Cisco Remote PHY System Bring Up

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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

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.

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

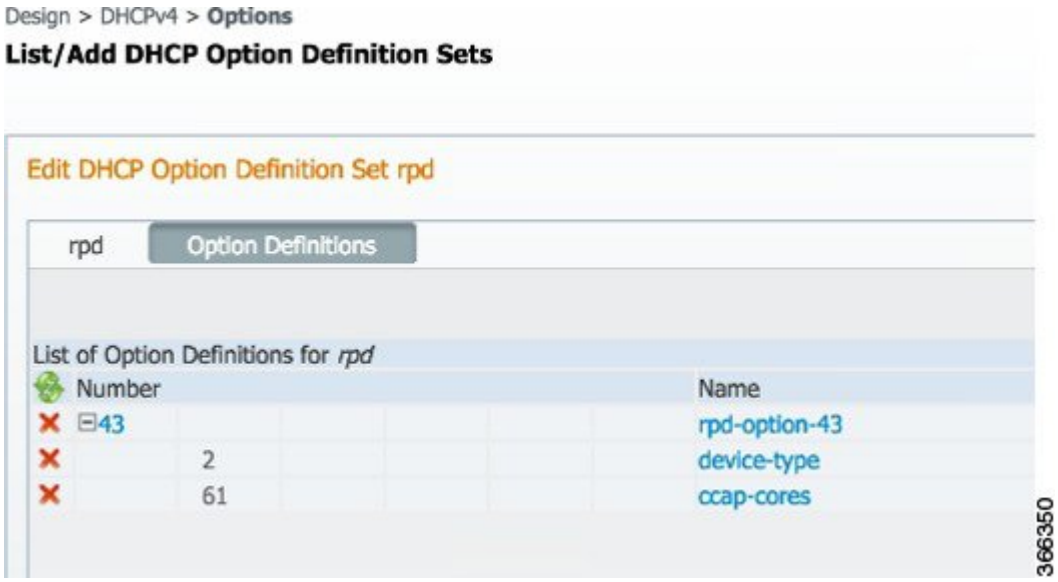
You can choose to configure the DHCP server using any of the following methods.

Configuring DHCP Server using IPv4

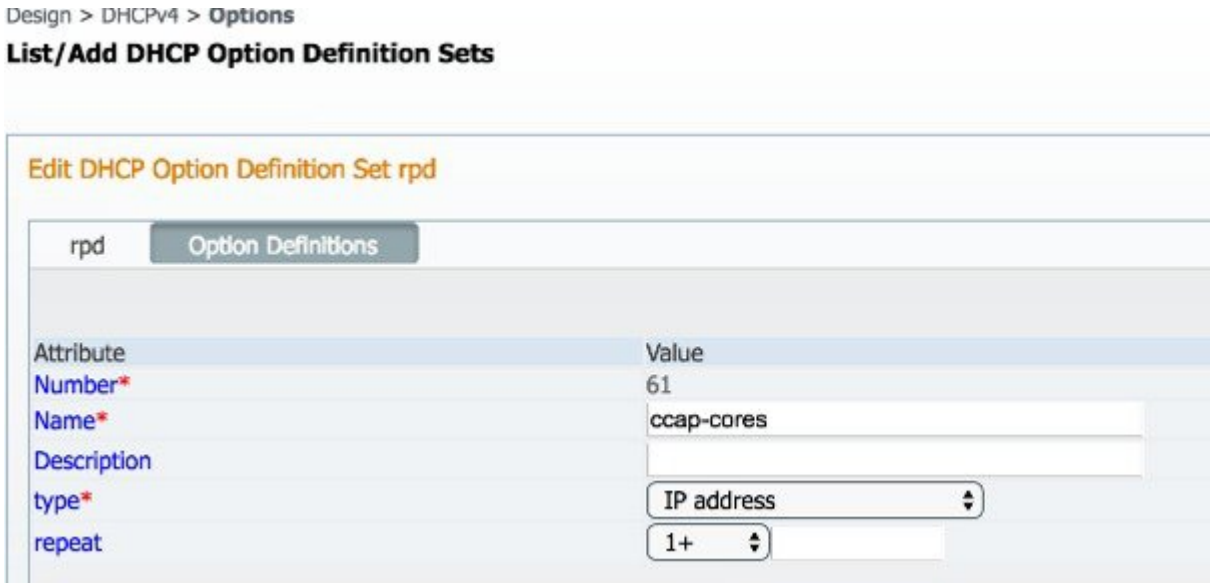
To configure DHCP server using IPv4, follow the steps below:

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

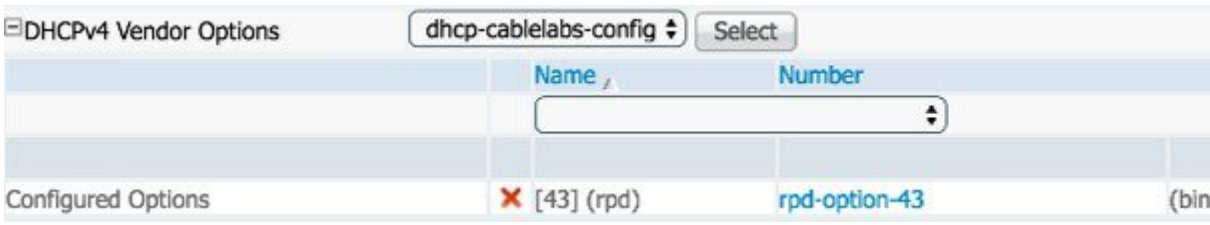
2. Define option. Fill in the option number and name as shown in the figure below.



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.

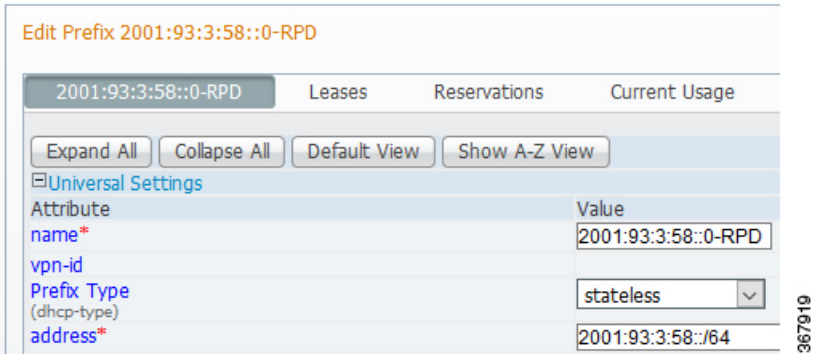


Configuring DHCP Server using IPv6 Stateless

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 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
```

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
```