrypt  Encrypt  Session
Bitrate Type    Status   Name
-----
1715446 PowerKey Encrypted 0x00000000000001
```

If the session is encrypted and transmitted properly, the session is displayed as shown in the above example. The input state is "ACTIVE-PSI". The output state is "ON". For PowerKEY encrypted sessions, the Encrypt Type will be "PowerKey" and the Encrypt Status will be "Encrypted".

If the session is created as a clear session, then the Encrypt Type will be "CLEAR" and the Encrypt Status will be "-".

Configuration Examples

This section provides configuration examples for the PowerKEY VOD feature:

Example: Configuring Encryption Type on the Line Card

The following example shows how to create a management IP interface:

```
configure terminal cable video encryption
linecard 6/0 ca-system powerkey scrambler des
exit
```

Example: Configuring Encrypted Virtual Carrier Groups

The following example shows how to configure the QAM channels from 64 to 158. These channels are encryption capable once the VCG is successfully bound to a Service Distribution Group. The sessions created on these QAM carriers are encrypted using the scrambler installed on the line card.

```
configure terminal cable video
virtual-carrier-group RPC_VCG
encrypt
rf-channel 20-47 tsid 20-47 output-port-number 20-47
virtual-edge-input-ip 174.102.1.1 input-port-number 1
exit
```

Example: Configuring Service Distribution Groups and Binding

The following example shows how to configure the service distribution groups and binding:

```
configure terminal cable video
  mgmt-intf VirtualPortGroup 0

service-distribution-group sdg1 id 1
  rpd downstream-cable 7/0/0
virtual-carrier-group vcg1 id 1
  service-type narrowcast
  encrypt
  rf-channel 0-10 tsid 1-11 output-port-number 1-11

bind-vcg
  vcg vcg1 sdg sdg1
logical-edge-device led1 id 1
  protocol gqi
  mgmt-ip 1.22.2.10
  mac-address c414.3c17.e001
  server 1.200.1.189
  keepalive retry 3 interval 10
  reset interval 8
  virtual-edge-input-ip 174.102.1.1 input-port-number 1
  vcg vcg2
  active
```

Feature Information for Rmote PHY PowerKEY VoD

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



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

Table 54: Feature Information for RPHY PowerKEY VoD

Feature Name	Releases	Feature Information
Remote PHY PowerKEY VoD	Cisco 1x2 / Compact Shelf RPD Software 3.1	This feature was integrated into Cisco Remonte PHY Device.



CHAPTER 28

Cisco Remote PHY Pre-encrypted Broadcast Video

This document describes how to configure pre-encrypted Broadcast Video sessions on Cisco cBR-8 routers.

Finding Feature Information

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

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

- [Hardware Compatibility Matrix for Cisco Remote PHY Device](#), on page 205
- [Information About Pre-encrypted Broadcast Video](#), on page 206
- [How to Configure Pre-encrypted Broadcast Video Sessions](#), on page 207
- [Configuration Example for Pre-encrypted Broadcast Video Session](#), on page 208
- [Feature Information for RPHY Pre-encrypted Broadcast Video](#), on page 208

Hardware Compatibility Matrix for Cisco Remote PHY Device



Note Unless otherwise specified, the hardware components introduced in a given Cisco Remote PHY Device Software Release are supported in all subsequent releases.

Table 55: Hardware Compatibility Matrix for the Cisco Remote PHY Device

Cisco HFC Platform	Remote PHY Device
Cisco GS7000 Super High Output Node	Cisco 1x2 / Compact Shelf RPD Software 2.1 and Later Releases

Cisco HFC Platform	Remote PHY Device
Cisco GS7000 Super High Output Intelligent Node (iNode)	Cisco 1x2 / Compact Shelf RPD Software 4.1 and Later Releases Cisco Intelligent Remote PHY Device 1x2 <ul style="list-style-type: none"> • PID—iRPD-1X2= • PID—iRPD-1X2-PKEY=



Note The -PKEY suffix in the PID indicates units that enable the SCTE-55-2 Out-of-Band protocol support.

Information About Pre-encrypted Broadcast Video

The Cisco cBR-8 line card supports broadcast video. It also provides support to the WAN ports for receiving Multi program Transport Streams (MPTS). The Cisco cBR passes the MPTS streams in its entirety to multiple RPDs in the network to provide an output on their RF ports.

The content is multiplexed and encrypted during upstream traffic and reaches Cisco cBR-8 router as pre-encrypted in a constant bit-rate MPTS with all the PSI present. The Cisco cBR routers perform the following:

- De-jittering
- Clock recovery
- PCR re-stamping
- Regenerates PAT with correct TSID

Typically, multi-system operators (MSO) have between 64 and 75 carriers of Broadcast video content in their system. In the RPHY environment, the Cisco cBR routers convert the Broadcast carriers into DEPI multicast streams and send them to an unlimited number of RPDs over the Converged Interconnect Network.

Multicast Table-based Sessions

Similar to table-based unicast session configuration, sessions can be configured as individual sessions under each QAM carrier that is assigned to a table-based LED. To configure multicast video session, you must configure a port-channel interface.

A multicast session can be configured with a single input multicast input source or multiple input sources for backup purpose. For multiple backup sources, a label is required to be associated with the session configuration. Same label can be applied to multiple sessions on different QAM channel. These sessions are considered as cloned sessions.

For session cloning on multiple QAMs within the same line card, only one copy of the traffic is forwarded to the line card. The line card replicates the input packets and forwards them to multiple QAMs. Each cloned copy of a remapped session will have the same or different output program number.

MPTS Pass-through Session

The Cisco cBR-8 router supports multicast MPTS pass-session type. For a pass-through session:

- The PMT and other program data are not changed.
- PID remapping is not performed.
- Input NULL packets are dropped.
- Oversubscription results in random TP dropping, and all ghost PIDs are preserved in the output.

How to Configure Pre-encrypted Broadcast Video Sessions

This section contains the following:

Configure a Port-Channel Interface

The following example shows how to configure a port-channel interface.

```
interface Port-channel27
description connection for Core A
ip address 2.27.1.1 255.255.255.252
ip pim sparse-mode
ip access-group 101 out
ip igmp version 3
ip ospf 64512 area 27
load-interval 30
carrier-delay msec 500
```

Configuring Pre-encrypted Broadcast Sessions

The following example shows how to configure the pre-encrypted Broadcast Video sessions on Cisco cBR routers.

```
cable video
multicast-uplink Port-channel32 access-list all-multicasts

table-based
  multicast-label label group group-ip source source-ip source2 source-ip source3 source-ip
  source4 source-ip
  multicast-label label group group-ip source source-ip source2 source-ip source3 source-ip
  source4 source-ip

  vcg vcg-name
  rf-channel channel
  session session-name multicast-label label processing-type {remap | passthru | data}
cbr
  rf-channel channel
  session session-name multicast-label label processing-type {remap | passthru | data}
cbr
```

Configuring the Service Distribution Groups and Binding

The Service Distribution Group (SDG) defines the physical slot/bay/port to be used in a video service. After you configure an SDG, you can bind a VCG to an SDG. The binding connects the carriers defined in the VCG to the physical port listed in the SDG. After binding, a path from the Virtual Edge Input (VEI) is mapped to the RF channels.

The following example shows how to configure the SDGs and binding:

```
configure terminal
cable video
service-distribution-group sdg99 id 99
    rpd downstream-cable 9/0/31

    virtual-carrier-group vcg99 id 99
        service-type broadcast
        rf-channel 64-78 tsid 38901-38915 output-port-number 1-15
        rf-channel 80-127 tsid 38917-38964 output-port-number 17-64

bind-vcg
    vcg vcg99 sdg sdg99

logical-edge-device led31 id 31
protocol table-based
vcg vcg99
active
```

Configuration Example for Pre-encrypted Broadcast Video Session

The following example shows an example of configuring pre-encrypted Broadcast Video sessions on Cisco cBR routers.

```
cable video
table-based
    multicast-label mpts1 group 236.0.1.1 source 175.10.5.2 source2 175.10.6.2 source3
175.10.7.2 source4 175.10.8.2
    multicast-label mpts2 group 236.0.1.2 source 175.10.5.2 source2 175.10.6.2 source3
175.10.7.2 source4 175.10.8.2
    vcg vcg99
    rf-channel 64
        session mpts1 multicast-label mpts1 processing-type passthru cbr
    rf-channel 65
        session mpts2 multicast-label mpts2 processing-type passthru cbr
```

Feature Information for RPHY Pre-encrypted Broadcast Video

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



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

Table 56: Feature Information for RPHY Pre-encrypted Broadcast Video

Feature Name	Releases	Feature Information
RPHY Pre-encrypted Broadcast Video	Cisco 1x2 / Compact Shelf RPD Software 3.1	This feature was integrated into Cisco Remote PHY Device.



CHAPTER 29

Remote PHY BFS QAM Configuration

This document provides information on how to configure Cisco cBR-8 as a Broadcast File System (BFS) Quadrature Amplitude Modulation (QAM), which interfaces with Explorer Controller (EC) versions 7.x and 8.x.

Finding Feature Information

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

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

- [Hardware Compatibility Matrix for Cisco Remote PHY Device, on page 211](#)
- [Information About BFS QAM Support, on page 212](#)
- [How to Configure BFS QAM for EC 7.x, on page 212](#)
- [How to Configure BFS QAM for RPD, on page 215](#)
- [How to Configure BFS QAM for EC 8.x, on page 216](#)
- [Configuration Example for BFS QAM Configuration, on page 218](#)
- [Feature Information for BFS QAM Configuration, on page 221](#)

Hardware Compatibility Matrix for Cisco Remote PHY Device



Note Unless otherwise specified, the hardware components introduced in a given Cisco Remote PHY Device Software Release are supported in all subsequent releases.

Table 57: Hardware Compatibility Matrix for the Cisco Remote PHY Device

Cisco HFC Platform	Remote PHY Device
Cisco GS7000 Super High Output Node	Cisco 1x2 / Compact Shelf RPD Software 2.1 and Later Releases

Cisco HFC Platform	Remote PHY Device
Cisco GS7000 Super High Output Intelligent Node (iNode)	Cisco 1x2 / Compact Shelf RPD Software 4.1 and Later Releases Cisco Intelligent Remote PHY Device 1x2 <ul style="list-style-type: none"> • PID—iRPD-1X2= • PID—iRPD-1X2-PKEY=



Note The -PKEY suffix in the PID indicates units that enable the SCTE-55-2 Out-of-Band protocol support.

Information About BFS QAM Support

The BFS provides a mechanism for a standardized downloading of applications, games, images, and other data formats required by the applications. The BFS QAM enables the router to transfer the broadcast data from an EC to the target platform such as a set-top unit. All forms of BFS data from EC flows as IP multicast, except the CVT carousel, which is through the GQI insert packets.

The BFS QAM configuration on the Cisco cBR-8 router varies based on the version of EC, which interfaces with the router.

- For EC 7.x-Model a GQI-based LED as BFS QAM. One for each LC on Cisco cBR-8.

For Remote PHY-A single GQI-based LED as BFS QAM for the entire Cisco cBR-8 chassis, as the Cisco cBR-8 can support DEPI multicast for all Remote PHY devices (RPD).

For EC 8.x-EC 8.x multicasts CVT carousel data in addition to GQI insert packets, but only in the presence of GQAM configured as BFS QAM. Hence, in this setup, a single table-based LED, modeled as BFS QAM, for each Cisco cBR-8 chassis is sufficient. Using cross LC replication, this BFS data can be replicated to other LCs on the Cisco cBR.

How to Configure BFS QAM for EC 7.x

This configuration applies to Cisco cBR-8 routers running Converged Cable Access Platform (CCAP) with Ethernet input and RF output.

If Cisco cBR-8 interacts with EC 7.x, configure an LED on each line card. Use the following procedure to configure BFS QAM on Cisco cBR router.

- Configure an LED with GQI protocol on each line card.
- On EC 7.x, provision BFS QAM.
- Manually create sessions on EC 7.x.
- Generate the QAM, based on GQI model.
- Generate a new source definition and use the new QAM as a target using the same PIDs.

- Ensure that everything is set up on the EC to match the Cisco cBR-8 LED configuration.

This section contains the following:

Mapping Cisco cBR-8 as a GQI QAM

On the EC 7.x, configure BFS sessions on the registered BFS QAM by using one of the following:

- Proprietary Remote Procedure Call (RPC) (with GQAM)
- GQI (with RFGW-1)

You can use a standard GQI model where the sessions will be generated on the individual line card on a single LED per line card basis. Individual BFS sessions are added to the LEDs at the Source Definition for all in-band BFS sources. Sessions must be unique in numbering and QAM selection, although all other settings must be duplicates of the original settings.

Creating VCG with One QAM Channel

The following example shows how to create a video virtual carrier group (VCG) with one QAM channel, which can carry the BFS data.

```
enable
configure terminal
cable video

virtual-carrier-group (name) id (id)
  service-type broadcast
  rf-channel (rf-channel number 1) tsid (id) output-port-number (port number 1)
virtual-carrier-group (name 2) id (id 2)
  service-type broadcast
  rf-channel (rf-channel number 1) tsid (id 2) output-port-number (port number 1)
```

Creating SDG for BFS Sessions on Cisco cBR

The following example shows how to create Service Distribution Group (SDG) for BFS sessions and map this to as many RF ports as required.

```
enable
configure terminal
cable video

service-distribution-group sdg_bdcast id 20
  rf-port integrated-cable 8/0/0
  rf-port integrated-cable 8/0/1
  rf-port integrated-cable 8/0/2
  rf-port integrated-cable 8/0/3
  rf-port integrated-cable 8/0/4
  rf-port integrated-cable 8/0/5
  rf-port integrated-cable 8/0/6
  rf-port integrated-cable 8/0/7
service-distribution-group sdg_bdcast-9 id 21
  rf-port integrated-cable 9/0/0
  rf-port integrated-cable 9/0/1
  rf-port integrated-cable 9/0/2
  rf-port integrated-cable 9/0/3
```

```

rf-port integrated-cable 9/0/4
rf-port integrated-cable 9/0/5
rf-port integrated-cable 9/0/6
rf-port integrated-cable 9/0/7

```

Create VCG for BFS

The following example shows how to create VCG for BFS.

```

configure terminal
cable video

virtual-carrier-group vcg_bdcast id 20
  service-type broadcast
  rf-channel 76 tsid 1011 output-port-number 1
virtual-carrier-group vcg_bdcast-9 id 21
  service-type broadcast
  rf-channel 76 tsid 1012 output-port-number 1

vcg vcg_bdcast sdg sdg_bdcast
vcg vcg_bdcast-9 sdg sdg_bdcast-9

bind-vcg
vcg vcg_bdcast sdg sdg_bdcast
vcg vcg_bdcast-9 sdg sdg_bdcast-9

```

Creating Logical Edge Device

The following example shows how to create an LED.



Note Ensure that the LED settings are the same as GQI QAM settings on the EC. For more details, see [Creating GQI QAM for BFS on EC 7.x](#)

```

enable
configure terminal
cable video

logical-edge-device led_BFS id 20
  protocol gqi
  mgmt-ip 192.0.2.1
  mac-address <MAC address>
  server 198.51.100.1
  keepalive retry 3 interval 10
  reset interval 8
  virtual-edge-input-ip 203.0.113.1 input-port-number 1
  vcg vcg_bdcast
  active
logical-edge-device led_BFS-9 id 21
  protocol gqi
  mgmt-ip 192.0.2.1
  mac-address <MAC address>
  server 198.51.100.1
  keepalive retry 3 interval 10

```

```
reset interval 8
virtual-edge-input-ip 203.0.113.1 input-port-number 1
vcg vcg_bdcast-9
active
```

Creating GQI QAM for BFS on EC 7.x

Prerequisites

- To create the GQI QAM on the EC, enable packet insertion in the QAM Model.
- You can duplicate the standard RFGW model to ensure that no interference occurs with the current operations.
- The router must have a GQI QAM per LED.
- The individual QAM must be BFS-capable.

Procedure

Use the following procedure to create GQI QAM for BFS.

1. Choose EC > GQI Based QAM Model List > Edit GQI Based QAM.
2. (Optional) Select the BFS Capable checkbox.
3. Choose RF Carriers from the left pane.
4. Ensure that the Carriers and Ethernet Port values are the same as those on the LEDs.

You can create the sessions for each BFS source by generating a Multicast Through GQI Based QAM session through each BFS source's Source Definition.

How to Configure BFS QAM for RPD

This configuration applies to Cisco cBR-8 routers running CCAP with Ethernet input and Ethernet output.

The configuration procedure for RPD is similar to the configuration on Cisco cBR-8 routers with EC 7.x. However, only one LED is needed for BFS QAM configuration.

You can use the sessions configured on the LED on every RPD by defining an Auxiliary Core on each RPD as needed for BFS distribution.

Creating SDG for BFS Sessions for RPD

The following example shows how to create SDG for BFS sessions on RPDs.

```
service-distribution-group sdg_bdcast id 20
  rpd downstream-cable 2/0/30

virtual-carrier-group vcg_bdcast id 20
  service-type broadcast
  rf-channel 79 tsid 1013 output-port-number 1
```

Creating LED for RPD

The following example shows how to create an LED.

```
logical-edge-device led_BFS id 20
  protocol gqi
    mgmt-ip 192.0.2.1
    mac-address <MAC address>
    server 198.51.100.1
    keepalive retry 3 interval 10
    reset interval 8
    virtual-edge-input-ip 203.0.113.1 input-port-number 1
    vcg vcg_bdcast
```

Defining Cable RPD

The RPD definition must include the RPD defined in the BFS SDG for every RPD to which you want to distribute BFS data: The following example shows how to define RPD.

```
cable rpd RPD07
  identifier xxxx.xxxx.xxxx
  core-interface Te2/1/4
  principal
    rpd-ds 0 downstream-cable 2/0/16 profile 11
    rpd-us 0 upstream-cable 2/0/12 profile 1
  core-interface Te2/1/6
    rpd-ds 0 downstream-cable 2/0/30 profile 10
  r-dti 3
  rpd-event profile 0
  rpd-55d1-us-event profile 0
!
cable rpd RPD08
  identifier xxxx.xxxx.xxxx
  core-interface Te2/1/4
  principal
    rpd-ds 0 downstream-cable 2/0/17 profile 11
    rpd-us 0 upstream-cable 2/0/14 profile 1
  core-interface Te2/1/6
    rpd-ds 0 downstream-cable 2/0/30 profile 10
  r-dti 3
  rpd-event profile 0
  rpd-55d1-us-event profile 0
```

For information on how to create GQI QAM on the EC, see [Creating GQI QAM for BFS](#).

How to Configure BFS QAM for EC 8.x

When Cisco cBR-8 interfaces with EC 8.x, all sessions on the router are configured as multicast and perform a multicast join.

The Cisco cBR routers are not directly mapped on the EC. Hence, this BFS QAM configuration requests and processes the multicast BFS sessions that are setup on the actual BFS QAM. If the Cisco cBR-8 routers have to process these sessions, you must set up table-based multicast sessions, which are similar to the ones available on the BFS QAM.

Configure QAM replication group (QRG), spanning across line cards (LC) to replicate these BFS sessions on every RF port (if each RF port is a service group) of every LC.

To replicate across line cards, you must configure table-based sessions. You can perform cross-line-card-replication only through table-based sessions.

Use the following procedure to configure BFS QAM on Cisco eBR router for EC 8.x.

1. Create a VCG with one QAM channel for carrying this BFS data.
2. Within the same VCG, allocate a few more QAM channels for MPTS pass-through sessions.
3. Create VCG for VoD QAM channels.
4. Create VCG for SDV QAM channels.

Creating VCG for VoD QAM Channels

The following example shows how to create VCG for VoD QAM channels.

```
enable
configure terminal
cable video

virtual-carrier-group vcg_VoD
service-type narrowcast
rf-channel 1-32 tsid 2-33 output-port 2-33
```

Creating VCG for SDV QAM Channels

The following example shows how to create VCG for SDV QAM channels.

```
enable
configure terminal
cable video

virtual-carrier-group vcg_SDV
service-type narrowcast
rf-channel 33-48 tsid 34-49 output-port 34-49
```

Creating SDG

The following procedures are applicable when you create an SDG.

1. Create SDG for broadcast sessions and map this to as many RF ports as required, depending on the Service Groups which need this broadcast data.
2. Create separate SDG for VoD.
3. Create separate SDG for SDV, which probably contains replication.

```
enable
configure terminal
cable video

service-distribution-group sdg_bdcast
```

```

rf-port integrated-cable 1/0/0
rf-port integrated-cable 1/0/1
rf-port integrated-cable 2/0/0
rf-port integrated-cable 2/0/1
rf-port integrated-cable 3/0/0
rf-port integrated-cable 3/0/1

service-distribution-group sdg_VoD
rf-port integrated-cable 1/0/0

service-distribution-group sdg_SDV
rf-port integrated-cable 1/0/0
rf-port integrated-cable 1/0/1

bind-vcg
vcg vcg_BFS sdg sdg_BFS
vcg vcg_VoD1 sdg sdg_VoD
vcg vcg_SDV sdg sdg_SDV

```

Creating LEDs

The following procedures are applicable for creating LEDs.

1. Create a table based LED for broadcast carrying BFS and MPTS pass-through sessions.
2. Create separate LEDs for VoD and SDV.

```

logical-edge-device led_BFS id 1
  protocol table-based
    virtual-edge-input-ip 203.0.113.1 input-port-number 1
    vcg vcg_bdcast
    active
  table-based
    vcg vcg_bdcast
    rf-channel 0
      session BFS group 203.0.113.4 start-udp-port 49152 num-sessions-per-qam 1
    processing-type remap start-program 20 bit-rate 300000 jitter 100 vbr
      rf-channel 48 session MPTS_passthru group 203.0.113.5 start-udp-port 49152
    num-sessions-per-qam 1 processing-type passthru jitter 100 vbr
      rf-channel 49 session MPTS_passthru group 203.0.113.6 start-udp-port 49152
    num-sessions-per-qam 1 processing-type passthru jitter 100 vbr

logical-edge-device led_VoD id 2
  protocol gqi
    virtual-edge-input-ip 203.0.113.1 input-port-number 1
    vcg vcg_VoD
    active

```

Configuration Example for BFS QAM Configuration

This section provides examples for BFS QAM support.

Example: BFS QAM Configuration on Cisco cBR for EC 7.x

The following example shows the BFS QAM configuration for EC 7.x.

```

virtual-carrier-group vcg_bdcast id 20
  service-type broadcast
  rf-channel 76 tsid 1011 output-port-number 1
virtual-carrier-group vcg_bdcast-9 id 21
  service-type broadcast
  rf-channel 76 tsid 1012 output-port-number 1

service-distribution-group sdg_bdcast id 20
  rf-port integrated-cable 8/0/0
  rf-port integrated-cable 8/0/1
  rf-port integrated-cable 8/0/2
  rf-port integrated-cable 8/0/3
  rf-port integrated-cable 8/0/4
  rf-port integrated-cable 8/0/5
  rf-port integrated-cable 8/0/6
  rf-port integrated-cable 8/0/7
service-distribution-group sdg_bdcast-9 id 21
  rf-port integrated-cable 9/0/0
  rf-port integrated-cable 9/0/1
  rf-port integrated-cable 9/0/2
  rf-port integrated-cable 9/0/3
  rf-port integrated-cable 9/0/4
  rf-port integrated-cable 9/0/5
  rf-port integrated-cable 9/0/6
  rf-port integrated-cable 9/0/7

virtual-carrier-group vcg_bdcast id 20
  service-type broadcast
  rf-channel 76 tsid 1011 output-port-number 1
virtual-carrier-group vcg_bdcast-9 id 21
  service-type broadcast
  rf-channel 76 tsid 1012 output-port-number 1

vcg vcg_bdcast sdg sdg_bdcast
vcg vcg_bdcast-9 sdg sdg_bdcast-9

bind-vcg
vcg vcg_bdcast sdg sdg_bdcast
vcg vcg_bdcast-9 sdg sdg_bdcast-9

logical-edge-device led_BFS id 20
  protocol gqi
  mgmt-ip 192.0.2.1
  mac-address <MAC address>
  server 198.51.100.1
  keepalive retry 3 interval 10
  reset interval 8
  virtual-edge-input-ip 203.0.113.1 input-port-number 1
  vcg vcg_bdcast
  active
logical-edge-device led_BFS-9 id 21
  protocol gqi
  mgmt-ip 192.0.2.1
  mac-address <MAC address>
  server 198.51.100.1
  keepalive retry 3 interval 10
  reset interval 8
  virtual-edge-input-ip 203.0.113.1 input-port-number 1
  vcg vcg_bdcast-9

```

```
active
```

Example: BFS QAM Configuration on RPD

The following example shows the BFS QAM configuration on RPD.

```
service-distribution-group sdg_bdcast id 20
  rpd downstream-cable 2/0/30

virtual-carrier-group vcg_bdcast id 20
  service-type broadcast
  rf-channel 79 tsid 1013 output-port-number 1

logical-edge-device led_BFS id 20
  protocol gqi
  mgmt-ip 192.0.2.1
  mac-address <MAC address>
  server 198.51.100.1
  keepalive retry 3 interval 10
  reset interval 8
  virtual-edge-input-ip 203.0.113.1 input-port-number 1
  vcg vcg_bdcast

cable rpd RPD07
  identifier xxxx.xxxx.xxxx
  core-interface Te2/1/4
  principal
  rpd-ds 0 downstream-cable 2/0/16 profile 11
  rpd-us 0 upstream-cable 2/0/12 profile 1
  core-interface Te2/1/6
  rpd-ds 0 downstream-cable 2/0/30 profile 10
  r-dti 3
  rpd-event profile 0
  rpd-55d1-us-event profile 0
!
cable rpd RPD08
  identifier xxxx.xxxx.xxxx
  core-interface Te2/1/4
  principal
  rpd-ds 0 downstream-cable 2/0/17 profile 11
  rpd-us 0 upstream-cable 2/0/14 profile 1
  core-interface Te2/1/6
  rpd-ds 0 downstream-cable 2/0/30 profile 10
  r-dti 3
  rpd-event profile 0
  rpd-55d1-us-event profile 0
```

Example: BFS QAM Configuration on Cisco cBR for EC 8.x

The following example shows the BFS QAM configuration for EC 8.x.

```
virtual-carrier-group vcg_bdcast
  service-type broadcast
  rf-channel 0 tsid 1 out 1
  rf-channel 49-63 tsid 50-64 output-port 50-64

virtual-carrier-group vcg_VoD
  service-type narrowcast
  rf-channel 1-32 tsid 2-33 output-port 2-33
```



```

virtual-carrier-group vcg_SDV
service-type narrowcast
rf-channel 33-48 tsid 34-49 output-port 34-49

service-distribution-group sdg_bdcast
rf-port integrated-cable 1/0/0
rf-port integrated-cable 1/0/1
rf-port integrated-cable 2/0/0
rf-port integrated-cable 2/0/1
rf-port integrated-cable 3/0/0
rf-port integrated-cable 3/0/1

service-distribution-group sdg_VoD
rf-port integrated-cable 1/0/0

service-distribution-group sdg_SDV
rf-port integrated-cable 1/0/0
rf-port integrated-cable 1/0/1

bind-vcg
vcg vcg_BFS sdg sdg_BFS
vcg vcg_VoD1 sdg sdg_VoD
vcg vcg_SDV sdg sdg_SDV

logical-edge-device led_BFS id 1
  protocol table-based
    virtual-edge-input-ip 203.0.113.1 input-port-number 1
    vcg vcg_bdcast
    active
  table-based
    vcg vcg_bdcast
    rf-channel 0
      session BFS group 203.0.113.4 start-udp-port 49152 num-sessions-per-qam 1
    processing-type remap start-program 20 bit-rate 300000 jitter 100 vbr
    rf-channel 48
      session MPTS_passthru group 203.0.113.5 start-udp-port 49152 num-sessions-per-qam 1
    processing-type passthru jitter 100 vbr
    rf-channel 49
      session MPTS_passthru group 203.0.113.6 start-udp-port 49152 num-sessions-per-qam 1
    processing-type passthru jitter 100 vbr

logical-edge-device led_VoD id 2
  protocol gqi
    virtual-edge-input-ip 203.0.113.1 input-port-number 1
    vcg vcg_VoD
    active

```

Feature Information for BFS QAM Configuration

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



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

Table 58: Feature Information for BFS QAM Configuration

Feature Name	Releases	Feature Information
BFS QAM Configuration	Cisco 1x2 / Compact Shelf RPD Software 3.1	This feature was integrated into Cisco Remote PHY Device.



CHAPTER 30

Remote PHY Switched Digital Video

This document provides information on how to configure Switched Digital Video for Cisco Remote PHY Device.

Finding Feature Information

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

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

- [Switched Digital Video Services, on page 223](#)
- [Information About Switched Digital Video, on page 225](#)
- [How to Configure the Switched Digital Video Services, on page 226](#)
- [Configuration Examples for Switched Digital Video, on page 230](#)
- [Feature Information for Switched Digital Video, on page 234](#)

Switched Digital Video Services

The Switched Digital Video (SDV) services are supported for the MPEG video subsystem on the Cisco Remote PHY Device. It consists of Multicast IP Packet based video streams that are managed as "Video Sessions". The Cisco Remote PHY Device supports both Any Source Multicast (ASM) and Source Specific Multicast (SSM) sessions.

- For ASM, the input is identified by the group IP address.
- For SSM, the input is identified by the source and group IP address pair.

In both cases, the UDP ports are ignored. Both ASM and SSM can co-exist but cannot overlap in a group IP address. Hence, for a group IP address, either a single ASM, or one or more SSM can be used.

Session Cloning

Session cloning refers to the ability of forwarding an input to multiple output QAM channels. Only multicast sessions can be cloned. The output QAM channels are located on the same or different line cards. However, an input cannot be cloned on the same QAM channel. Cloning is available on session-based GQIv2 or Table-based sessions. It is applicable to re-mapped, pass-through, and data piping sessions. All cloned sessions must have the same processing type, bitrate and jitter value. For re-mapped sessions, each output copy will have a different output program number.

Redundant Multicast Sources

The redundant multicast sources feature supports up to four SSM/ASM multicast address pairs per video session. However, only multicast traffic from one source is forwarded to the output QAMs. When the active source fails, another source is chosen automatically. Multicast sources must be unique within a redundant group and cannot overlap across redundant groups.

The order of the sources is critical when multicast sessions are configured via GQI or VSRM. For a given group IP address, the source IP addresses must be specified in the same order.

For example: The group IP address 232.1.2.3 used with two sessions must have the source IP addresses specified in the same order.

Session A configured with group IP 232.1.2.3 source 174.2.3.4 source2 174.4.5.6 source3 174.7.8.9 and session B or any session created after session A configured using group IP 232.1.2.3, must have the source IP addresses in this same order as specified for session A. That is, source 174.2.3.4 source2 174.4.5.6 source3 174.7.8.9.

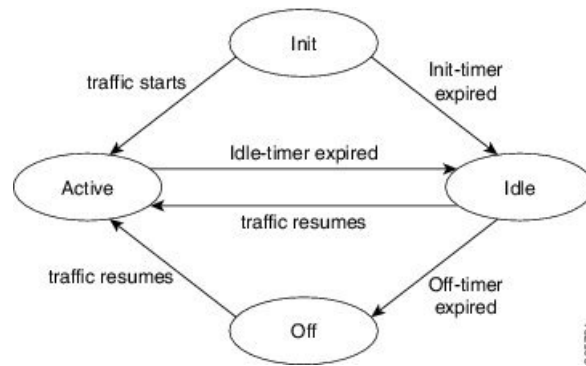
This ensures that all sessions switch to the same source IP address when a source switch occurs. Additionally, sessions configured via GQI have up to three sources available for redundancy, whereas multicast labels configured for table-based sessions have up to four sources available for redundancy.

Multicast labels must use unique groups and S/G pairs. These pairs cannot be used by other multicast labels or by multicast sessions that use S/G pairs. For example, when one multicast session uses {[S1, G], [S2, G] and [S3, G]}, another session cannot use {[S1, G], [S4, G]}.

Multicast source change is based on the session state; INIT, IDLE, ACTIVE or OFF. A session configured for the first time is in INIT state and stays in this state for a brief time. If traffic starts before the INIT timer expires, it moves to the ACTIVE state, otherwise to the IDLE state.

When traffic starts, the session remains in ACTIVE state as long as traffic continues to flow. When traffic stops for a time longer than the IDLE timer, the session moves to IDLE state. During IDLE state, PAT and PMT of the session is retained as the output. If traffic resumes in this state, the session moves to ACTIVE state again with all its previous PSI and remapping information unaltered.

In IDLE state, if traffic does not start or resume before the OFF timer expires, the session transitions to OFF state. When traffic resumes for a session in OFF state, it is treated as a new session.



Sessions that transition from ACTIVE to IDLE have higher priority and will be moved to the backup source than those that were newly created and have changed from INIT to IDLE.

Benefits of Switched Digital Video

Switched Digital Video provides the following benefits:

- Saves space, maintenance and cost.
- Allows customers to oversubscribe bandwidth.

Prerequisites for Switched Digital Video

- To access multicast capability, configure multicast routing.
- To switch sources for table-based sessions, configure at least two sources for a multicast label and then associate with the desired session.

Restrictions for Switched Digital Video

- While creating a multicast label, up to four sources can be associated with one group IP address.
- Labels are used with table-based video sessions only.
- Sessions created with GQI Tools do not use labels. However, they can have up to three sources associated with one group IP address.

Information About Switched Digital Video

QAM Sharing

Unicast and multicast video sessions can co-exist on the same QAM channel for VOD, SDV or Gaming sessions. QAM sharing requires a common Edge Resource Manager to avoid oversubscription of QAM resources between services.



Note QAM sharing with MPTS pass-thru sessions is not supported.

QAM Replication

Multicast sessions can be replicated from one port to other ports on the same line card and/or across line cards.

The difference between a cloned session and replicated sessions is:

- Cloned sessions are initiated by a user on session creation. Each session has a unique session id and may have different output configuration.
- Replicated sessions have the same output configuration attributes. For sessions that are replicated across line cards, session on each line card will have its own unique session id.

MPTS Pass-through Session

Switched digital video (SDV) sessions are typically multicast SPTS remap type. The Cisco Remote PHY Device also supports multicast MPTS pass-through and data-piping session types.

The MPTS session is assumed to have no collision in the PID space and program number space with other sessions that already exist within a QAM. Hence, SPTS remap and MPTS pass-through sessions cannot co-exist on the same QAM. Otherwise, there might be conflict when the PID and program numbers in the MPTS and SPTS remuxing are not unique on the output QAM channel.

For a pass-through session:

- The PAT is snooped and regenerated with the correct TSID.
- The PMT and other program data are not changed.
- PID remapping is not performed.
- Input NULL packets are dropped.
- Oversubscription results in random TP dropping, and all ghost PIDs are preserved in the output.

How to Configure the Switched Digital Video Services

Configuring Multicast Routing

You can enable IP Multicast Distributed Switching (MDS) to provide distributed switching of multicast packets received at the line cards.

```
enable
configure terminal
ip multicast-routing distributed
ip pim ssm range all-multicasts
ip pim rp-address ip-address
```

```

interface type number
  ip pim sparse-dense-mode
  ip igmp version 3
cable video
  multicast-uplink interface-name access-list access-list-name

```

When more than one physical or logical interfaces are used for reverse path forwarding (RPF) lookup, use loopback interface in **multicast-uplink** command and make sure that the loopback interface is routable/reachable on your network. Loopback interface of the cBR-8 can be enabled with **ip pim sparse-mode** command and it is reachable to multicast source or reverse path.

Below is an example of configuration:

```

Router> enable
Router# configure terminal
Router(config)# cable video
Router(config-video)# multicast-uplink 'Loopback0' access-list "acl_name1" access-list-global
  "acl_name2" rp "rp-address"

Router(config)# interface Loopback0
Router(config-if)# ip address <ipaddress> <mask>
Router(config-if)# ip pim sparse-mode
Router(config-if)# end

Router(config)# ip access-list standard acl_name2
Router(config-std-nacl)# 10 permit 232.0.0.0 0.255.255.255
Router(config-std-nacl)#20 permit 227.0.0.0 0.255.255.255
Router(config-std-nacl)#30 permit 228.0.0.0 0.255.255.255
Router(config-std-nacl)#40 permit 231.0.0.0 0.255.255.255
Router(config-std-nacl)#50 permit 230.0.0.0 0.255.255.255

Router(config)# ip access-list standard acl_name1
Router(config-std-nacl)#10 permit 232.0.0.0 0.255.255.255
Router(config-std-nacl)#20 permit 231.0.0.0 0.255.255.255

```

`acl_name1` is a named-access-list to provisioned by user which provides multicast prefix belong to SSM range. Default is 232.*.*.*

`acl_name2` is a named-access-list to provisioned by user which provides multicast prefix belong to both SSM/ASM range.

`rp-address` is the actual IP address of the RP if ASM used.

Configuring Multicast Label

The Cisco Remote PHY Device supports up to four multicast address pairs per multicast session for backup purpose. To specify additional sources for a multicast session for table-based, a label needs to be configured and attached to the session configuration. A maximum of 2000 multicast labels can be created but only 2048 multicast addresses can be active at a time.

Multicast label is used for table-based session configuration when more than one multicast source [S, G] is used as backup for the sessions. A multicast label can only be created or deleted; it cannot be modified. The multicast label cannot be deleted before the sessions using it are removed.

Groups used by multicast labels must be unique like the multicast S/G pairs. However, sources may be used by more than one label as long as the group is unique. A maximum of 4 multicast sources is allowed in one label. If the label is used in multiple sessions, the sessions are considered as cloned sessions.

```

enable
configure terminal
  cable video
    table-based
      multicast-label label group group-ip source source-ip source2 source-ip source3
source-ip source4 source-ip

```

Configuring Multicast Table-based Sessions

Similar to table-based unicast session configuration, sessions can be configured as individual sessions under each QAM carrier that is assigned to a table-based LED.

A multicast session can be configured with a single input multicast input source or multiple input sources for backup purpose. For multiple backup sources, a label is required to be associated with the session configuration. Same label can be applied to multiple sessions on different QAM channel. These sessions are considered as cloned sessions.

For session cloning on multiple QAMs within the same line card, only one copy of the traffic is forwarded to the line card. The line card replicates the input packets and forwards them to multiple QAMs. Each cloned copy of a remapped session will have the same or different output program number.

```

enable
configure terminal
  cable video
    table-based
      vcg vcg-name
      rf-channel channel
      session session-name group group-ip source source-ip processing-type {remap
| passthru | data} start-program program-num [bit-rate bit-rate-number] [jitter
jitter-number] [cbr | vbr]

```

Configuring Source Switching

Source switching happens automatically when the current source goes down. If more than one source IP is configured, the software will automatically switch to the next valid source IP, if it is available. However, to force switch from one valid source to another valid source, use the following commands:

```

Router(config)# cable video source-switch from-group group-ip from-source
source-ip

```

or

```

Router(config)# cable video source-switch to-group group-ip to-source source-ip

```

Verifying Switched Digital Video Configuration

```

Router#show cable video session logical-edge-device id 2
Total Sessions = 4

```


Session Input Id State	Output Output Port State	Streaming Input Type Bitrate	Output Output Type Bitrate	Session Encrypt Type	Session Encrypt Ucast Dest Status	Source IP/Mcast IP (S,G)	Session IP (S,G) Name	UDP Port	Output Program
2097152	142 ON 0	Remap 0	SSM CLEAR	175.2.5.6,232.5.6.7 -	SESS_PME2.1.7.338	0	1	OFF	
2097153 INIT	163 ON 0	Remap 0	SSM CLEAR	175.6.1.13,232.2.1.6 -	SESS_PME3.1.7.497	0	2		
2097154	184 ON 0	Passthru 0	SSM CLEAR	175.2.6.7,232.5.6.15 -	SESS_PME4.1.7.656	0	-	OFF	
2097155	230 ON 0	Data-Piping 0	SSM CLEAR	175.7.2.2,232.2.6.7 -	SESS_PME6.1.7.978	0	-	OFF	

Router#show cable video session logical-edge-device id 2 session-id 2097152

Session Name : SESS_PME2.1.7.338
 Session Id: : 2097152
 Creation Time: : Fri Jun 24 16:30:45 2016

Output Port : 142
 TSID : 142
 ONID : 0
 Number of Sources : 1
 Source IP : 175.2.5.6
 Group IP : 232.5.6.7
 UDP Port : 0
 Config Bitrate : not specified
 Jitter : 100 ms
 Processing Type : Remap
 Stream Rate : VBR
 Program Number : 1
 Idle Timeout : 2000 msec
 Init Timeout : 2000 msec
 Off Timeout : 60 sec
 Encryption Type : CLEAR
 Encryption Status : -

Input Session Stats:

=====
 State: OFF, Uptime: 0 days 00:26:35
 IP Packets: In 0, RTP 0, Drop 0
 TP Packets: In 0, PCR 0, PSI 0, Null 0
 Unreference 0, Discontinuity 0
 Errors: Sync loss 0, CC error 0, PCR Jump 0,
 Underflow 0, Overflow 0, Block 0
 Bitrate: Measured 0 bps, PCR 0 bps

Output Session Stats:

=====
 State: ON, Uptime: 0 days 00:26:35
 TP Packets: In 0, PCR 0, PSI 0,
 Drop 0, Forward 0, Insert 0
 Errors: Info Overrun 0, Info Error 0, Block 0, Overdue 0,
 Invalid Rate 0, Underflow 0, Overflow 0
 Bitrate: Measured 0 bps

Troubleshooting Switched Digital Video Configuration

Problem	Possible Causes	Recommended Solution
%ERROR: Duplicate multicast source 175.2.5.6 group 232.5.6.7 not allowed for use in label groupDuplicate.	Group and Source are already used in an existing label.	Assign unique group and source IPs across multicast labels.
%ERROR: Duplicate multicast source 178.3.3.3 group 232.222.222.222 not allowed within label DuplicateSourceHere.	Source has been repeated within a label.	Assign unique source IP within a multicast label.
%ERROR: Duplicate multicast source 175.2.5.6 group 232.5.6.7 not allowed for use in this session.	Session has been created with a duplicate group IP. This group IP has been used in an existing multicast label.	Create the session with a unique group IP.
%ERROR Only one multicast session can be created per multicast session command; rf-channel range values, such as rf-channel 20-30, not allowed.	Session has been created on a range of RF channels.	RF channel range is not allowed. Create the session on an RF channel.

Configuration Examples for Switched Digital Video

Example 1: Table-based Multicast Session Configuration

```

enable
configure terminal
ip pim rp-address 9.1.1.1
ip pim ssm range all-multicasts
ip access-list standard all-multicasts
permit 233.0.0.0 0.255.255.255
permit 234.0.0.0 0.255.255.255
permit 235.0.0.0 0.255.255.255
permit 236.0.0.0 0.255.255.255
permit 237.0.0.0 0.255.255.255
permit 238.0.0.0 0.255.255.255
permit 232.0.0.0 0.255.255.255
permit 224.0.0.0 0.255.255.255
permit 239.0.0.0 0.255.255.255
interface TenGigabitEthernet4/1/2
ip address 2.33.1.1 255.255.255.252
ip pim sparse-mode
ip igmp version 3
ip ospf 64512 area 9
load-interval 30
cable video
multicast-uplink TenGigabitEthernet4/1/2 access-list all-multicasts
service-distribution-group sdg-1 id 1
rf-port downstream-cable 7/0/0

```

```

virtual-carrier-group vcg-1 id 1
  service-type narrowcast
  rf-channel 0-55 tsid 1-56 output-port-number 1-56
bind-vcg
  vcg vcg-1 sdg sdg-1
logical-edge-device led_multicast id 1
  protocol table-based
    virtual-edge-input-ip 174.102.1.1 input-port-number 1
    vcg vcg-1
    active
  table-based
    multicast-label labell group 232.2.1.1 source 175.2.2.2
    vcg vcg-1
    rf-channel 0
      session mcast1 multicast-label labell processing-type remap start-program 1 jitter
100 vbr
      session mcast2 group 236.0.1.1 source 175.10.5.2 processing-type passthru jitter
100 cbr

```

Example 2: Table-based Configuration for Replicated Multicast Pass-through Sessions

Below is a table-based configuration for multicast pass-through sessions replicated to all QAM ports on the same line card.

```

enable
configure terminal
cable video
multicast-uplink TenGigabitEthernet4/1/2 access-list all-multicasts
service-distribution-group sdg1 id 1
  rf-port downstream-cable 7/0/0
  rf-port downstream-cable 7/0/1
  rf-port downstream-cable 7/0/2
  rf-port downstream-cable 7/0/3
  rf-port downstream-cable 7/0/4
  rf-port downstream-cable 7/0/5
  rf-port downstream-cable 7/0/6
  rf-port downstream-cable 7/0/7
virtual-carrier-group vcg1 id 1
  rf-channel 0-95 tsid 0-95 output-port-number 1-96
bind-vcg
  vcg vcg1 sdg sdg1
logical-edge-device led1 id 1
  protocol table-based
    virtual-edge-input-ip 174.102.1.1 input-port-number 1
    vcg vcg1
    active
  table-based
    multicast-label mlabell group 236.0.1.1 source 175.10.5.2 source2 175.10.6.20 source3
175.10.7.2
    vcg vcg1
    rf-channel 0
      session mcast1 multicast-label mlabell processing-type passthru vbr
    rf-channel 5
      session mcast2 group 237.0.1.1 source 175.10.6.2 processing-type passthru vbr

```

Example 3: QAM Sharing Configuration

Below is an example of how to create a PMT encrypted table-based session for both VOD and SDV on the same QAM channel on 7/0/0 RF port.

```

cable video
 multicast-uplink TenGigabitEthernet4/1/2 access-list all-multicasts
 mgmt-intf VirtualPortGroup 0
 encryption
  linecard 7/0 ca-system pme scrambler dvs042
  pme vodsid 111
  pme cem 1.200.1.163 5000
  pme mgmt-ip 1.33.2.6
 service-distribution-group sdg1 id 1
  rf-port downstream-cable 7/0/0
 virtual-carrier-group vcg1 id 1
  virtual-edge-input-ip 174.102.1.1 input-port-number 1
  encrypt
  service-type narrowcast
  rf-channel 20-34 tsid 20-34 output-port-number 20-34
 bind-vcg
  vcg vcg1 sdg sdg1
 logical-edge-device led1 id 1
  protocol table-based
  vcg vcg1
  active
 table-based
  multicast-label mlabell group 236.0.1.1 source 175.10.5.2 source2 175.10.6.2 source3
 175.10.7.2
  vcg vcg1
  rf-channel 20
    session VOD input-port 1 start-udp-port 49152 processing-type remap start-program
 1 jitter 100 vbr
    session SDV multicast-label mlabell processing-type remap start-program 1000 jitter
 100 vbr
  !

```

Example 4: QAM Replication Configuration

Below is an example of how to configure multicast sessions with four backup sources and replicated on multiple line cards and multiple RF ports within the same line card.

```

cable video
 multicast-uplink TenGigabitEthernet4/1/2 access-list all-multicasts
 service-distribution-group sdg-1 id 1
  rf-port downstream-cable 7/0/0
  rf-port downstream-cable 7/0/1
  rf-port downstream-cable 8/0/0
  rf-port downstream-cable 8/0/1
 virtual-carrier-group vcg-1 id 1
  service-type broadcast
  rf-channel 0-55 tsid 1-56 output-port-number 1-56
 bind-vcg
  vcg vcg-1 sdg sdg-1
 logical-edge-device led_multicast id 1
  protocol table-based
  virtual-edge-input-ip 174.102.1.1 input-port-number 1
  vcg vcg-1
  active
 table-based
  multicast-label labell group 232.2.1.1 source 175.2.2.2 source2 175.2.3.2 source3
 175.2.4.2 source4 175.5.1.12
  vcg vcg-1
  rf-channel 0
    session mcast1 multicast-label labell processing-type remap start-program 1 jitter

```

```
100 vbr
```

Example 5: SSM Session Configuration

The following examples show how to configure SSM sessions on a range of QAM channels with three multicast sources.

```
table-based
  multicast-label label110_1 group 232.2.1.35 source 175.2.2.2 source2 175.6.1.12 source3
  175.2.9.2
  multicast-label label103_1 group 232.2.1.30 source 175.2.2.2 source2 175.6.1.12 source3
  175.2.9.2
  vcg vcg-uni-multi0
  rf-channel 0
    session mcast multicast-label label110_1 processing-type remap start-program 1
  jitter 100 cbr
  rf-channel 6
    session mcast multicast-label label103_1 processing-type remap start-program 1
  jitter 100 cbr
```

Example 6: Multicast Session with Virtual Carrier Group as Service Type Broadcast Configuration

```
virtual-carrier-group VCG_PME0 id 1
  service-type broadcast
  rf-channel 20-35 tsid 100-115 output-port-number 100-115

table-based
  multicast-label a2 group 232.5.6.7 source 175.2.5.6
  multicast-label exampleLabel group 232.2.1.6 source 175.6.1.13 source2 175.6.1.12 source3
  180.1.1.1 source4 175.6.1.14
  vcg VCG_PME2
  rf-channel 22
    session SESS_PME2 multicast-label a2 processing-type remap start-program 1
  vcg VCG_PME3
  rf-channel 23
    session SESS_PME3 multicast-label exampleLabel processing-type remap start-program
  2
```

Example 7: Sessions with Passthru and Data Processing Type

```
table-based
  multicast-label a2 group 232.5.6.7 source 175.2.5.6
  multicast-label exampleLabel group 232.2.1.6 source 175.6.1.13 source2 175.6.1.12 source3
  180.1.1.1 source4 175.6.1.14
  vcg VCG_PME2
  rf-channel 22
    session SESS_PME2 multicast-label a2 processing-type remap start-program 1
  vcg VCG_PME3
  rf-channel 23
    session SESS_PME3 multicast-label exampleLabel processing-type remap start-program
  2
  vcg VCG_PME4
  rf-channel 24
    session SESS_PME4 group 232.5.6.15 source 175.2.6.7 processing-type passthru
  vcg VCG_PME6
  rf-channel 30
```

```
session SESS_PME6 group 232.2.6.7 source 175.7.2.2 processing-type data
```

Feature Information for Switched Digital Video

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



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

Feature Name	Releases	Feature Information
Switched Digital Video	Cisco 1x2 / Compact Shelf RPD Software 3.1	This feature was integrated into the Cisco Remote PHY Device.



CHAPTER 31

Remote PHY QAM Profile Configuration

This document describes how to configure the QAM profile on the Cisco cBR Series Converged Broadband Router.

Finding Feature Information

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

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

- [Information About QAM Profile, on page 235](#)
- [How to Configure Remote PHY QAM Profile, on page 236](#)
- [Configuration Example, on page 237](#)
- [Feature Information for QAM Profile Configuration, on page 237](#)

Information About QAM Profile

A QAM profile describes the common downstream channel modulator settings, referred to as physical layer parameters. This includes QAM constellation, symbol rate, interleaver-depth, spectrum-inversion, and annex.

The QAM profile is described by CCAP DownPhyParams object. Default QAM profiles are supported and customized for DOCSIS or MPEG Video, which are described as DocsisPhyDefault and VideoPhyDefault objects, respectively.

A maximum of 32 QAM profiles can be defined. There are four system-defined QAM profiles (0 to 3), which cannot be deleted or modified. You can define profiles 4 to 31.

The system defined profiles are:

- Profile 0 - default-annex-b-64-qam
 - interleaver-depth: I32-J4
 - symbol rate: 5057 kilo-symbol/second
 - spectrum-inversion: off

- Profile 1 - default-annex-b-256-qam
 - interleaver-depth: I32-J4
 - symbol rate: 5361 kilo-symbol/second
 - spectrum-inversion: off
- Profile 2 - default-annex-a-64-qam
 - interleaver-depth: I12-J17
 - symbol rate: 6952 kilo-symbol/second
 - spectrum-inversion: off
- Profile 3 - default-annex-a-256-qam
 - interleaver-depth: I12-J17
 - symbol rate: 6952 kilo-symbol/second
 - spectrum-inversion: off

How to Configure Remote PHY QAM Profile

Configuring the QAM Profile on Downstream Channels

```

Enable
configure terminal
  cabledownstream qam-profile Qam_Profile_ID D

  annex {A | B | C}
  description LINE
  interleaver-depth {I12-J17 | I128-J1 | I128-J2 |
I128-J3 | I128-J4 | I128-J5 | I128-J6 | I128-J7 |
I128-J8 | I16-J8 | I32-J4 | I64-J2 | I8-J16}
  modulation {256 | 64}  spectrum-inversion {off | on}
  symbol-rate value
exit

```

You can configure symbol rate for Annex A video and Annex C video. The valid range for Annex A video is 3500 to 7000 kilo-symbols/sec. The valid range for Annex C video is 3500 to 5309 kilo-symbols/sec. The channel width in kHz is symbol-rate * (1 + alpha) with 0.15 alpha for Annex A and 0.13 alpha for Annex C.

Verifying QAM Profile on Downstream Channels

Use the following commands to verify the QAM Profile on Downstream Channels:

```

Router#show running-config | section downstream controller-profile
cable downstream controller-profile 0
  rf-chan 0 3
  type DOCSIS
  frequency 111000000
  rf-output NORMAL

```



```
qam-profile 1
docsis-channel-id 1
```

Configuration Example

QAM Profile Configuration

```
configure terminal
cable downstream controller-profile 1
  multicast-pool 20
  Rf-channel 0 15
  Type docsis
  Frequency 111000000
  Rf-output NORMAL
  Qam-profile 1
  Docsis-channel-id 1
cable downstream controller-profile 2
  multicast-pool 20
  Rf-channel 20 47
  Type video sync
  Frequency 231000000
  Rf-output NORMAL
  Qam-profile 14
```

Feature Information for QAM Profile Configuration

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



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

Table 59: Feature Information for QAM Profile Configuration

Feature Name	Releases	Feature Information
QAM Profile Configuration-RPHY Annex B	Cisco 1x2 / Compact Shelf RPD Software 1.1	This feature was introduced on the Cisco Remote PHY Device.
QAM Profile Configuration-RPHY Annex A and C	Cisco 1x2 / Compact Shelf RPD Software 3.1	This feature was introduced on the Cisco Remote PHY Device.



CHAPTER 32

Cisco Remote PHY Out of Band

Finding Feature Information

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

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

- [Hardware Compatibility Matrix for Cisco Remote PHY Device, on page 239](#)
- [Information About Out of Band, on page 240](#)
- [How to Configure 55-1 OOB , on page 242](#)
- [Example: OOB Configuration, on page 245](#)
- [Feature Information for OOB, on page 246](#)

Hardware Compatibility Matrix for Cisco Remote PHY Device



Note Unless otherwise specified, the hardware components introduced in a given Cisco Remote PHY Device Software Release are supported in all subsequent releases.

Table 60: Hardware Compatibility Matrix for the Cisco Remote PHY Device

Cisco HFC Platform	Remote PHY Device
Cisco GS7000 Super High Output Node	Cisco 1x2 / Compact Shelf RPD Software 2.1 and Later Releases

Cisco HFC Platform	Remote PHY Device
Cisco GS7000 Super High Output Intelligent Node (iNode)	Cisco 1x2 / Compact Shelf RPD Software 4.1 and Later Releases Cisco Intelligent Remote PHY Device 1x2 <ul style="list-style-type: none"> • PID—iRPD-1X2= • PID—iRPD-1X2-PKEY=



Note The -PKEY suffix in the PID indicates units that enable the SCTE-55-2 Out-of-Band protocol support.

Information About Out of Band

Out of Band (OOB) data is used by set-top boxes on the cable plant for the delivery of data streams that support set-top box operation in the downstream and to convey responses and commands from the STB in the upstream.

The two OOB systems are OOB 55-1 and OOB 55-2. The OOB 55-2 system has a scheduled TDMA upstream, which is intolerant of packet network latency. The SCTE 55-1 system does not include such upstream scheduling capabilities, however requires multiple upstream frequencies to operate.

OOB 55–1

A solution that delivers the OOB streams to the RPD via the same Ethernet carriers that the rest of the services traverse is necessary. This solution is necessary to facilitate the delivery of OOB streams from the headend to the customer-facing CPE using the Remote PHY (R-PHY) architecture. The following sections describe 55–1 OOB approaches to this transport:

For downstream:

- Ethernet from the out-of-band Modulator (OM) device: The OM processes OOB source streams as per SCTE-55-1 and outputs datagrams via IP multicast.
- CCAP-Core forward as virtual OM.: The CCAP joins and processes streams from the OM device as per SCTE-55-1 and forwards them downstream to the RPD.

For upstream:

- ATM from STB: The STB sends augmented ATM upstream packet to RPD according to SCTE-55-1. RPD builds up upstream packet as per ARPD protocol (version 2) and forwards it to the CCAP core.
- CCAP-Core forward as virtual ARPD: The CCAP receives 55–1 packet via UEPI and forwards them upstream to the Network Controller (NC).

The out-of-band Modulator (OM) handles receiving of OOB source data streams and creating multiplexed signal according to OOB 55–1. The MPEG transport stream, containing the OOB is IP multicast using the UDP to the CCAP Core over an Ethernet link.

Each OM can output only a single OOB multiplex. Hence, a CCAP Core may receive OOB streams from multiple OMs. Each of these streams is intended for a different set of RPDs.

OM2000 does not include null frames in its Ethernet output stream. The OM outputs nonnull packets in its Ethernet output transport streams. Hence, the downstream QPSK modulator must insert nulls when necessary. The Remote PHY device inserts null packets as necessary to maintain the required module rate of the OOB 55-1 downstream QPSK channel. The downstream modulator need not maintain precise interpacket timing. The modulator can effectively insert null packets wherever necessary without checking for excessive data packet displacement.

Each virtual ARPD uses a unique source IP address and a unique destination UDP port in packets that are sent to the NC. The NC relies on IP addresses and UDP ports to identify the ARPD from which the traffic is arriving.

Using GCP, the CCAP Core configures the attached RPDs with the appropriate ARPD source ID, RF port ID, and demodulator ID corresponding to each UEPI tunnel. The RPD uses this information when forming the ARPD datagram.

From Cisco IOS XE Amsterdam 17.3.1x release, the CCAP core can merge 55-1 upstream data-path traffic from both physical RF ports of an RPD before forwarding to the NC. You can do this by configuring the same profile (ARPD source ID, RF port ID, and demodulator ID) to both Upstream physical RF ports in an RPD. This feature enables service providers to expand the 55-1 service group on to the second US port without the need for extra hardware for 55-1 headend.

The RPD aggregates multiple physical demodulators into a single virtual ARPD demodulator ID.

The RPD supports power level settings in the range of -7 to 0 dBc relative to the 256-QAM level in 0.2-dB steps for the OOB 55-1 FDC.

Forward Channels

To support the orderly transition of set-top boxes to a higher frequency, the SCTE 55-1 forward data can be carried on two forward channels with distinct frequencies. The data content sent on both channels is identical.

The RPD can support two SCTE 55-1 forward channels on any of its downstream RF port.

OOB 55-2

In the video headend, the OOB 55-2 Controller maintains all interfaces with the existing applications and services but contains only a subset of the functions available with the existing 55-2 Modulator/Demodulator. The remaining functions are moved to the RPD.

The OOB 55-2 Remote PHY solution places components necessary for performing ATM slot receipt acknowledgement within the RPD, and all other components of the OOB 55-2 MAC located in the 55-2 Controller where feasible. The OOB 55-2 Controller handles the configuration and monitoring of 55-2 specific functions within the RPD. Some monitoring is also included in the upstream data packets sent by the RPD to the 55-2 Controller.

The current 55-2 Digital Home Communication Terminal (DHCT) service group sizes are more than 10,000 DHCTs, versus the expected RPD DHCT counts which can be 1000 or lower. For compatibility with existing infrastructure, RPDs are grouped with a single 55-2 Controller as follows:

- Multiple RPDs are bound by operator configuration to a single 55-2 Controller which can service >10,000 DHCTs.

- RPD demodulators are assigned an Upstream Group ID between 0 and 7. All demodulators in the same Upstream Group logically-share the same upstream slot assignments for 55-2 compatibility. Upstream Group ID is equivalent to SCTE 55-2 Demodulator Number, but is zero indexed instead of 1 indexed. Upstream Group ID 0 corresponds to SCTE 55-2 Demodulator Number 1 (R1), Upstream Group ID 7 corresponds to SCTE 55-2 Demodulator Number 8 (R8).
- All RPDs bound to a single 55-2 Controller share a single L2TPv3 multicast tunnel for downstream data.

An RPD can incorporate a number of SCTE 55-2 modules, each represented by Oob55d2Module object. The number of SCTE 55-2 Modules is communicated using RPD capabilities. Common parameters for all 55-2 modules are grouped into an Oob55-2Config object.

Each SCTE55-2 module consists of one modulator and one to eight demodulators. The Oob55-2Modulator can be associated with one or more downstream RF ports, and the Oob55-2Demodulator can be associated with zero or one upstream RF ports.

The RPD reports these associations to the CCAP Core.

Prerequisites

The RPD must support the following:

- RPD connects to only one 55-2 controller.
- OOB 55-2 specific L2TPv3 multicast packets containing downstream ATM cells and metadata.
- OOB 55-2 specific IP and L2TPv3 encapsulation of upstream ATM cells and metadata.
- Sending at least one L2TPv3 upstream tunnel per RPD to the 55-2 Controller.
- Forwarding the IP unicast packets to the 55-2 Controller.
- GCP configuration by the 55-2 Controller using authenticated and secured connections.
- An authenticated and secured L2TPv3 control connection with the 55-2 Controller.

How to Configure 55-1 OOB

This section describes how to configure OOB on Cisco cBR-8.

Configuring Global 55-1 OOB

To configure OOB, complete the following procedure:

```

configure terminal
cable oob
virtual-om o-id
ip ip subnet_mask
join-group ip source-ip ip out-group ip
virtual-arpd id
ip ip subnet_mask
nc ip udp-port number
source-id s-id

```



Note By default, the source ID is set to **virtual-arpd ip**. If you want to configure a different value for the source ID, then configure the source ID that is applicable to the Network Controller (NC).



Caution The NC may drop upstream packets from this virtual-arpd, if the source ID is not compatible with the NC.

Configuring Profile for 55-1 OOB

To configure profile to use OOB, complete the following procedure:

```
configure terminal
controller downstream-oob 55d1-profile dp-id
no ds-channel 0 rf-mute
no ds-channel 0 shutdown
ds-channel 0 frequency f-value
ds-channel 0 poweradjust p-value
controller upstream-oob 55d1-profile up-id
no us-channel 0 shutdown
us-channel 0 frequency f-value
us-channel 0 varpd-portid va-id (ID range is 1-6) varpd-demodid vd-id
us-channel 0 poweradjust p-value
no us-channel 1 shutdown
us-channel 1 frequency f-value
us-channel 1 varpd-portid va-id varpd-demodid vd-id
us-channel 1 poweradjust p-value
no us-channel 2 shutdown
us-channel 2 frequency f-value
us-channel 2 varpd-portid va-id varpd-demodid vd-id
us-channel 2 poweradjust p-value
```



Note Upstream channel **poweradjust** is an optional configuration and should be configured based on the application requirement. The valid range is 50 to -100, in tenth of a dB.

Configuring Remote PHY Device for 55-1 OOB

To configure the RPD to use OOB, complete the following procedure:

```
configure terminal
cable rpd name
identifier id
no sbfd enable
core-interface TenGigabitEthernet slot/subslot/port
principal
rpd-ds 0 downstream-oob-vom o-id profile dp-id
rpd-us 0 upstream-oob-varpd a-id profile up-id
```

```

rpd-us 1 upstream-oob-varpd a-id profile up-id
r-dti value
rpd-event profile id
rpd-55d1-us-event profile id

```

Configuring OOB with VRF

The following example shows how to configure the OOB with VRF:

```

cable oob
  virtual-om 1
    ip 100.100.100.100 255.255.255.0 vrf xxx
    join-group 235.1.1.1 source-ip 2.3.4.5 out-group 239.2.2.2
  virtual-arpd 1
    ip 20.20.20.20 255.255.255.0 vrf xxx
    nc 200.1.1.100 udp-port 100

```



Note The `source-id` is an optional configuration and needs to be configured only when the Network controller (NC) requires it. The value has to be decimal value of the IP address of VARPD interface on CBR-8. In the above example, it should be 336860180 for 20.20.20.20.

Configuring Two Forward Channels

The following example shows how to configure two forward channels. This configuration is OOB DS profile: (1 port per RPD, 1 channel per port, 2 output RF frequency per channel):

```

controller downstream-oob 55d1-profile 100
  no ds-channel 0 rf-mute
  no ds-channel 0 shutdown
  ds-channel 0 frequency 70000000
  ds-channel 0 poweradjust 0
  no ds-channel 0 sf-mute
  no ds-channel 0 sf-shutdown
  ds-channel 0 second-frequency 130000000
  ds-channel 0 sf-poweradjust -10

```

Configuring Virtual OM with Multicast Pool

The outgroup of virtual-om can be configured with IP or a multicast pool. When an multicast pool id is configured, an IP is automatically assigned from the configured **cable depi multicast pool**. This multicast pool can either be IPv4 or IPv6, based on the RPD IP scheme.

```

Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# cable depi multicast pool 10
Router(config-multicast-pool)# ipv6 address FF3A::8001:0/120

Router(config)# cable oob
Router(config-oob)# virtual-om 1
Router(config-oob-vom)# join-group 233.1.1.11 source-ip 10.10.2.10 out-group ?
  A.B.C.D      group IPv4 address
  X:X:X:X::X   group IPv6 address

```



```
mcast-pool multicast pool for out-group
Router(config-oob-vom)# join-group 233.1.1.11 source-ip 10.10.2.10 out-group mcast-pool ?
<0-127> multicast pool id
Router(config-oob-vom)# join-group 233.1.1.11 source-ip 10.10.2.10 out-group mcast-pool 10
```

Verifying OOB DS Details

Use the following commands to verify the DS details.

```
show platform software cable F0 oob-ds
show platform software cable F0 oob-ds statistics
clear platform software cable F0 oob-ds statistics
show platform software cable F0 oob-ds group <G2 address>
```

Verifying OOB US Details

Use the following commands to verify the US details.

```
show platform software cable F0 oob-us
show platform software cable F0 oob-us statistics
clear platform software cable F0 oob-us statistics
show platform software cable F0 oob-us source-id <RPD source id>
```

Verifying OOB Channel Details

Use the following commands to view the OOB channel details.

```
show cable rpd db-dump rpd-oob-ds-chan (all)
show cable rpd db-dump rpd-oob-us-chan (all)
```

Debugging OOB

Use the following commands to view the OOB channel details.

```
debug cable rphy-oob
```

The following command provides information on US RF ports, 55-1 Channels, and packet count information of the UEPI sessions.

```
show platform software cable fp active oob-chn-pkts
```

The following command provides debug information and is especially useful in case of profile duplication.

```
show cable rpd 55d1-us cpp-cache
```

Example: OOB Configuration

The following example shows how to configure OOB:

```
Router#configure terminal
Router(config)# cable oob
Router(config-oob)# virtual-om 1
Router(config-oob-vom)# ip 100.100.100.100 255.255.255.0
Router(config-oob-vom)# join-group 235.1.1.1 source-ip 2.3.4.5 out-group 239.2.2.2
```

```

Router(config-oob-vom)# exit

Router(config-oob)# virtual-arpd 1
Router(config-oob-varpd)# ip 32.32.32.32 255.255.255.0
Router(config-oob-varpd)# nc 3.3.3.3 udp-port 100
Router(config-oob-varpd)# exit
Router(config-oob)# exit

Router(config)# controller downstream-OOB 55d1-profile 1
Router(config-profile)# no ds-channel 0 rf-mute
Router(config-profile)# no ds-channel 0 shutdown
Router(config-profile)# ds-channel 0 frequency 70000000
Router(config-profile)# ds-channel 0 poweradjust 1
Router(config-profile)# exit

Router(config)# controller upstream-OOB 55d1-profile 1
Router(config-profile)# no us-channel 0 shutdown
Router(config-profile)# us-channel 0 frequency 5216000
Router(config-profile)# us-channel 0 varpd-portid 3 varpd-demodid 2
Router(config-profile)# no us-channel 1 shutdown
Router(config-profile)# us-channel 1 frequency 6000000
Router(config-profile)# us-channel 1 varpd-portid 3 varpd-demodid 4
Router(config-profile)# no us-channel 2 shutdown
Router(config-profile)# us-channel 2 frequency 8000000
Router(config-profile)# us-channel 2 varpd-portid 3 varpd-demodid 6
Router(config-profile)# exit

Router(config)# cable rpd nodel
Router(config-rpd)# identifier 0004.9f00.0685
Router(config-rpd)# no sbfd enable
Router(config-rpd)# core-interface Te7/1/0
Router(config-rpd-core)# principal
Router(config-rpd-core)# rpd-ds 0 downstream-cable 7/0/0 profile 3
Router(config-rpd-core)# rpd-ds 0 downstream-oob-vom 1 profile 1
Router(config-rpd-core)# rpd-us 0 upstream-cable 7/0/0 profile 3
Router(config-rpd-core)# rpd-us 0 upstream-oob-varpd 1 profile 1
Router(config-rpd-core)# exit

Router(config-rpd)# r-dti 1
Router(config-rpd)# rpd-event profile 0
Router(config-rpd)# rpd-55d1-us-event profile 0

```

Feature Information for OOB

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



Note

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

Table 61: Feature Information for OOB

Feature Name	Releases	Feature Information
Out of Band	Cisco 1x2 / Compact Shelf RPD Software 3.1	This feature was integrated into the Cisco Remote PHY Device.
Support for OOB 55-2	Cisco 1x2 / Compact Shelf RPD Software 3.1	This feature was integrated into the Cisco Remote PHY Device.



PART **V**

Remote PHY Management

- [Secure Software Download, on page 251](#)
- [Cisco Remote PHY Fault Management, on page 255](#)
- [Cisco Remote PHY Device Operations and Debugging, on page 261](#)
- [RPD Reset, on page 267](#)
- [Archiving RPD Logs, on page 273](#)
- [SSH Account Management, on page 279](#)



CHAPTER 33

Secure Software Download

This document describes how to upgrade software from RPD and Cisco cBR by using Secure Software Download feature.

- [Hardware Compatibility Matrix for Cisco Remote PHY Device, on page 251](#)
- [Information About Secure Software Download, on page 252](#)
- [How to Upgrade Software from RPD and Cisco cBR Using SSD, on page 252](#)
- [Examples for Upgrading HA RPHY Software, on page 253](#)
- [Feature Information for Secure Software Download, on page 254](#)

Hardware Compatibility Matrix for Cisco Remote PHY Device



Note Unless otherwise specified, the hardware components introduced in a given Cisco Remote PHY Device Software Release are supported in all subsequent releases.

Table 62: Hardware Compatibility Matrix for the Cisco Remote PHY Device

Cisco HFC Platform	Remote PHY Device
Cisco GS7000 Super High Output Node	Cisco 1x2 / Compact Shelf RPD Software 2.1 and Later Releases
Cisco GS7000 Super High Output Intelligent Node (iNode)	Cisco 1x2 / Compact Shelf RPD Software 4.1 and Later Releases Cisco Intelligent Remote PHY Device 1x2 <ul style="list-style-type: none">• PID—iRPD-1X2=• PID—iRPD-1X2-PKEY=



Note The -PKEY suffix in the PID indicates units that enable the SCTE-55-2 Out-of-Band protocol support.

Information About Secure Software Download

The secure software download (SSD) feature allows you to authenticate the source of a code file and verify the downloaded code file before using it in your system. The SSD is applicable to Remote PHY (R-PHY) devices installed in unsecure locations.

The Remote PHY architecture allows RPDs to download code. Hence, authenticating the source and checking the integrity of the downloaded code is important.

To authenticate and verify downloading of the code, SSD helps in verifying the manufacturer signature and the operator signature, if any. The manufacturer signature affirms the source and integrity of the code file to the RPD. If an additional signature is available from the operator, the RPD verifies both signatures with a certificate chain before accepting a code file.

Prerequisites for Upgrading Software using SSD

The following prerequisites are applicable to upgrading RPD software using SSD:

- The R-PHY node supports downloading software initiated through the GCP message sent from Cisco cBR.
- RPD supports a secure software download initiated using SSH and CLI directly on the RPD.
- R-PHY uses TFTP or HTTP to access the server to retrieve the software update file.

How to Upgrade Software from RPD and Cisco cBR Using SSD

Initiating RPD Software Upgrade from Cisco cBR

The RPD software upgrade can be initiated from Cisco cBR-8 Router. Use the following commands for initiating the upgrade:

```
cable rpd {all|oui|slot|RPD IP|RPD MAC} ssd server_IP {  
    tftp|http} file_name [c-cvc-c|m-cvc-c]  
    [CVC Chain File Name]
```

Initiating Software Upgrade from RPD Using SSD

If you want to initiate the software upgrade from RPD, set the SSD parameters on RPD. Use the following commands.

Setting the value for SSD CVC (Manufacturer's and Co-signer Code Validation Certificates) parameter is optional.

Configure the values for the following parameters

- SSD server IP address
- Filename

- Transport method

```

ssd set server server_IP filename file_name transport {tftp|http}
ssd set cvc {manufacturer|co-signer} cvc_chain_file_name
ssd control start

```

Verifying Software Upgrade Using SSD Configuration

To display the RPD SSD status, use the **cable rpd [all|oui|slot|RPD IP|RPD MAC] ssd status** command as given in the following example.

```

Router# cable rpd all ssd status
RPD-ID          ServerAddress Protocol Status          Filename
0004.9f00.0591 192.0.2.0      TFTP      ImageDownloading image/RPD_seres_rpd_20170216_010001.itb.SSA
0004.9f00.0861 192.0.2.2      TFTP      CodeFileVerified  userid/RPD_seres_rpd_20170218_010001.itb.SSA
0004.9f03.0091 192.0.2.1      TFTP      ImageDownloadFail chuangli/openwrt-seres-rpd-rdb.itb.SSA

```

The available statuses are the following:

- CVCVerified
- CVCRejected
- CodeFileVerified
- CodeFileRejected
- ImageDownloading
- ImageDownloadSucceed
- ImageDownloadFail
- MissRootCA

Examples for Upgrading HA RPHY Software

See examples for the software upgrade from cBR-8 and FCC or Primary eRPD.

Example: HA RPHY Software Upgrade from Cisco cBR

```

Router# upgrade set server 203.0.113.1 filename bundle/test.itb.sign transport http
Router# upgrade control show config

```

```

file path: bundle/test.itb.sign
server: 203.0.113.1
transport: HTTP
Router# upgrade control start
Router# upgrade control show status.
Downloading image on FCC.

```

```

Router# cable rpd group all upgrade 203.0.113.2 http bundle/test.itb.sign
Router# cable rpd group all upgrade status

```

Example: HA RPHY Software Upgrade from FCC or Primary eRPD

```

This group 0027.900a.4c1a is not HA-Shelf group.
GROUP-ID: 7abd.44a1.0000
ServerAddress: 203.0.113.2
Protocol: HTTP
Status: Image downloading on RPDLC
Filename: bundle/test.itb.sign

```

Example: HA RPHY Software Upgrade from FCC or Primary eRPD

```

Router# upgrade set server 203.0.113.2 filename bundle/test.itb.sign transport http
Router# upgrade control start
Router# upgrade control show status
Downloading image on FCC.
Router# upgrade control abort
Abort software upgrade process successfully.
Router# upgrade control show status
Image download aborted.

```

```

Router# show cable rpd-upgrade group all status
GROUP-ID: 7abd.44a1.0000
ServerAddress: 203.0.113.2
Protocol: HTTP
Status: Idle
Filename: bundle/test.itb.sign

```

Feature Information for Secure Software Download

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



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

Table 63: Feature Information for Secure Software Download

Feature Name	Releases	Feature Information
Upgrade Software Image	Cisco Smart PHY 7200	This feature was introduced on the Cisco Remote PHY Device.



CHAPTER 34

Cisco Remote PHY Fault Management

This document describes how to configure the events for fault management on the Cisco cBR Series Converged Broadband Router.

- [Information About Fault Management, on page 255](#)
- [How to Configure RPD Events, on page 256](#)
- [Configuration Examples , on page 259](#)
- [Feature Information for R-PHY Fault Management, on page 260](#)

Information About Fault Management

Fault management on RPD is required for remote monitoring, detection, diagnosis, reporting, and correcting the issues.

The Fault management module provides the following support:

- RPD can send events to the CCAP core
- CCAP core can get events from RPD
- Send RPD events using SNMP traps
- On the CCAP core, view log in to the CLI
- SNMP poll events are supported

RPD Event Reporting

An RPD logs events, generates asynchronous notifications that indicate malfunction situations, and notifies the operator about important events. The RPD event reporting includes two methods of reporting.

- During the initialization of RPD, CCAP core synchronizes events from the RPD.
- During run-time operations, RPD notifies the CCAP Core of the events

Restrictions for Configuring RPD Events

Following restrictions are applicable:

A maximum of 1000 events are retained on Cisco cBR. The RPD retains 1000 events locally and 1000 events in pending state.

How to Configure RPD Events

Configuring RPD Events

You can configure an event profile and apply it to RPD. Use the following commands to configure RPD events:

```
enable
configure terminal
cable profile rpd-event profile_id
  priority {emergency|alert|critical|error|warning|notice|informational|debug}
  {0x0|0x1|0x2|0x3}
enable-notify
```

- 0x0—No log
- 0x1— Save log in RPD local storage
- 0x2—Report to Cisco cBR
- 0x3— Save log in RPD local storage and report to Cisco cBR

You must enable-notifications for the RPD to report any event to the Core.

Configuring 55-1 Upstream RPD Events

You can configure an event profile and apply it to RPD. The 55-1 US events can be viewed only using log. For more information, go through [Viewing RPD Events Using Log, on page 259](#).

SUMMARY STEPS

1. Use the following commands to configure RPD 55-1 US events:

DETAILED STEPS

	Command or Action	Purpose
Step 1	Use the following commands to configure RPD 55-1 US events:	<pre>configure terminal cable profile rpd-55d1-us-event <profile_id> corrected-cells-threshold <threshold value> high-power-threshold <threshold value> low-power-threshold <threshold value> total-cells-threshold <threshold value> uncorrectable-cells-threshold <threshold value></pre> <ul style="list-style-type: none"> • corrected-cells-threshold - <-1-65535> US Excessive Corrected Cells Threshold. • high-power-threshold - <-16 - 16> High power threshold in dBmV.

	Command or Action	Purpose
		<ul style="list-style-type: none"> • <code>low-power-threshold - <-16 - 16></code> Low power threshold in dBmV. • <code>total-cells-threshold - <1-65535></code> US Excessive Total Cells Threshold. • <code>uncorrectable-cells-threshold - <1-65535></code> US Excessive Uncorrectable Cells Threshold. <p>Ensure that you have enabled notifications for the RPD to report any event to the core.</p>

Applying the Event Profile to RPD

Use the following commands to apply the Event Profile to an RPD:

```
enable
configure terminal
cable rpd rpd_name
rpd-event profile profile_id
rpd-55d1-us-event profile profile_id
```



Note If RPD is online when changing the profile, ensure that you have reset the RPD after you change the profile.

Enable RPD Event Trap

You can enable RPD event traps to send RPD events using SNMP traps. Use the following commands to configure RPD event traps:

```
enable
configure terminal
snmp-server enable traps rpd-event priority
```

Priority can be 1-8, where:

- 1—Enable RPD event trap for emergency priority
- 2— Enable RPD event trap for alert priority
- 3—Enable RPD event trap for critical priority
- 4— Enable RPD event trap for error priority
- 5— Enable RPD event trap for warning priority
- 6— Enable RPD event trap for notice priority
- 7— Enable RPD event trap for informational priority
- 8— Enable RPD event trap for debug priority

The priority higher than the selected priority is also displayed.

Configure SNMP Trap Server

You can configure SNMP trap server on the cable modem using the following commands:

```
enable
configure terminal
Router# snmp-server host ip_address traps version 2c public udp-port port_number
```

where,

- *ip_address*—IP address of the server
- *port_number*—UDP port number assigned to receive the SNMP traps. The same port number must also be configured on the SNMP server.

Getting RPD Events

To retrieve events from RPD, use the **cable rpd [RPD IP|RPD MAC|all] event {locallog|pending}** command, as given in the following example:

```
Router#cable rpd 30.84.2.111 event pending
```

Clearing All Events on Cisco cBR Database

To remove all Events on Cisco cBR, use the **clear cable rpd all event** command, as given in the following example:

```
Router#clear cable rpd all event
```

Viewing the RPD Events

To view all RPD Events, use the **show cable rpd [RPD IP|RPD MAC] event** command as given in the following example.

```
Router# show cable rpd 93.3.50.7 event
RPD          EventId      Level Count  LastTime      Message
0004.9f00.0861 66070204   Error  1    Feb21 12:11:06 GCP Connection Failure
CCAP-IP=30.85.33.2;RPD-ID=0004.9f00.0861;
0004.9f00.0861 2148074241 Error  1    Feb21 12:11:25 Session failed:connecting timeout,
@SLAVE: 93.3.50.7:None --> 30.85.33.2:8190;RPD-ID=0004.9f00.0861;
```

To view specific RPD event groups, use the **show cable rpd event group [RPD IP|RPD MAC] [fcc|slot]** command as shown in this example.

```
Router# show cab rpd event group 7abd.44a1.0000 fcc
RPD          EventId      Level Count  LastTime      Message
7abd.44a1.0040 66070303 Criti  2    Oct16 20:50:35 FCC event
example;GROUP-ID=7abd.44a1.0000;
SLOT-ID=FCC;RPD-ID=7abd.44a1.0040;
```

```
Router# show cab rpd event group 7abd.44a1.0000 slot 9
RPD          EventId      Level Count  LastTime      Message
7abd.44a1.0140 66070700 Notic  1    Oct16 17:20:34 RPD=7a:bd:44:a1:01:40 PTP clock
synchronized to Master=10.90.3.93;GROUP-ID=7abd.44a1.0000;
```

```
SLOT-ID=LC9;RPD-ID=7abd.44a1.0140;
```

Viewing RPD Events Using Log

To view all RPD Events, use the show logging command, as given in the following example.

```
Router# show logging | include RPD-ID=0004.9f00.0861
004181: Feb 21 12:18:59.649 CST: %RPHYMAN-3-RPD_EVENT_ERROR: CLC5: rphyman:
GCP Connection Failure CCAP-IP=30.85.33.2;RPD-ID=0004.9f00.0861;EVENT-ID=66070204;
FirstTime=2017-2-21,12:11:6.0;
LastTime=2017-2-21,12:11:6.0;
Count=1;PendingQueue;
004185: Feb 21 12:19:18.875 CST: %RPHYMAN-3-RPD_EVENT_ERROR: CLC5: rphyman:
Session failed:connecting timeout, @SLAVE: 93.3.50.7:None --> 10.10.10.12:1190;
RPD-ID=0004.9f00.0861;
EVENT-ID=2148074241;
FirstTime=2017-2-21,12:11:25.0;
LastTime=2017-2-21,12:11:25.0;
Count=1;PendingQueue;
```

Configuration Examples

This section provides example for the fault management configuration on Cisco cBR-8.

Example: RPD Event Configuration

```
enable
configure terminal
cable profile rpd-event 6
    priority warning 0x3
    enable-notify
cable rpd node6
    identifier badb.ad13.5e08
    core-interface Te3/1/5
        principal
            rpd-ds 0 downstream-cable 3/0/17 profile 10
            rpd-us 0 upstream-cable 3/0/34 profile 13
        r-dti 16
    rpd-event profile 6
```

The following event reportings are supported:

- **alert**: Event reporting for alert priority.
- **critical**: Event reporting for critical priority.
- **debug**: Event reporting for debug priority.
- **emergency**: Event reporting for emergency priority.
- **error**: Event reporting for error priority.
- **informational**: Event reporting for informational priority.
- **notice**: Event reporting for notice priority.
- **warning**: Event reporting for warning priority.

Example: RPD 55-1 Upstream Event Configuration

```

cable profile rpd-event 6
  priority warning 0x3
  enable-notify

cable profile rpd-55d1-us-event 10
  corrected-cells-threshold 11
  high-power-threshold 7
  low-power-threshold 2
  total-cells-threshold 20
  uncorrectable-cells-threshold 8

cable rpd node 6
  identifier badb.ad13.5e08
  core-interface Te3/1/5
  principal
  rpd-ds 0 downstream-cable 3/0/17 profile 10
  rpd-us 0 upstream-cable 3/0/34 profile 13
  r-dti 16
  rpd-event profile 6
  rpd-55d1-us-event profile 10

```

Feature Information for R-PHY Fault Management

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



Note

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

Table 64: Feature Information for R-PHY Fault Management

Feature Name	Releases	Feature Information
R-PHY Fault Management	Cisco 1x2 / Compact Shelf RPD Software 3.1	This feature was integrated into the Cisco Remote PHY Device.



CHAPTER 35

Cisco Remote PHY Device Operations and Debugging

This document describes the RPD operations and debugging of an RPD.

- [Hardware Compatibility Matrix for Cisco Remote PHY Device, on page 261](#)
- [Information about RPD Operations and Debugging, on page 262](#)
- [How to Access and Debug RPD, on page 262](#)
- [Configuration Examples, on page 264](#)
- [Feature Information for RPD Operations and Debugging, on page 265](#)

Hardware Compatibility Matrix for Cisco Remote PHY Device



Note Unless otherwise specified, the hardware components introduced in a given Cisco Remote PHY Device Software Release are supported in all subsequent releases.

Table 65: Hardware Compatibility Matrix for the Cisco Remote PHY Device

Cisco HFC Platform	Remote PHY Device
Cisco GS7000 Super High Output Node	Cisco 1x2 / Compact Shelf RPD Software 2.1 and Later Releases
Cisco GS7000 Super High Output Intelligent Node (iNode)	Cisco 1x2 / Compact Shelf RPD Software 4.1 and Later Releases Cisco Intelligent Remote PHY Device 1x2 <ul style="list-style-type: none">• PID—iRPD-1X2=• PID—iRPD-1X2-PKEY=



Note The -PKEY suffix in the PID indicates units that enable the SCTE-55-2 Out-of-Band protocol support.

Information about RPD Operations and Debugging

The operators might need secure remote access to the RPD for activities such as setting up the RPD before the installation, maintenance, or troubleshooting. The RPD supports Secure Shell (SSH) server that allows secure access to the RPD.

Prerequisites for RPD Operations

The following prerequisites are applicable for debugging or checking RPD operations:

- RPD has established GCP connection with the CCAP-core, and RPD IP address is retrievable from CCAP-core.
- RPD is assigned an IP address through the DHCP process, and the IP address is retrievable from the DHCP server.

How to Access and Debug RPD

Accessing RPD using SSH

After logging in to the RPD for the first time, the system shows a security warning.

```
2020-01-13 04:48:26,584-rpd_logging.py-119-ERROR-0x80090807:Service Disabled - PLEASE CHANGE
RPD SSH PASSWORD IMMEDIATELY - default login credentials detected in use
2020-01-13 04:48:26,586-cli_main.py-216-WARNING-Default password detected in use
```

```
*****
***** SERVICE IMPACTING *****
***** PLEASE READ *****
*****
Default login credentials detected in use.
In order to enhance the security of your network,
default login credentials must be changed on this RPD.
```

```
@@@ RPD SERVICE HAS BEEN DISABLED !!! @@@
```

```
*****
***** CHANGE SSH PASSWORD *****
***** IMMEDIATELY *****
*****
```

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
SECURITY WARNING: ssh password login is accessible!
Please use pubkey login and set password login off!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

```
Welcome to Cisco R-PHY
```

```
R-PHY>
```

The following procedure shows how to use SSH to access RPD without password from NMS.

1. Check whether NMS already has an SSH key. If yes, do not generate a new key.
2. Generate a new SSH key in NMS.

```
cat ~/.ssh/id_rsa.pub
ssh-keygen -t rsa
```

3. Add the NMS public key in RPD.

```
ssh pubkey add ?
LINE          NMS's pubkey
```

4. Verify whether NMS can connect using SSH to RPD without a password.

```
ssh -l admin <RPD ip>
```

Disabling SSH Login Password

Use the following commands to apply the Event Profile to an RPD:

```
R-PHY#conf t
R-PHY(config)#ssh password ?
off          disable ssh password login
on           enable ssh password login
R-PHY(config)#ssh password off
R-PHY(config)#end
```

Debugging RPD

Use the following procedure to debug RPD:

1. Disable RPD auto reboot by setting the reboot hold.


```
R-PHY# set reboot hold
```
2. Secure copy the logs of RPD to the server using the following command.


```
logging provision-archive scp server_ip user_id dst_location
```
3. Collect the show CLI output.

For RPD online issues, check which status is failed. You can check the following outputs:

- show provision all
- show provision history
- show dot1x detail
- show dhcp
- show tod
- show ptp clock 0 config
- show ptp clock 0 state

For modem online issue, check ds/us config and l2tp session.

You can collect the following outputs:

- show downstream channel configuration
- show downstream channel counter dps (show multiple times)
- show downstream depi configuration
- show upstream channel configuration <port number> <channel number>
- show upstream iuc counter <port number> <channel number> (show multiple times)
- show upstream map counter <port number> <channel number> (show multiple times)
- show upstream uepi configuration
- show l2tp tunnel
- show l2tp session

4. Enable RPD auto reboot, after collecting all logs and CLI output.

```
R-PHY#clear reboot hold
```

Verifying Disabled SSH Password Login

To check whether the SSH logging in using a password is disabled, use the show ssh session command as given in the following example.

```
R-PHY#show ssh session
connected session: 1
ssh password auth: off
ssh NMS pubkey num: 1
R-PHY#
```

Configuration Examples

This section provides example for the fault management configuration on R-PHY.

Example: Generating a New NMS pubkey

```
$ cat ~/.ssh/id_rsa.pub

$ ssh-keygen -t rsa

$ cat ~/.ssh/id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAEAtQCXVFmRIwemejbTx0+U8taMq5n4Zetu
71xb+dtHV8Rr0wej iK1YJkT93n9hcBxsjHRu76bLp991+DDNL3+TH1jwnMQC1CsdvRmGXoe
Gf1mT9aTlGDf/ RW9ZywY9t8Kep9VnANu2DWSoh0wg2pE49HFOJAbGfuFOvPEdwZGGDMQNws
Eq/3xAQjBxajQqfgu4IqjVzKoo4PM/xx9X4Z1aMwxS3DvyN7L8O0o33mcDNsas13SslIjMSNfq
YpwOFvQve8c2onrYHUx2p3BwQOb/b0FzFQhZMTBXm/pDMXq/fkkD0uguk1xOGnqAATMJsSHIN
0UOdvbzhmrFRBBM4NzqQG5kNt7KvnWgxE7HdalERvMyBC2MCGbFShmQFyWmHHBPPmLIxK98W
XutoR8fzszs+4hingZ4X9DMMNwTQ6WOzjuKq6iU= userid@example.cisco.com
```

Example: Adding NMS pubkey in RPD

```
R-PHY#conf t
R-PHY(config)#ssh pubkey add ?
LINE
      NMS's pubkey
R-PHY(config)#ssh pubkey add ssh-rsa AAAAB3NzaC1yc26876bhjdsK
EEEEAAAABiWAAAgerP3nFp0v0k3Nf4UvSTuOOQi2h0mAfAtQCXVfMriWemejbTx0+U8taM
q5n4Zetu71xb+dtHV8Rr0wejiKlYJkT93n9hcBxsjHRu76bLp991+DDNL3+THljwnMQC1
CsdvRmGXoeGf1mT9aTlGDf/YfKxZMozMnR9qlGJFXlRAwGmsCR11lnV6IkFyh59P9Udkd
SSWv+QL8lCftWBmMnyt/CkqL98NK0Vp0gIYRv7UKCwhK40c8X7PhzxCMKVFTUv3bf9VIP
NA2esgzKDFpoJZkqCjrnXU1Xu00j8Ttwci7f0ytSrFvVKuWp4XZbVdpWGH90BOQR8gKHmq
urP3nFp0v0k3Nf4UvSTuOOQi2h0mAf+9wzm+ab41ToadUbMawHyFYyuU= xxx@xxx.xxx.com
R-PHY(config)#end
```

```
R-PHY#show ssh nms-pubkey ssh-rsa AAAAB3NzaC1yc2EAAAABiWAAAgerP3nFp0v0k3Nf4UvSTuOOQi2h0mAfAtQCXVfMriWemejbTx0+U8taMq5n4Zetu71xb+dtHV8Rr0wejiKlYJkT93n9hcBxsjHRu76bLp991+DDNL3+THljwnMQC1CsdvRmGXoeGf1mT9aTlGDf/YfKxZMozMnR9qlGJFXlRAwGmsCR11lnV6IkFyh59P9UdkdSSWv+QL8lCftWBmMnyt/CkqL98NK0Vp0gIYRv7UKCwhK40c8X7PhzxCMKVFTUv3bf9VIPNA2esgzKDFpRvMyBC2MCGbFShmQFyWmHBHPmLiXK98WXutoR8fzsz+4hingZ4X9DMMNwtQ6WOzjuKq6iU= xxx@xxx.xxx.com
```

Feature Information for RPD Operations and Debugging

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



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

Table 66: Feature Information for RPD Operations and Debugging

Feature Name	Releases	Feature Information
RPD Operations and Debugging	Cisco 1x2 / Compact Shelf RPD Software 3.1	This feature was integrated into the Cisco Remote PHY Device.



CHAPTER 36

RPD Reset

Finding Feature Information

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

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

- [Hardware Compatibility Matrix for Cisco Remote PHY Device, on page 267](#)
- [Information about RPD Reset, on page 268](#)
- [Resetting RPD, on page 268](#)
- [RPD TACACS, on page 270](#)
- [Feature Information for RPD Reset, on page 270](#)

Hardware Compatibility Matrix for Cisco Remote PHY Device



Note Unless otherwise specified, the hardware components introduced in a given Cisco Remote PHY Device Software Release are supported in all subsequent releases.

Table 67: Hardware Compatibility Matrix for the Cisco Remote PHY Device

Cisco HFC Platform	Remote PHY Device
Cisco GS7000 Super High Output Node	Cisco 1x2 / Compact Shelf RPD Software 2.1 and Later Releases

Cisco HFC Platform	Remote PHY Device
Cisco GS7000 Super High Output Intelligent Node (iNode)	Cisco 1x2 / Compact Shelf RPD Software 4.1 and Later Releases Cisco Intelligent Remote PHY Device 1x2 <ul style="list-style-type: none"> • PID—iRPD-1X2= • PID—iRPD-1X2-PKEY=



Note The -PKEY suffix in the PID indicates units that enable the SCTE-55-2 Out-of-Band protocol support.

Information about RPD Reset

Starting from Cisco 1x2 / Compact Shelf RPD Software 6.1, factory reset and NVRAM reset via TLV and CLI are supported. In the factory reset, RPD restores the factory configuration and performs cold reboot. In this case, it is better for the RPD to have golden image, otherwise users need to boot the RPD manually. In the NVRAM reset, RPD clears the non-volatile configuration and performs cold reboot.

Resetting RPD

To clear the configuration, image and logs of the RPD, perform factory reset as shown in the following example:

```
R-PHY#reboot factory-reset
```

```
Warning: This action will restore the factory configuration. Are you sure you want to do
the factory reset (yes/no)?
```

To clear the non-volatile configuration of the RPD, perform NVRAM reset as shown in the following example:

```
R-PHY#reboot nv-reset
```

```
Warning: This action will clear the non-volatile configuration. Are you sure you want to
do the nvreset (yes/no)?
```

Soft-reset

Soft-reset is supported from Cisco 1x2 / Compact Shelf RPD Software 6.6 release. You can perform a soft-reset on the RPD using the RPD CLI or write TLV 40.1.1 (RpdResetCtrl to softReset(1)).

To perform soft-reset using RPD CLI, use the **reboot soft-reset** command:

```
R-PHY# reboot soft-reset
```

```
Warning: This action will perform a soft reset. Are you sure you want to do the soft reset
(yes/no)?yes
SoftReset in 10 seconds
```


History of RPD Reset Instances

Cisco RPD supports the ResetHistory (TLV 100.3) object, which provides a record of the occurrences of a reset of an RPD. The RPD can be reset for many reasons, such as a loss of Principal Core, loss of IP connection, power failure, hardware or software failure, or reset command from CCAP Core or CLI.

This ResetHistory object provides details of the conditions that caused the RPD to reset and to assist operators with understanding why a service interruption occurred. It also provides details of how much time it took for the RPD to boot its software stack and to become operational with the principal core.



Note

- If the `rebootdisable` parameter is set, the RPD does not save any record.
- If the power cycle is triggered during a reboot, the application is not notified about it. Hence, after recovery, the recovery time and the related information are saved in the latest record. New records are not generated for the power cycle reboot.
- Recovery time (recoveryTime—TLV 100.31.7)
 - `softReset`—The recovery time of the soft-reset is the RCP process up-time when the system becomes operational.
 - `hardReset/nvReset/factoryReset`—The recovery time is the system up-time when the system becomes operational.
- It stores up to 100 records.

Display or Clear Reset-History

Use the following command to show the RPD reset-history: **show reset-history:**

```
R-PHY#show reset-history
Index  Type           ResetTimeStamp           RecoveryTimeStamp         RecoveryTime  EventRef
1      hardReset      2020-01-13 01:42:42     2020-01-13 01:51:22     481          66070212
2      softReset      2020-01-13 01:30:18     1970-01-01 00:00:00     0            66070212
3      hardReset      2020-01-13 01:19:19     2020-01-13 01:29:26     568          66070212
4      hardReset      2020-01-13 00:57:43     2020-01-13 01:16:23     1099         66070411
5      softReset      2020-01-10 20:02:52     2020-01-11 01:11:40     18527        66070212
6      softReset      2020-01-10 20:00:30     2020-01-10 20:02:29     118          66070212
7      softReset      2020-01-10 19:57:51     2020-01-10 19:59:56     124          66070212
8      softReset      2020-01-10 19:51:30     2020-01-10 19:52:53     82           66070212
9      hardReset      2020-01-10 19:25:23     2020-01-10 19:40:51     898          66070212
10     hardReset      2020-01-10 19:19:39     1970-01-01 00:00:00     0            66070212
11     hardReset      2020-01-10 19:13:51     1970-01-01 00:00:00     0            66070212
...
R-PHY#clear reset-history
```

Use the following command to clear the RPD reset-history: **clear reset-history:**

```
R-PHY#clear reset-history
```

RPD TACACS

The RPD TACACS (Terminal Access Controller Access-Control System) feature is supported from Cisco 1x2 / Compact Shelf RPD Software V7.2 and later. The RPD TACACS feature disables local access if the server is available.

When the TACACS server can be reached from RPD, you can only access the RPD by TACACS account. Local access will be disabled, and you cannot access RPD by local account. But if the TACACS server cannot be reached, for example, due to a wrong server address, network issue, or so on, you can then access RPD by local account.

TACACS is a security protocol that provides centralized validation of users who are attempting to gain access to a router or NAS. TACACS+, a more recent version of the original TACACS protocol, provides separate authentication, authorization, and accounting (AAA) services.

```
R-PHY(config)#tacacs add-server 10.0.0.113
Server '10.0.0.113' is configured on RPD successfully.
```

```
R-PHY(config)#tacacs add-key
Please add a secret key:
Please re-enter your secret key:
Add secret key successfully.
```

User can also delete server and change the secret key.

```
R-PHY(config)#tacacs delete-server 10.0.0.112
Delete server '10.0.0.112' successfully.
```

```
R-PHY(config)#tacacs change-key
Please change secret key:
Please re-enter your secret key:
Change secret key successfully.
```

To display the configured TACACS server, use the **show tacacs-server** command as shown in the following example:

```
R-PHY#show tacacs-server
TACACS server configured:
10.0.0.113
```

Feature Information for RPD Reset

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



Note

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

Table 68: Feature Information for RPD Reset

Feature Name	Releases	Feature Information
Factory reset support	Cisco 1x2 / Compact Shelf RPD Software 6.1	This feature was introduced on the Cisco Remote PHY Device.
Softreset support	Cisco 1x2 / Compact Shelf RPD Software 6.6	This feature was introduced on the Cisco Remote PHY Device.
RPD TACACS support	Cisco 1x2 / Compact Shelf RPD Software 7.2	This feature was introduced on the Cisco Remote PHY Device.
RPD Reset-history	Cisco 1x2 / Compact Shelf RPD Software 7.7	This feature was introduced on the Cisco Remote PHY Device.



CHAPTER 37

Archiving RPD Logs

Finding Feature Information

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

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

- [Hardware Compatibility Matrix for Cisco Remote PHY Device, on page 273](#)
- [Information About Archiving Logs, on page 274](#)
- [Archiving Logs Using SCP or TFTP, on page 274](#)
- [Archiving Logs Locally, on page 276](#)
- [Copying RPD Log Files using SCP, on page 277](#)
- [Feature Information for Archiving Logs, on page 277](#)

Hardware Compatibility Matrix for Cisco Remote PHY Device



Note Unless otherwise specified, the hardware components introduced in a given Cisco Remote PHY Device Software Release are supported in all subsequent releases.

Table 69: Hardware Compatibility Matrix for the Cisco Remote PHY Device

Cisco HFC Platform	Remote PHY Device
Cisco GS7000 Super High Output Node	Cisco 1x2 / Compact Shelf RPD Software 2.1 and Later Releases

Cisco HFC Platform	Remote PHY Device
Cisco GS7000 Super High Output Intelligent Node (iNode)	Cisco 1x2 / Compact Shelf RPD Software 4.1 and Later Releases Cisco Intelligent Remote PHY Device 1x2 <ul style="list-style-type: none"> • PID—iRPD-1X2= • PID—iRPD-1X2-PKEY=



Note The -PKEY suffix in the PID indicates units that enable the SCTE-55-2 Out-of-Band protocol support.

Information About Archiving Logs

You can archive logs to the SCP or TFTP server, or RPD itself.

When an RPD SSH session is closed during an RPD logging archive process, the RPD logging temp file is retained in the RPD file system. In this release, only the latest temp file is retained. The legacy temp files are removed.

Archiving Logs Using SCP or TFTP

To archive logs, use the **logging** command.

To transfer files to the TFTP server, use the **logging [provision-archive|1588-archive|corefile-archive] tftp server_ip save_path** command.

To transfer files to the SCP server, use the **logging [provision-archive|1588-archive|corefile-archive] scp server_ip user save_path** command.

To archive logs created during RPD provisioning to the SCP server, use the **logging provision-archive scp server_ip user save_path** command.

**Note**

- Use **provision-archive** to archive logs created during RPD provisioning.
- Use **1588-archive** to archive PTP logs.
- Use **corefile-archive** to archive logs created during system crashes.
- *user* is the username of the SCP or TFTP server account to which files are transferred.
- *save_path* is the relative path of the folder in the SCP or TFTP server. You must have write permission to access the folder. Make sure that the folder has sufficient space.
- *server_ip* can be IPv4 or IPv6 address. The server IP address type must be the same as the RPD IP address.
- For SCP file transfer, type the password of your server account when prompted. For TFTP file transfer, password is not required.
- RPD should be able to successfully ping the SCP or TFTP server. If the ping is unsuccessful, files are not archived.

This is an example of how to archive logs created during RPD provisioning to the SCP server.

```
R-PHY#logging provision-archive scp 198.51.100.1 <user> /tmp
Wait for archiving logs
Collect tech-support info...

Wait for upload archive to server. It would take 3 minutes or more.
RPD logs will be saved in
<user>@<server_ip>:~/<save_path>/RPD_PROV_10049fc20200_LOG_2018-08-20_00_12_22_419798.tar.gz

Host '<server_ip>' is not in the trusted hosts file.
(ssh-rsa fingerprint md5 b6:bb:d4:20:92:47:bb:29:d7:2c:5d:47:7a:a5:c6:8d)
Do you want to continue connecting? (y/n) y
<user>@<server_ip>'s password:
RPD_PROV_10049fc20200_LOG_2018-08-20_00_12_22 100% 61MB 1.9MB/s 00:32
[Done]
```

This is an example of how to archive PTP logs to the SCP server.

```
R-PHY#logging 1588-archive scp 198.51.100.1 <user> /tmp

wait for archiving 1588 logs
Wait for upload archive to server. It would take 3 minutes or more.
RPD logs are saved in
user@198.51.100.1:~/tmp/RPD_1588_0027900a0cf8_LOG_1977-01-08_21_26_05_222552.tar.gz

Host '198.51.100.1' is not in the trusted hosts file.
(ssh-rsa fingerprint md5 1d:9d:69:0c:17:1e:66:03:11:7e:ff:a3:c1:55:b1:a7)
Do you want to continue connecting? (y/n) user@198.51.100.1's password:
RPD_1588_0027900a0cf8_LOG_1977-01-08_21_26_05 100% 29 0.0KB/s 00:00
[Done]
```

This is an example of how to archive logs created during system crashes to the SCP server.

```
R-PHY#logging corefile-archive scp 198.51.100.1 <user> /tmp

wait for archiving corefile
```

```

Wait for upload archive to server. It would take 3 minutes or more.
RPD logs are saved in
user@198.51.100.1:/tmp/RPD_COREFILE_0027900a0cf8_LOG_1977-01-08_21_27_59_522646.tar.gz
jianyzha@198.51.100.1's password:
RPD_COREFILE_0027900a0cf8_LOG_1977-01-08_21_2 100% 9126KB 8.9MB/s 00:01
[Done]

```

This is an example of how to archive logs created during RPD provisioning to the TFTP server.

```

R-PHY#logging provision-archive tftp 198.51.100.1 .

wait for archiving logs
Collect tech-support info...

wait for upload archive to server
RPD provision logs are saved in
198.51.100.1:$TFTP_DIR/./RPD_0027900a0cf8_LOG_1977-01-08_18_20_10_509660.tar.gz
[Done]

```

This is an example of how to archive PTP logs to the TFTP server.

```

R-PHY#logging 1588-archive tftp 198.51.100.1 .

wait for archiving 1588 logs
Wait for upload archive to server. It would take 3 minutes or more.
RPD logs are saved in
198.51.100.1:$TFTP_DIR/./RPD_1588_0027900a0cf8_LOG_1977-01-08_21_25_26_352484.tar.gz
[Done]

```

This is an example of how to archive logs created during system crashes to the TFTP server.

```

R-PHY#logging corefile-archive tftp 198.51.100.1 .

wait for archiving corefile
Wait for upload archive to server. It would take 3 minutes or more.
RPD logs are saved in
198.51.100.1:$TFTP_DIR/./RPD_COREFILE_0027900a0cf8_LOG_1977-01-08_21_27_37_782555.tar.gz
[Done]

```

Archiving Logs Locally

Starting from Cisco 1x2 / Compact Shelf RPD Software 7.3, user can save a log archive to **/rpd/archive** on the RPD using the command **logging [provision-archive|1588-archive|corefile-archive] local**. This archive can then be transferred or viewed locally.



Note

- Use **provision-archive** to archive logs created during RPD provisioning.
- Use **1588-archive** to archive PTP logs.
- Use **corefile-archive** to archive logs created during system crashes.

```

R-PHY#logging provision-archive local
Collect tech-support info...
Please wait, archiving...
Created archive: /rpd/archive/RPD_PROV_badbad13ac3e_LOG_2019-08-28_11_59_01_898484.tar.gz
Created archive: /rpd/archive/RPD_running_log.tar.gz

```



```
Created archive: /rpd/archive/RPD_config_log.tar.gz
[Done]
```

Copying RPD Log Files using SCP

Remotely retrieving log files from the RPD via SCP is supported starting from Cisco 1x2 / Compact Shelf RPD Software 7.3 release. For security reasons, the SCP support would be limited to specific directories that contain the log files and only certain types of files under these directories. Only files from /tmp/, /rpd/, /rpd/archive/, /rpd/log/, and /rpd/log/<logname>.log/ are allowed. Filename must include one of: 'log', '.gz', or '.pcap'. This feature will only allow copying-out of files and will not allow copying-in of files to the RPD.

Feature Information for Archiving Logs

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



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

Table 70: Feature Information for Archiving Logs

Feature Name	Releases	Feature Information
Archiving Logs	Cisco 1x2 / Compact Shelf RPD Software 6.1	This feature was introduced on the Cisco Remote PHY Device.
SCP Support to Copy RPD Logfiles	Cisco 1x2 / Compact Shelf RPD Software 7.3	This feature was introduced on the Cisco Remote PHY Device.
Support for Local Archive	Cisco 1x2 / Compact Shelf RPD Software 7.3	This feature was introduced on the Cisco Remote PHY Device.



CHAPTER 38

SSH Account Management

Finding Feature Information

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

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

- [Hardware Compatibility Matrix for Cisco Remote PHY Device, on page 279](#)
- [Information About SSH Account Management, on page 280](#)
- [Configure SSH Account Management, on page 280](#)
- [Feature Information for SSH Account Management, on page 281](#)

Hardware Compatibility Matrix for Cisco Remote PHY Device



Note Unless otherwise specified, the hardware components introduced in a given Cisco Remote PHY Device Software Release are supported in all subsequent releases.

Table 71: Hardware Compatibility Matrix for the Cisco Remote PHY Device

Cisco HFC Platform	Remote PHY Device
Cisco GS7000 Super High Output Node	Cisco 1x2 / Compact Shelf RPD Software 2.1 and Later Releases
Cisco GS7000 Super High Output Intelligent Node (iNode)	Cisco 1x2 / Compact Shelf RPD Software 4.1 and Later Releases Cisco Intelligent Remote PHY Device 1x2 <ul style="list-style-type: none">• PID—iRPD-1X2=• PID—iRPD-1X2-PKEY=



Note The -PKEY suffix in the PID indicates units that enable the SCTE-55-2 Out-of-Band protocol support.

Information About SSH Account Management

Manage your SSH account for an RPD SSH login. This feature enables you to add, delete, and change password of an SSH account.

Configure SSH Account Management

Add, delete, or modify your SSH account. You can also view your account details.

Add a New SSH Account



Note You can add a maximum of ten accounts at a time.

To add a new SSH account, run the **ssh adduser <newuser>** command. This example shows how to add a new SSH account.

```
R-PHY>enable
R-PHY#configure terminal
R-PHY(config)#ssh adduser <newuser>
Changing password for <newuser>
New password:
Retype password:
Password for <newuser> changed by root
R-PHY(config)#end
```

Delete an SSH Account



Note You cannot delete the last account.

To delete an SSH account, run the **ssh delete <newuser>** command. This example shows how to delete an SSH account.

```
R-PHY>enable
R-PHY#configure terminal
R-PHY(config)#ssh delete <newuser>
Warning: Are you sure to delete this account? [No/Yes]
Yes
delete account '<newuser>' successfully
R-PHY(config)#end
```

Change an SSH Account Password

To change an SSH account password, run the `ssh chpasswd <user>` command. This example shows how to change an SSH account password.

```
R-PHY>enable
R-PHY#configure terminal
R-PHY(config)#ssh chpasswd <user>
Please enter password for '<user>':
Please re-enter your password:
Password for '<user>' changed
R-PHY(config)#end
```

View SSH Account Details

To view an SSH account details, run the `show ssh account` command. This example shows how to view an SSH account details.

```
R-PHY#show ssh account
Account Num: 2
Current SSH Accounts:
admin
user
```

Feature Information for SSH Account Management

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



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

Table 72: Feature Information for SSH Account Management

Feature Name	Releases	Feature Information
SSH Account Management	Cisco 1x2 RPD Software 6.1	This feature was introduced on the Cisco Remote PHY Device.

