Cisco Remote PHY System Startup Configuration for Cisco 1x2 / Compact Shelf RPD Software 10.x

First Published: 2021-07-30

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

© 2012 Cisco Systems, Inc. All rights reserved.

CONTENTS

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 4
- Network Topologies 5
  - Daisy Chain Architecture 5

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 Dying Gasp 11
  - Configuring PTP 13
  - Configuring cBR-8 14
  - Setting Device Alias 15
- Updating the Default RPD Password 16

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 20
Configuring Switch 21
Verifing 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
Configuring DEPI Statistics Synchronization Interval 38
Feature Information for DEPI/UEPI/L2TP integration with RPD 39

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 46
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

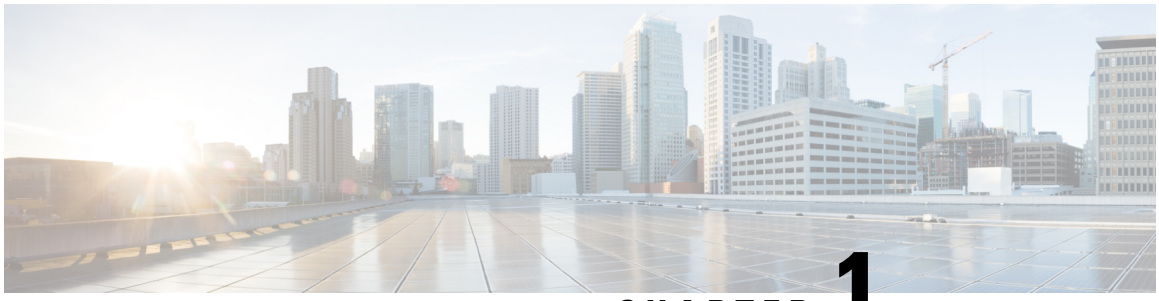
Example: GCPP Configuration 52
Feature Information for GCPP Support 52

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



CHAPTER 1

Cisco Remote PHY System Overview

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

- 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 4
- 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 • 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-G2-R—This line card with no downstream and upstream PHY modules 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
- 50 gigabit DOCSIS traffic bandwidth when connected with the Cisco CBR-CCAP-LC-G2-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

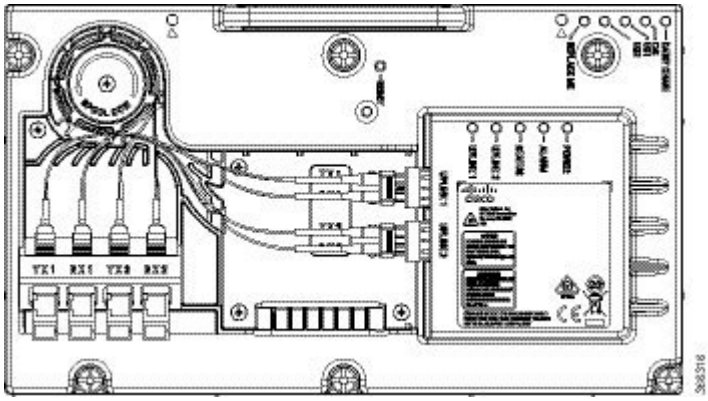
Cisco Remote PHY Device

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.

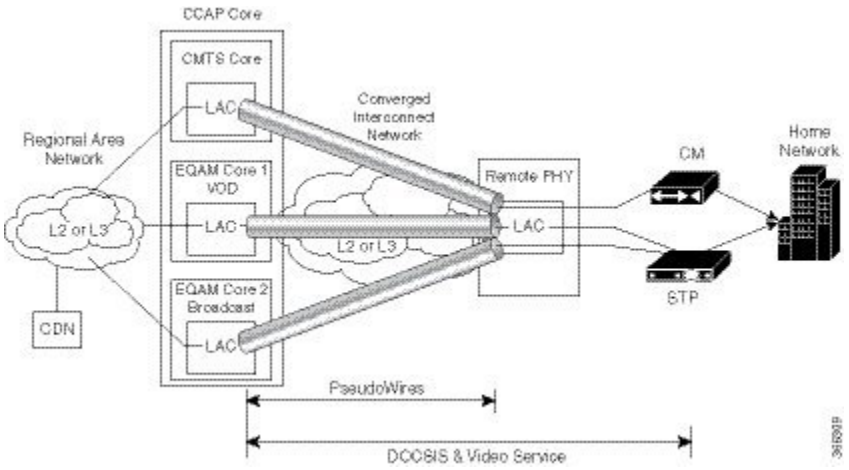
Figure 1: Cisco RPD



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.

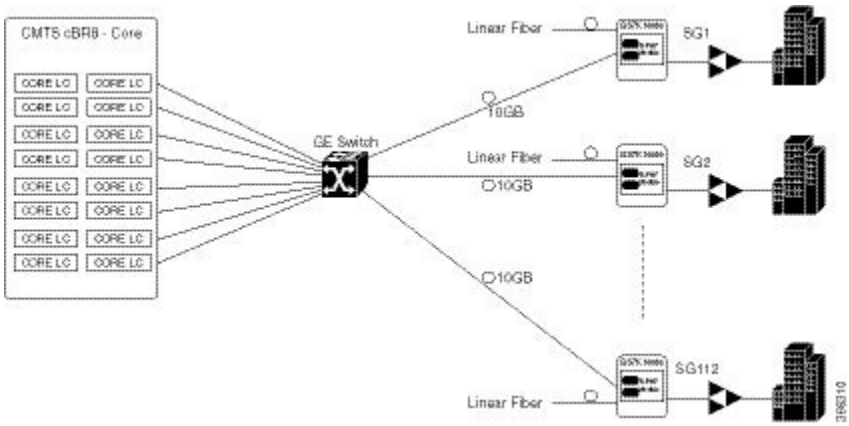
Figure 2: Single Controller Sharing Architecture



Network Topologies

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

Figure 3: Standard Deployment



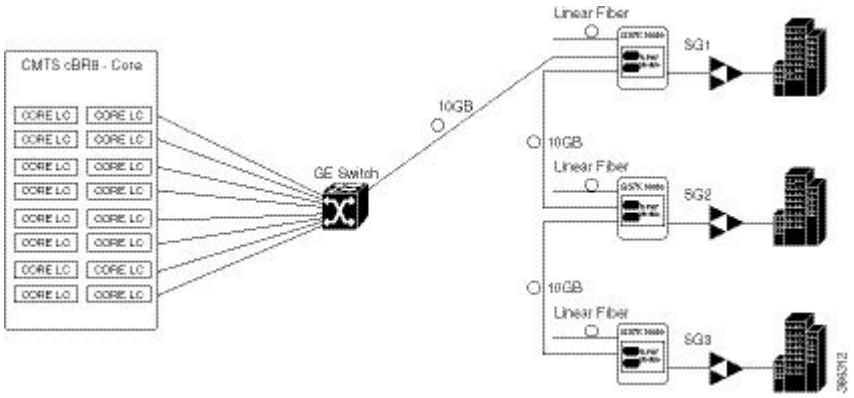
Note If you want to establish Equal-Cost Multi-Path (ECMP) connection between cBR-8 and RPD, pay attention to the ECMP configuration on both cBR-8 and the Converged Interconnect Network (CIN) routers. The number of maximum paths configured must be equal as or larger than the number of ECMP paths you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

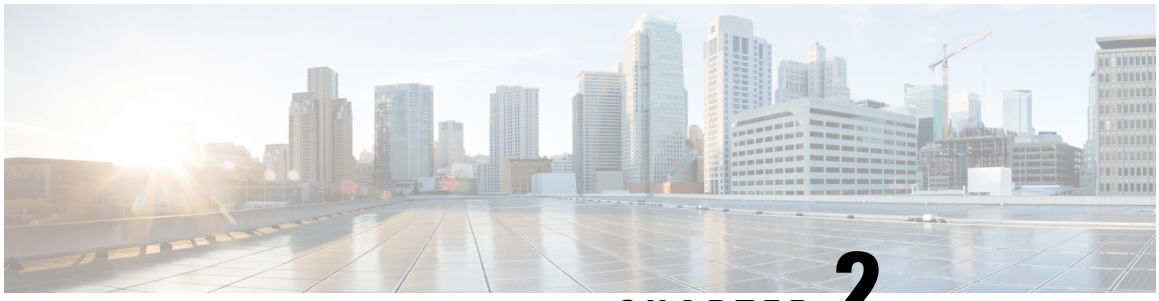
notified about the chain topology because before the RPD sets up a GCP connection, notification flow is not configured.

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 reprograming 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

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

- 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 16

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 • 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.

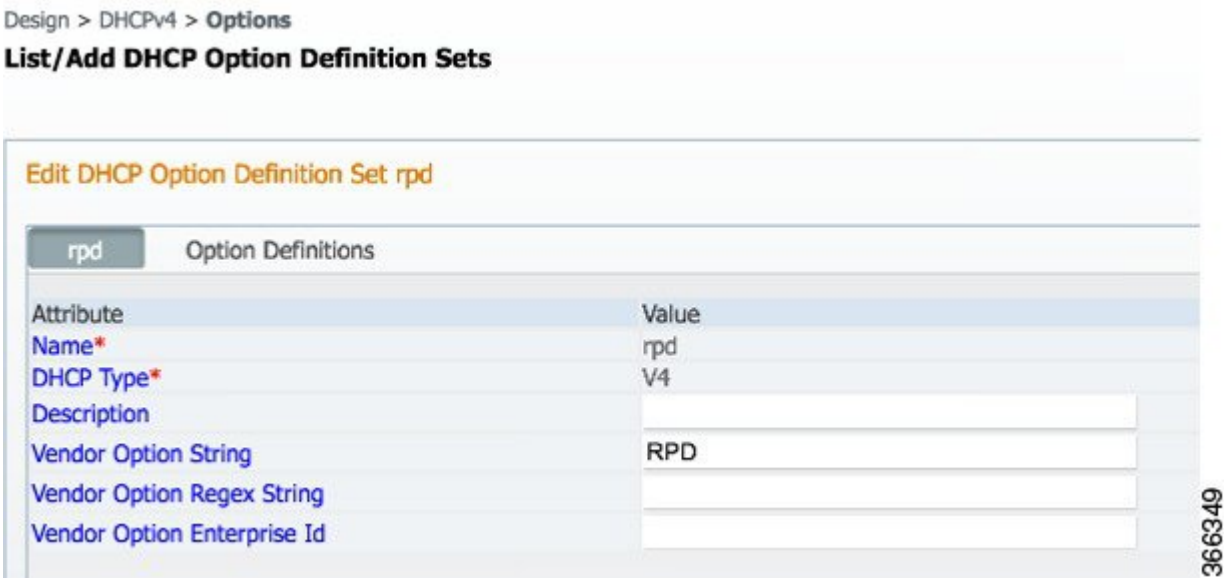
Configuring DHCP Server

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

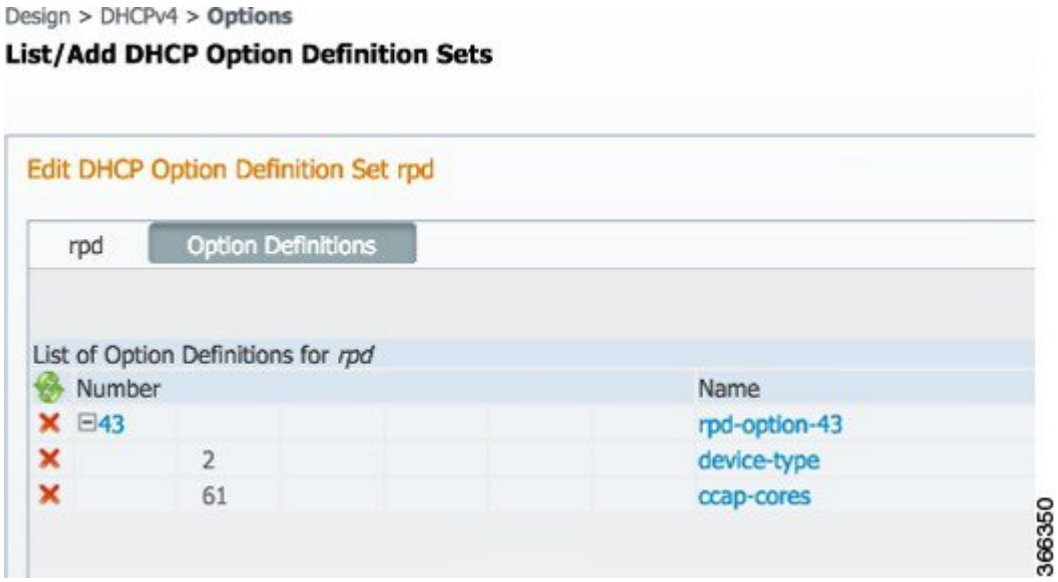
Configuring DHCP Server using IPv4

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

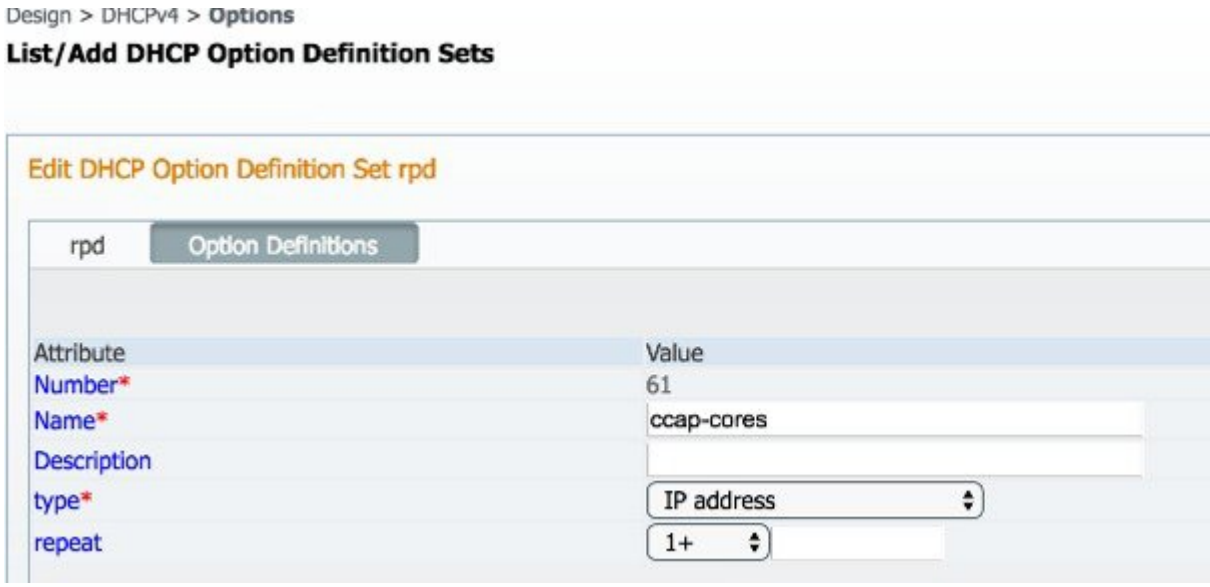
1. Add option for CCAP-Core. Fill in the name, DHCP type, and vendor option string as shown in the figure below.



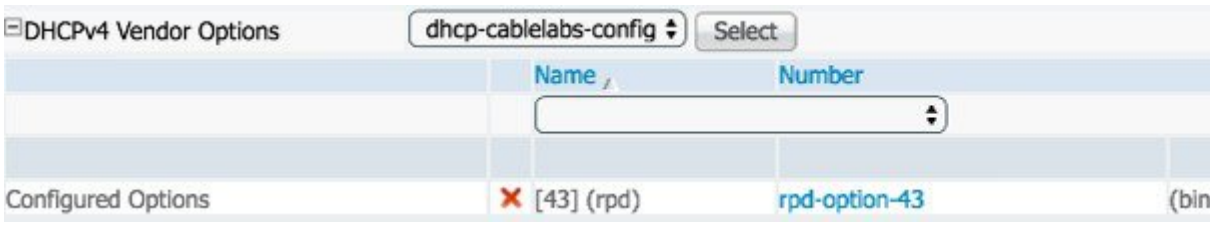
2. Define option. Fill in the option number and name as shown in the figure below.



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



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.

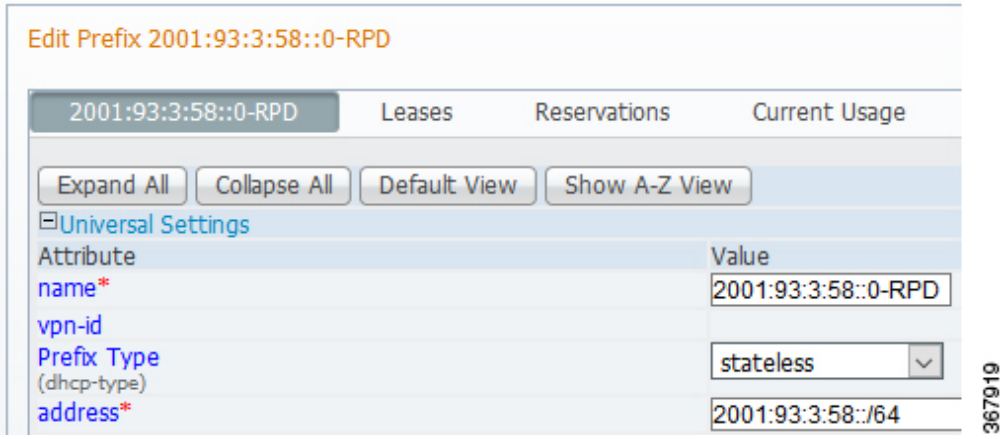


Configuring DHCP Server using IPv6 Stateless

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.

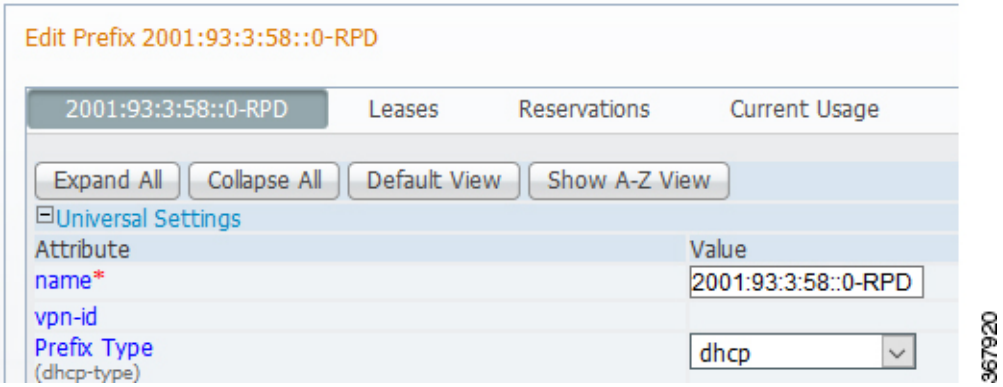
```
R-PHY#show dhcp
Interface  IP-Address                          Subnet-Mask
vbh0       2001:93:3:58:1204:9fff:fec1:100  ffff:ffff:ffff:ffff::

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 Dying Gasp

Cisco RPD 8.4 supports the Dying Gasp feature, allowing you to receive a UDP syslog message notification when a Node RPD loses power.

Dying Gasp is enabled by default on RPD firmware version 8.4 or later, and if the power-controller firmware is at version 2.05 or later.

To enable Dying Gasp, ensure that the default power-controller firmware is version 2.05 or later.

A syslog message example is as follows:

```
Feb 14 17:06:37 SYSTEM.CRITICAL 2020-02-14 22:08:30
POWER OFF ALARM NOTIFICATION; RPD-ID: 00:01:02:03:04:05
```

The RPD sends multiple copies of the message to the syslog server as it loses power. This ensures that the syslog server recieves the notification.

Complete the following steps to configure Dying Gasp:

1. Configure the Node RPD syslog server information through the DHCP server.

   Ensure that you use a valid IP address for the syslog server that is reachable from the RPD. An invalid IP address can cause loss of service.

2. Update Node RPD power controller firmware to version V2.05. Run the following CLI on the RPD to update the power controller firmware:

   ```
   firmware power-controller [update|version|verify]
   ```

   For example:

```
R-PHY# firmware power-controller
update               update adm1260 firmware
verify               verify the firmware in chip
version              show adm1260 firmware version


R-PHY# firmware power-controller version
chip 0: version:V2.03
chip 1: version:V2.03
chip 2: version:V2.03
```

The **firmware power-controller verify** verification function compares the power-controller firmware with the current RPD release.

```
R-PHY# firmware power-controller verify
Verify input Ihex file for chip 0: OK
Verify input Ihex file for chip 1: OK
Verify input Ihex file for chip 2: OK
Successful verification of /firmware/Adm1260_v2_05.hex, checking firmware version next
chip 0: version:V2.05 file 0: version:V2.05
chip 1: version:V2.05 file 1: version:V2.05
chip 2: version:V2.05 file 2: version:V2.05
chip 0, verifying eeprom: OK
chip 1, verifying eeprom: OK
chip 2, verifying eeprom: OK

R-PHY#


R-PHY#firmware power-controller update
Verify input Ihex file for chip 0: OK
Verify input Ihex file for chip 1: OK
Verify input Ihex file for chip 2: OK
Successful verification of /firmware/Adm1260_v2_05.hex, checking firmware version next
chip 0: version:V2.03 file 0: version:V2.05
chip 1: version:V2.03 file 1: version:V2.05
chip 2: version:V2.03 file 2: version:V2.05
Warning, if you choose to continue, you must maintain power on for at least 30 seconds

Are you sure to continue with firmware update? [No/Yes]Yes
chip 0, erasing eeprom
chip 0, programming eeprom
chip 1, erasing eeprom
chip 1, programming eeprom
chip 2, erasing eeprom
chip 2, programming eeprom
chip 0, verifying eeprom: OK
chip 1, verifying eeprom: OK
chip 2, verifying eeprom: OK
all done

R-PHY#
```

The update process takes less than 30 seconds. The RPD might turn unusable if it loses power, is reset, or rebooted during this process. Replace the RPD when it becomes unusable.

Note When the RPD detects drop in input power, it sends a syslog message to the configured syslog server (Step 1). This drop in power may be the first stage of a complete power failure, or a partial temporary reduction in total system capacity. The RPD continues to send the syslog message in either case.

3. Check the version and verify using the **firmware power-controller verify** command to see that the power-controller is running version 2.05 or later.

If the firmware is already up to date, the update process terminates without overwriting. If the command fails for any reason, run the command again before power cycling or rebooting the RPD. Failure to program completely before power cycling may result in an unusable RPD.

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 minislot-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 Srate   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 AAAAB3NzaC1yc2EAAAABIwAAAgEAtQCXVFmRIwemejbTx0+U8taMq5n4Zetu
71xb+dtHV8Rr0wejiK1YJkT93n9hcBxsjHRu76bLp99l+DDNL3+THljwnMQC1CsdvRmGXoe
Gf1mT9aTlGDf/ RW9ZywY9t8Kep9VnANu2DWSoh0wg2pE49HFOJAbGfuFOvPEdwZGGDMQNWs
Eq/3xAQjBxajQqfgu4IqjVzKoo4PM/xx9X4Z1aMwxS3DvyN7L8O0o33mcDNsasl3SslIjMSNfq
YpwOFvQve8c2onrYHUx2p3BwQOb/b0FzFQhZMTBXm/pDMXq/fkkD0uguk1xOGnqAATMJsSHIN
0UOdvbzhhmrFRBBM4NzqQG5kNt7KvnWgxE7HdalERvMyBC2MCGbFSHmQFyWmHBHPPmLIxK98W
XutoR8fzzs+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
EEEAAAABIwAAAgErP3nFp0v0k3Nf4UvSTuOOQi2h0mAfAtQCXVFmRIwemejbTx0+U8taM
q5n4Zetu71xb+dtHV8Rr0wejiK1YJkT93n9hcBxsjHRu76bLp99l+DDNL3+THljwnMQC1
CsdvRmGXoeGf1mT9aTlGDf/YfKxZMozMnR9qlGJFXlRAwGMsCRlllnV6IkFyh59P9Udkd
SSWv+QL8lCftWBmMnyt/CkqL98NK0Vp0gIYRv7UKCwhK40c8X7PhzxCmKVFTUv3bf9VIP
NA2esgzKDFpoJZkqCjrnXU1Xu0Oj8Twci7f0ytSrFxVKuWp4XZbVDpWGH90BOQR8gKHmq
urP3nFp0v0k3Nf4UvSTuOOQi2h0mAf+9wzm+ab41ToadUbMawHyFYyuU= xxx@xxx.xxx.com
R-PHY(config)#end
```

```
R-PHY#show ssh nms-pubkey ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAgEAtQCXVFm
RIwemejbTx0+U8taMq5n4Zetu71xb+dtHV8Rr0wejiK1YJkT93n9hcBxsjHRu76bLp99l
+DDNL3+THljwnMQC1CsdvRmGXoeGf1mT9aTlGDf/YfKxZMozMnR9qlGJFXlRAwGMsCRll
lnV6IkFyh59P9UdkdSSWv+QL8lCftWBmMnyt/CkqL98NK0Vp0gIYRv7UKCwhK40c8X7Ph
zxCmKVFTUv3bf9VIPNA2esgzKDFpRvMyBC2MCGbFSHmQFyWmHBHPPmLIxK98WXutoR8fzz
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

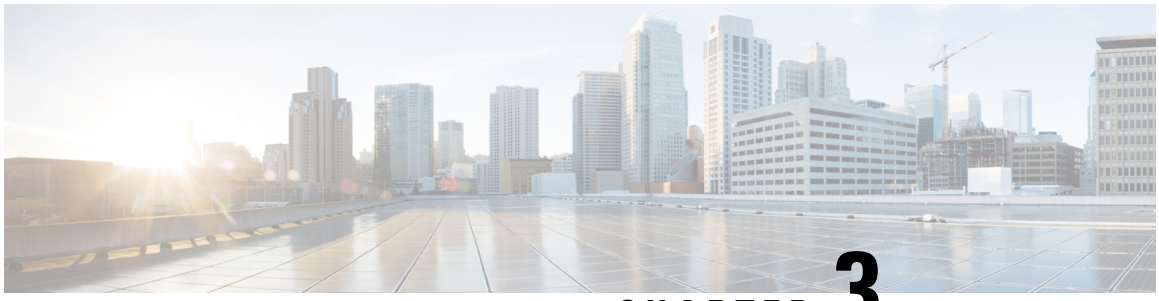
```
R-PHY#config terminal
R-PHY(config)#ssh chpasswd admin
Please enter password for 'admin':
Please re-enter your password:
chpasswd: password for 'admin' changed

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.

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

- 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 GS7000 Super High Output Intelligent Node (iNode)	Cisco 1x2 / Compact Shelf RPD Software 4.1 and Later Releases Cisco Intelligent Remote PHY Device 1x2 • 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:

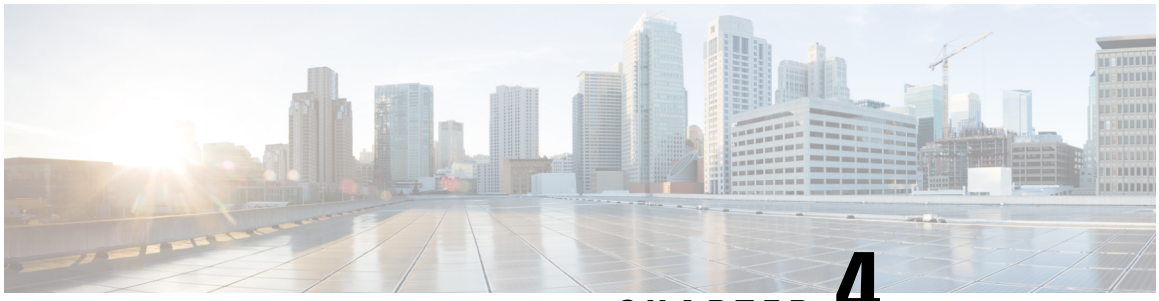
```
authentication port-control auto
dot1x pae authenticator
```

Verifing 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
bssid=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=0d53798f5b46014cc92a4ac1151521bae6a14c98f919eb5e8c81a701b7272be7f812e7e5a75881768d74d311795a3b1f0e37bfa7fff7dcc4685d36f216bec59850
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 • 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) subordinate mode, in which the PTP suborinate ports are from the backhaul 10 GE 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 subordinate 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 unware 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 packets0-7(-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 ipccl log-history 0
platform punt-policer 10 10
platform punt-policer 10 10 high
platform punt-policer 80 10
platform punt-sbrl 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 Lo1588 negotiation
  clock source 10.10.10.11
  clock source 192.168.0.0
 clock-port master-local master
  transport ipv4 unicast interface Lo1588 negotiation
!
-----
r-dti 2
 rpd-event profile 0
 rpd-55d1-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 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
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
```

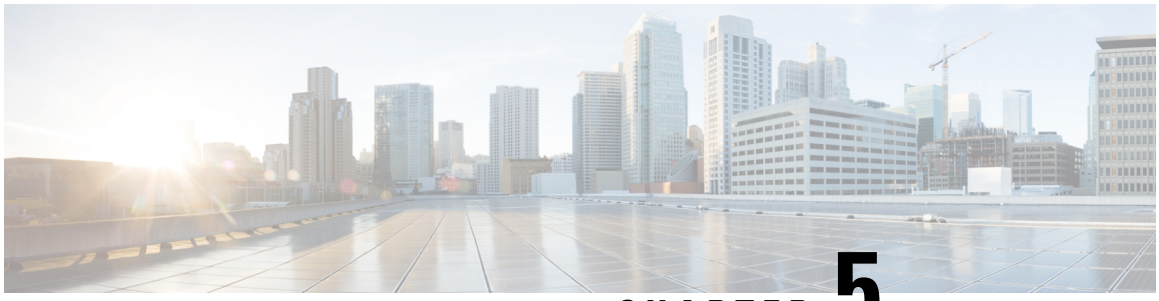
Feature Information for Synchronizing Time on R-PHY Devices

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 https://cfnng.cisco.com/ 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.

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

- 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 39

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 • 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 MHAv2 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 MHAv2 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 Te1/1/7
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 Te1/1/7
  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-55d1-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    Te1/1/0  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.

Configuring DEPI Statistics Synchronization Interval

In Cisco cBR-8 router, the DEPI statistics is synchronized from cdman (us-schedular) to IOSd. The previous synchronization interval is 15 seconds, which consumes extra CPU resources and may impact the overall cBR-8 system performance. Starting from Cisco IOS XE Amsterdam 17.3.1z, the default DEPI statistics synchronization interval is set to 60 seconds to reduce the CPU usage of the synchronization process. You can also configure the interval by using **cable rphy statistics session update-freq** command in global configuration mode to accommodate your specific needs. But Cisco recommends the default setting unless a change is requested by a Cisco service representative for a particular topology or use case. You must keep in mind that never use short interval in large scale deployment to avoid high CPU usage.

Use the following command to configure the DEPI statistics synchronization interval. This command is applied on all the CLC cards.

```
Router(config)#cable rphy statistics session update-freq 20
```

To verify the DEPI statistics synchronization interval configuration, use the following procedure as an example:

```
Router#sh run | in update-freq
cable rphy statistics session update-freq 20
```

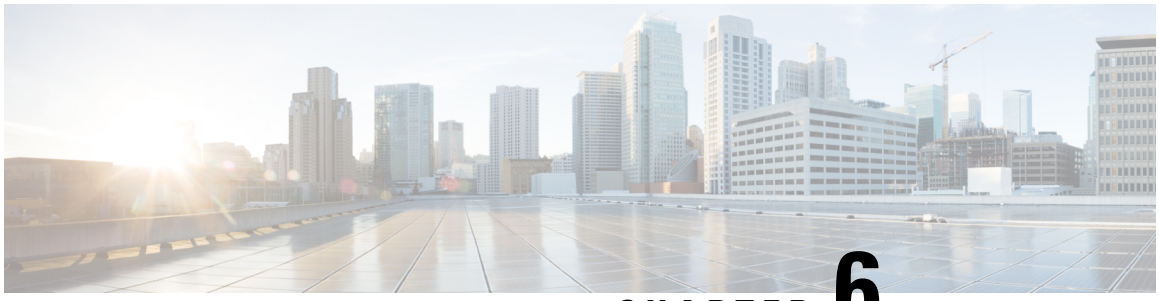
Feature Information for DEPI/UEPI/L2TP integration with RPD

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 https://cfnng.cisco.com/ 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.

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

- 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 • 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
```

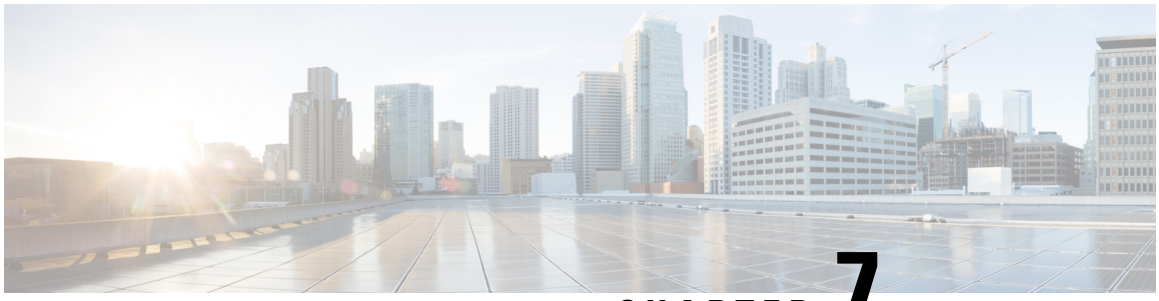
Feature Information for DLM

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 https://cfnng.cisco.com/ 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.

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

- 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 GS7000 Super High Output Intelligent Node (iNode)	Cisco 1x2 / Compact Shelf RPD Software 4.1 and Later Releases Cisco Intelligent Remote PHY Device 1x2 • 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 mutiple 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 downstram 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
```

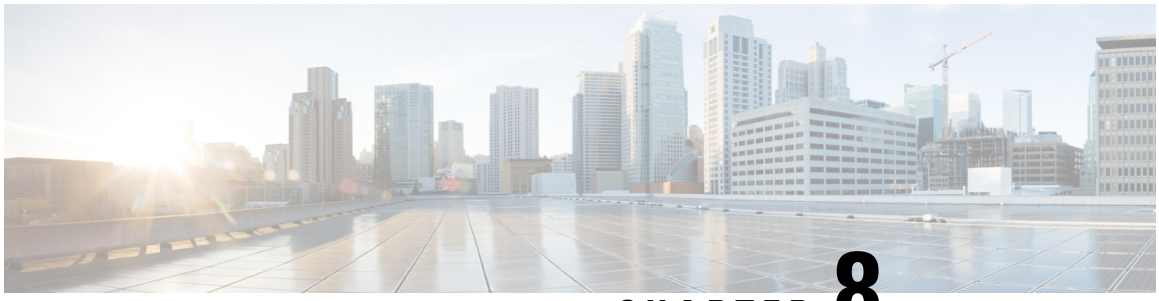
```
services below */
Router(config-rpd-core)# principal   /* Specify the principal core */
Router(config-rpd-core)# rpd-ds 0 controller downstream-cable 3/0/0 profile 100 /* DS docsis
 channel config*/
Router(config-rpd-core)# rpd-ds 0 controller downstream-cable 3/0/1 profile 200 /* DS docsis
 channel 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-55d1-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     Te1/1/6   online       Pri   Act  node
0004.9f00.0907  120.100.2.20     Te1/1/0   online       Aux  Act  node
0004.9f00.0907  120.100.2.20     Te1/1/1   online       Aux  Act  node
0004.9f00.0907  120.100.2.20     Te1/1/2   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.

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

- 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

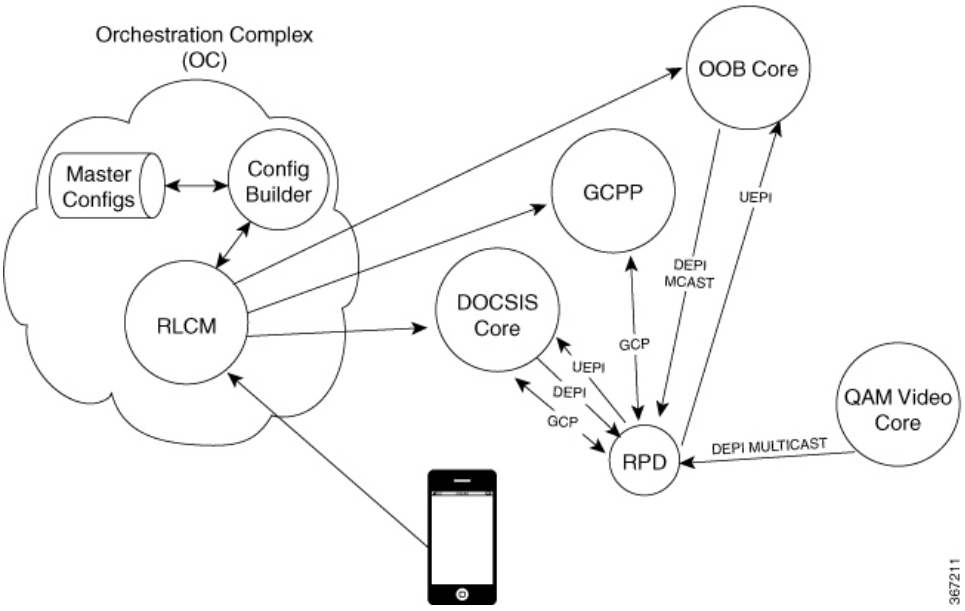
Information About GCPP Support

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 • 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 p1_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
```

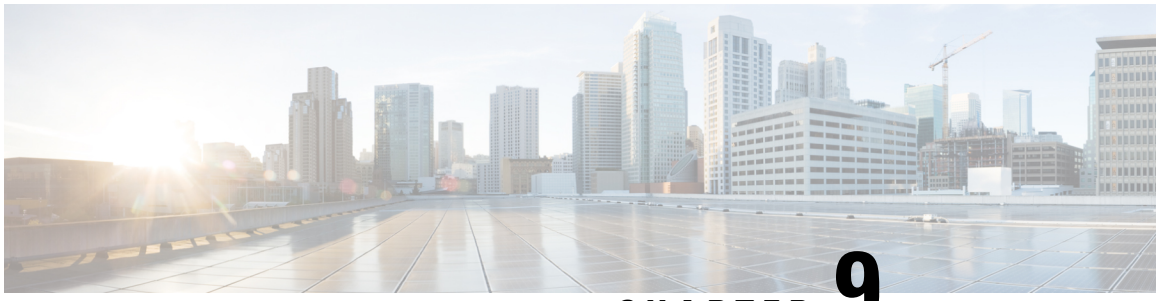
Feature Information for GCPP Support

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 https://cfnng.cisco.com/ 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.

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

- 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   onlisssne    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
```

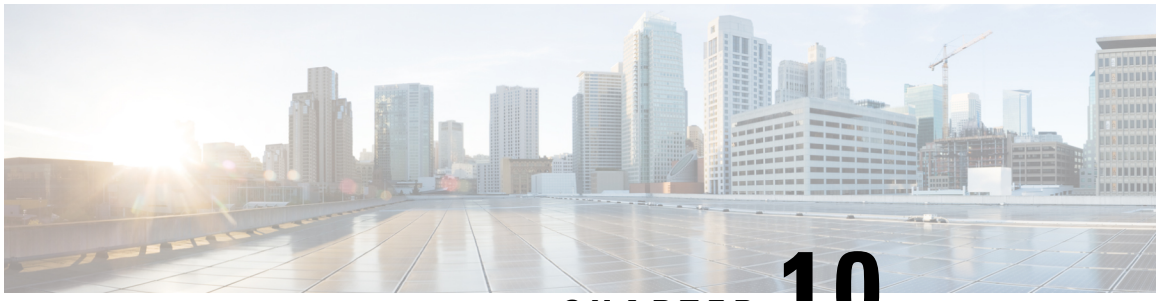
Feature Information for IKEv2 Mutual Authentication

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 https://cfnng.cisco.com/ 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.

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

- 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 • 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 powel 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

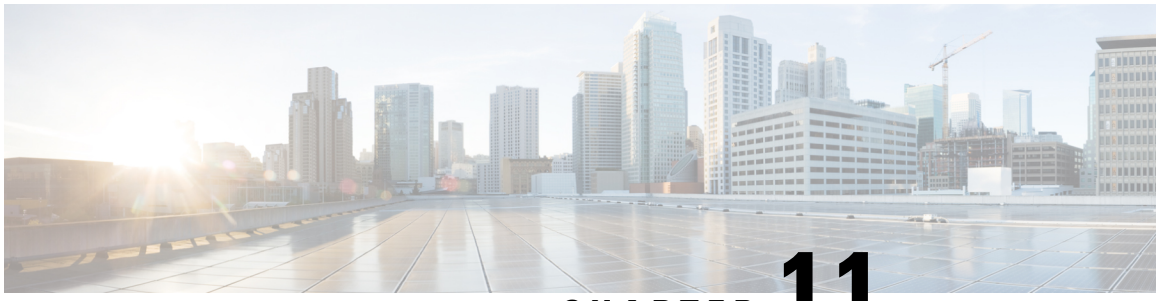
```
configure terminal
cable rpd name
rpd-ds port rf-channel number power-adjust value
```

This is an example of RF channel power 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.

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

- 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 • 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
```

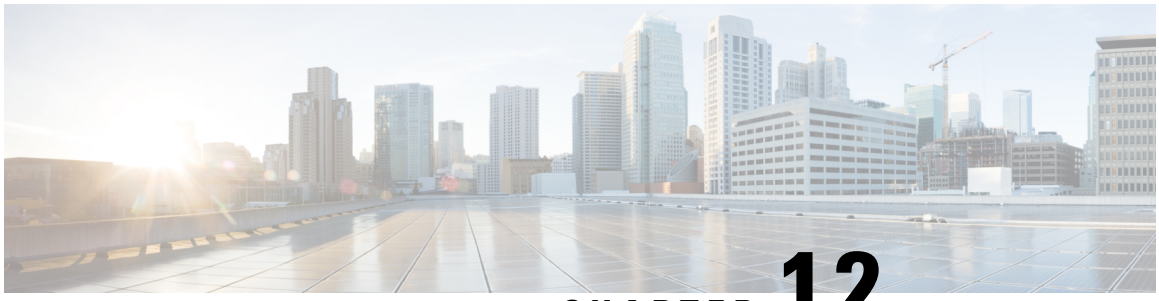
Feature Information for LLDP

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 https://cfnng.cisco.com/ 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 • 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.