Cisco Remote PHY Device Management Guide for Cisco 1x2 / Compact Shelf RPD Software 9.x

First Published: 2020-09-30

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

© 2020 Cisco Systems, Inc. All rights reserved.

CONTENTS

CHAPTER 1

Secure Software Download

This document describes how to upgrade software from RPD and Cisco cBR by using Secure Software Download feature.

Hardware Compatibility Matrix for Cisco Remote PHY Device

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 Secure Software Download

The secure software download (SSD) feature allows you to authenticate the source of a code file and verify the downloaded code file before using it in your system. The SSD is applicable to Remote PHY (R-PHY) devices installed in unsecure locations.

The Remote PHY architecture allows RPDs to download code. Hence, authenticating the source and checking the integrity of the downloaded code is important.

To authenticate and verify downloading of the code, SSD helps in verifying the manufacturer signature and the operator signature, if any. The manufacturer signature affirms the source and integrity of the code file to the RPD. If an additional signature is available from the operator, the RPD verifies both signatures with a certificate chain before accepting a code file.

Prerequisites for Upgrading Software using SSD

The following prerequisites are applicable to upgrading RPD software using SSD:

- The R-PHY node supports downloading software initiated through the GCP message sent from Cisco cBR.
- RPD supports a secure software download initiated using SSH and CLI directly on the RPD.
- R-PHY uses TFTP or HTTP to access the server to retrieve the software update file.

How to Upgrade Software from RPD and Cisco cBR Using SSD

Initiating RPD Software Upgrade from Cisco cBR

The RPD software upgrade can be initiated from Cisco cBR-8 Router. Use the following commands for initiating the upgrade:

```
cable rpd {all|oui|slot|RPD IP|RPD MAC} ssd server_IP {
            tftp|http} file_name [c-cvc-c|m-cvc-c]
                [CVC Chain File Name]
```

Initiating Software Upgrade from RPD Using SSD

If you want to initiate the software upgrade from RPD, set the SSD parameters on RPD. Use the following commands.

Setting the value for SSD CVC (Manufacturer's and Co-signer Code Validation Certificates) parameter is optional.

Configure the values for the following parameters

- SSD server IP address
- Filename

- Transport method

```
ssd set server server_IP filename file_name transport {tftp|http}
ssd set cvc {manufacturer|co-signer} cvc_chain_file_name
ssd control start
```

Verifying Software Upgrade Using SSD Configuration

To display the RPD SSD status, use the **cable rpd [all|oui|slot|RPD IP|RPD MAC] ssd status** command as given in the following example.

```
Router# cable rpd all ssd status
RPD-ID         ServerAddress Protocol Status            Filename
0004.9f00.0591 192.0.2.0     TFTP     ImageDownloading
image/RPD_seres_rpd_20170216_010001.itb.SSA
0004.9f00.0861 192.0.2.2     TFTP     CodeFileVerified
userid/RPD_seres_rpd_20170218_010001.itb.SSA
0004.9f03.0091 192.0.2.1    TFTP    ImageDownloadFail chuangli/openwrt-seres-rpd-rdb.itb.SSA
```

The available statuses are the following:

- CVCVerified
- CVCRejected
- CodeFileVerified
- CodeFileRejected
- ImageDownloading
- ImageDownloadSucceed
- ImageDownloadFail
- MissRootCA

Examples for Upgrading HA RPHY Software

See examples for the software upgrade from cBR-8 and FCC or Primary eRPD.

Example: HA RPHY Software Upgrade from Cisco cBR

```
Router# upgrade set server 203.0.113.1 filename bundle/test.itb.sign transport http
Router# upgrade control show config

file path: bundle/test.itb.sign
server: 203.0.113.1
transport: HTTP
Router# upgrade control start
Router# upgrade control show status.
Downloading image on FCC.



Router# cable rpd group all upgrade 203.0.113.2 http bundle/test.itb.sign
```

```
Router# cable rpd group all upgrade status
This group 0027.900a.4c1a is not HA-Shelf group.
GROUP-ID: 7abd.44a1.0000
ServerAddress: 203.0.113.2
Protocol: HTTP
Status: Image downloading on RPDLC
Filename: bundle/test.itb.sign
```

Example: HA RPHY Software Upgrade from FCC or Primary eRPD

```
Router# upgrade set server 203.0.113.2 filename bundle/test.itb.sign transport http
Router# upgrade control start
Router# upgrade control show status
Downloading image on FCC.
Router# upgrade control abort
Abort software upgrade process successfully.
Router# upgrade control show status
Image download aborted.
```

```
Router# show cable rpd-upgrade group all status
GROUP-ID: 7abd.44a1.0000
ServerAddress: 203.0.113.2
Protocol: HTTP
Status: Idle
Filename: bundle/test.itb.sign
```

Feature Information for Secure Software Download

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

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

Table 2: Feature Information for Secure Software Download

Feature Name	Releases	Feature Information
Upgrade Software Image	Cisco Smart PHY 7200	This feature was introduced on the Cisco Remote PHY Device.

CHAPTER 2

Cisco Remote PHY Fault Management

This document describes how to configure the events for fault management on the Cisco cBR Series Converged Broadband Router.

Information About Fault Management

Fault management on RPD is required for remote monitoring, detection, diagnosis, reporting, and correcting the issues.

The Fault management module provides the following support:

- RPD can send events to the CCAP core
- CCAP core can get events from RPD
- Send RPD events using SNMP traps
- On the CCAP core, view log in to the CLI
- SNMP poll events are supported

RPD Event Reporting

An RPD logs events, generates asynchronous notifications that indicate malfunction situations, and notifies the operator about important events. The RPD event reporting includes two methods of reporting.

- During the initialization of RPD, CCAP core synchronizes events from the RPD.
- During run-time operations, RPD notifies the CCAP Core of the events

Restrictions for Configuring RPD Events

Following restrictions are applicable:

A maximum of 1000 events are retained on Cisco cBR. The RPD retains 1000 events locally and 1000 events in pending state.

How to Configure RPD Events

Configuring RPD Events

You can configure an event profile and apply it to RPD. Use the following commands to configure RPD events:

```
enable
configure terminal
cable profile rpd-event profile_id
  priority {emergency|alert|critical|error|warning|notice|informational|debug}
{0x0|0x1|0x2|0x3}
  enable-notify
```

- 0x0—No log
- 0x1— Save log in RPD local storage
- 0x2—Report to Cisco cBR
- 0x3— Save log in RPD local storage and report to Cisco cBR

You must enable-notifications for the RPD to report any event to the Core.

Configuring 55-1 Upstream RPD Events

You can configure an event profile and apply it to RPD. The 55-1 US events can be viewed only using log. For more information, go through Viewing RPD Events Using Log, on page 9.

SUMMARY STEPS

1. Use the following commands to configure RPD 55-1 US events:

DETAILED STEPS

	Command or Action	Purpose

Step 1	Use the following commands to configure RPD 55-1 US events:	`configure terminal`
		`cable profile rpd-55d1-us-event <profile_id>`
		`corrected-cells-threshold <threshold value>`
		`high-power-threshold <threshold value>`
		`low-power-threshold <threshold value>`
		`total-cells-threshold <threshold value>`
		`uncorrectable-cells-threshold <threshold value>`
		• corrected-cells-threshold - <1-65535> US Excessive Corrected Cells Threshold.
		• high-power-threshold - <-16 - 16> High power threshold in dBmV.

	Command or Action	Purpose
		• low-power-threshold - <-16 - 16> Low power threshold in dBmV. • total-cells-threshold - <1-65535> US Excessive Total Cells Threshold. • uncorrectable-cells-threshold - <1-65535> US Excessive Uncorrectable Cells Threshold. Ensure that you have enabled notifications for the RPD to report any event to the core.

Applying the Event Profile to RPD

Use the following commands to apply the Event Profile to an RPD:

```
enable
configure terminal
cable rpd rpd_name
rpd-event profile profile_id
rpd-55d1-us-event profile profile_id
```

Note If RPD is online when changing the profile, ensure that you have reset the RPD after you change the profile.

Enable RPD Event Trap

You can enable RPD event traps to send RPD events using SNMP traps. Use the following commands to configure RPD event traps:

```
enable
configure terminal
snmp-server enable traps rpd-event priority
```

Priority can be 1-8, where:

- 1—Enable RPD event trap for emergency priority
- 2— Enable RPD event trap for alert priority
- 3—Enable RPD event trap for critical priority
- 4— Enable RPD event trap for error priority
- 5— Enable RPD event trap for warning priority
- 6— Enable RPD event trap for notice priority
- 7— Enable RPD event trap for informational priority
- 8— Enable RPD event trap for debug priority

The priority higher than the selected priority is also displayed.

Configure SNMP Trap Server

You can configure SNMP trap server on the cable modem using the following commands:

```
enable
cnfigure terminal
Router# snmp-server host ip_address traps version 2c public udp-port port_number
```

where,

- *ip_address*—IP address of the server
- *port_number*—UDP port number assigned to receive the SNMP traps. The same port number must also be configured on the SNMP server.

Getting RPD Events

To retrieve events from RPD, use the **cable rpd [RPD IP|RPD MAC|all] event {locallog|pending}** command, as given in the following example:

```
Router#cable rpd 30.84.2.111 event pending
```

Clearing All Events on Cisco cBR Database

To remove all Events on Cisco cBR, use the clear cable rpd all event command, as given in the following example:

```
Router#clear cable rpd all event
```

Viewing the RPD Events

To view all RPD Events, use the **show cable rpd [RPD IP|RPD MAC] event** command as given in the following example.

```
Router# show cable rpd 93.3.50.7 event
RPD            EventId    Level Count  LastTime       Message
0004.9f00.0861 66070204   Error  1     Feb21 12:11:06 GCP Connection Failure
CCAP-IP=30.85.33.2;RPD-ID=0004.9f00.0861;
0004.9f00.0861 2148074241 Error  1     Feb21 12:11:25 Session failed:connecting timeout,
@SLAVE: 93.3.50.7:None --> 30.85.33.2:8190;RPD-ID=0004.9f00.0861;
```

To view specific RPD event groups, use the **show cable rpd event group [RPD IP|RPD MAC] [fcc|slot]** command as shown in this example.

```
Router# show cab rpd event group 7abd.44a1.0000 fcc
RPD            EventId         Level Count  LastTime       Message
7abd.44a1.0040 66070303 Criti  2            Oct16 20:50:35 FCC event
example;GROUP-ID=7abd.44a1.0000;
                                                        SLOT-ID=FCC;RPD-ID=7abd.44a1.0040;


Router# show cab rpd event group 7abd.44a1.0000 slot 9
RPD            EventId         Level Count  LastTime         Message
7abd.44a1.0140 66070700 Notic  1          Oct16 17:20:34   RPD=7a:bd:44:a1:01:40 PTP clock
 synchronized to Master=10.90.3.93;GROUP-ID=7abd.44a1.0000;
```

```
SLOT-ID=LC9;RPD-ID=7abd.44a1.0140;
```

Viewing RPD Events Using Log

To view all RPD Events, use the show logging command, as given in the following example.

```
Router# show logging | include RPD-ID=0004.9f00.0861
004181: Feb 21 12:18:59.649 CST: %RPHYMAN-3-RPD_EVENT_ERROR:  CLC5: rphyman:
GCP Connection Failure CCAP-IP=30.85.33.2;RPD-ID=0004.9f00.0861;EVENT-ID=66070204;
FirstTime=2017-2-21,12:11:6.0;
LastTime=2017-2-21,12:11:6.0;
Count=1;PendingQueue;
004185: Feb 21 12:19:18.875 CST: %RPHYMAN-3-RPD_EVENT_ERROR:  CLC5: rphyman:
Session failed:connecting timeout, @SLAVE: 93.3.50.7:None --> 10.10.10.12:1190;
RPD-ID=0004.9f00.0861;
EVENT-ID=2148074241;
FirstTime=2017-2-21,12:11:25.0;
LastTime=2017-2-21,12:11:25.0;
Count=1;PendingQueue;
```

Configuration Examples

This section provides example for the fault management configuration on Cisco cBR-8.

Example: RPD Event Configuration

```
enable
configure terminal
cable profile rpd-event 6
    priority warning 0x3
    enable-notify
cable rpd node6
    identifier badb.ad13.5e08
    core-interface Te3/1/5
        principal
        rpd-ds 0 downstream-cable 3/0/17 profile 10
        rpd-us 0 upstream-cable 3/0/34 profile 13
    r-dti 16
    rpd-event profile 6
```

The following event reportings are supported:

- **alert**: Event reporting for alert priority.
- **critical**: Event reporting for critical priority.
- **debug**: Event reporting for debug priority.
- **emergency**: Event reporting for emergency priority.
- **error**: Event reporting for error priority.
- **informational**: Event reporting for informational priority.
- **notice**: Event reporting for notice priority.
- **warning**: Event reporting for warning priority.

Example: RPD 55-1 Upstream Event Configuration

```
cable profile rpd-event 6
  priority warning 0x3
  enable-notify

cable profile rpd-55d1-us-event 10
  corrected-cells-threshold 11
  high-power-threshold 7
  low-power-threshold 2
  total-cells-threshold 20
  uncorrectable-cells-threshold 8

  cable rpd node 6
    identifier badb.ad13.5e08
    core-interface Te3/1/5
      principal
      rpd-ds 0 downstream-cable 3/0/17 profile 10
      rpd-us 0 upstream-cable 3/0/34 profile 13
    r-dti 16
    rpd-event profile 6
    rpd-55d1-us-event profile 10
```

Feature Information for R-PHY Fault Management

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

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

Table 3: Feature Information for R-PHY Fault Management

Feature Name	Releases	Feature Information
R-PHY Fault Management	Cisco 1x2 / Compact Shelf RPD Software 3.1	This feature was integated into the Cisco Remote PHY Device.

CHAPTER 3

Cisco Remote PHY Device Operations and Debugging

This document describes the RPD operations and debugging of an RPD.

Hardware Compatibility Matrix for Cisco Remote PHY Device

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 RPD Operations and Debugging

The operators might need secure remote access to the RPD for activities such as setting up the RPD before the installation, maintenance, or troubleshooting. The RPD supports Secure Shell (SSH) server that allows secure access to the RPD.

Prerequisites for RPD Operations

The following prerequisites are applicable for debugging or checking RPD operations:

- RPD has established GCP connection with the CCAP-core, and RPD IP address is retrievable from CCAP-core.
- RPD is assigned an IP address through the DHCP process, and the IP address is retrievable from the DHCP server.

How to Access and Debug RPD

Accessing RPD using SSH

After logging in to the RPD for the first time, the system shows a security warning.

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


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

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

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




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


        Welcome to Cisco R-PHY
```

```
R-PHY>
```

The following procedure shows how to use SSH to access RPD without password from NMS.

1. Check whether NMS already has an SSH key. If yes, do not generate a new key.
2. Generate a new SSH key in NMS.

   ```
   cat ~/.ssh/id_rsa.pub
   ssh-keygen -t rsa
   ```

3. Add the NMS public key in RPD.

   ```
   ssh pubkey add ?
   LINE          NMS's pubkey
   ```

4. Verify whether NMS can connect using SSH to RPD without a password.

   ```
   ssh -l admin <RPD ip>
   ```

Disabling SSH Login Password

Use the following commands to apply the Event Profile to an RPD:

```
R-PHY#conf t
R-PHY(config)#ssh password ?
off                  disable ssh password login
on                   enable ssh password login
R-PHY(config)#ssh password off
R-PHY(config)#end
```

Debugging RPD

Use the following procedure to debug RPD:

1. Disable RPD auto reboot by setting the reboot hold.

   ```
   R-PHY# set reboot hold
   ```

2. Secure copy the logs of RPD to the server using the following command.

   ```
   logging provision-archive scp server_ip user_id dst_location
   ```

3. Collect the show CLI output.

   For RPD online issues, check which status is failed. You can check the following outputs:

   - show provision all
   - show provision history
   - show dot1x detail
   - show dhcp
   - show tod
   - show ptp clock 0 config
   - show ptp clock 0 state

For modem online issue, check ds/us config and l2tp session.

You can collect the following outputs:

- show downstream channel configuration
- show downstream channel counter dps (show multiple times)
- show downstream depi configuration
- show upstream channel configuration <port number> <channel number>
- show upstream iuc counter <port number> <channel number> (show multiple times)
- show upstream map counter <port number> <channel number> (show multiple times)
- show upstream uepi configuration
- show l2tp tunnel
- show l2tp session

4. Enable RPD auto reboot, after collecting all logs and CLI output.

```
R-PHY#clear reboot hold
```

Verifying Disabled SSH Password Login

To check whether the SSH logging in using a password is disabled, use the show ssh session command as given in the following example.

```
R-PHY#show ssh session
connected session: 1
ssh password auth: off
ssh NMS pubkey num: 1
R-PHY#
```

Configuration Examples

This section provides example for the fault management configuration on R-PHY.

Example: Generating a New NMS pubkey

```
$ cat ~/.ssh/id_rsa.pub

$ ssh-keygen -t rsa

$ cat ~/.ssh/id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAgEAtQCXVFmRIwemejbTx0+U8taMq5n4Zetu
71xb+dtHV8Rr0wejiK1YJkT93n9hcBxsjHRu76bLp99l+DDNL3+THljwnMQC1CsdvRmGXoe
Gf1mT9aTlGDf/ RW9ZywY9t8Kep9VnANu2DWSoh0wg2pE49HFOJAbGfuFOvPEdwZGGDMQNWs
Eq/3xAQjBxajQqfgu4IqjVzKoo4PM/xx9X4Z1aMwxS3DvyN7L8O0o33mcDNsasl3SslIjMSNfq
YpwOFvQve8c2onrYHUx2p3BwQOb/b0FzFQhZMTBXm/pDMXq/fkkD0uguk1xOGnqAATMJsSHIN
0UOdvbzhhmrFRBBM4NzqQG5kNt7KvnWgxE7HdalERvMyBC2MCGbFSHmQFyWmHBHPPmLIxK98W
XutoR8fzzs+4hingZ4X9DMMNwTQ6WOzjuKq6iU= userid@example.cisco.com
```

Example: Adding NMS pubkey in RPD

```
R-PHY#conf t
R-PHY(config)#ssh pubkey add ?
LINE                 NMS's pubkey
R-PHY(config)#ssh pubkey add ssh-rsa AAAAB3NzaC1yc26876bhjdsk
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
```

Feature Information for RPD Operations and Debugging

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

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

Table 5: Feature Information for RPD Operations and Debugging

Feature Name	Releases	Feature Information
RPD Operations and Debugging	Cisco 1x2 / Compact Shelf RPD Software 3.1	This feature was integrated into the Cisco Remote PHY Device.

CHAPTER 4

RPD Reset

Finding Feature Information

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

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 6: 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 RPD Reset

Starting from Cisco 1x2 / Compact Shelf RPD Software 6.1, factory reset and NVRAM reset via TLV and CLI are supported. In the factory reset, RPD restores the factory configuration and performs cold reboot. In this case, it is better for the RPD to have golden image, otherwise users need to boot the RPD manually. In the NVRAM reset, RPD clears the non-volatile configuration and performs cold reboot.

Resetting RPD

To clear the configuration, image and logs of the RPD, perform factory reset as shown in the following example:

```
R-PHY#reboot factory-reset
Warning: This action will restore the factory configuration. Are you sure you want to do
the factory reset (yes/no)?
```

To clear the non-volatile configuration of the RPD, perform NVRAM reset as shown in the following example:

```
R-PHY#reboot nv-reset
Warning: This action will clear the non-volatile configuration. Are you sure you want to
do the nvreset (yes/no)?
```

Soft-reset

Soft-reset is supported from Cisco 1x2 / Compact Shelf RPD Software 6.6 release. You can perform a soft-reset on the RPD using the RPD CLI or write TLV 40.1.1 (RpdResetCtrl to softReset(1)).

To perform soft-reset using RPD CLI, use the **reboot soft-reset** command:

```
R-PHY# reboot soft-reset
Warning: This action will perform a soft reset. Are you sure you want to do the soft reset
 (yes/no)?yes
SoftReset in 10 seconds
```

History of RPD Reset Instances

Cisco RPD supports the ResetHistory (TLV 100.3) object, which provides a record of the occurrences of a reset of an RPD. The RPD can be reset for many reasons, such as a loss of Principal Core, loss of IP connection, power failure, hardware or software failure, or reset command from CCAP Core or CLI.

This ResetHistory object provides details of the conditions that caused the RPD to reset and to assist operators with understanding why a service interruption occured. It also provides details of how much time it took for the RPD to boot its software stack and to become operational with the principal core.

Note

- If the `rebootdisable` parameter is set, the RPD does not save any record.
- If the power cycle is triggered during a reboot, the application is not notified about it. Hence, after recovery, the recovery time and the related information are saved in the latest record. New records are not generated for the power cycle reboot.
- Recovery time (recoveryTime—TLV 100.31.7)
  - softReset—The recovery time of the soft-reset is the RCP process up-time when the system becomes operational.
  - hardReset/nvReset/factoryReset—The recovery time is the system up-time when the system becomes operational.
- It stores up to 100 records.

Display or Clear Reset-History

Use the following command to show the RPD reset-history: **show reset-history**:

```
R-PHY#show reset-history
Index Type            ResetTimeStamp       RecoveryTimeStamp    RecoveryTime EventRef
1     hardReset       2020-01-13 01:42:42  2020-01-13 01:51:22  481          66070212
2     softReset       2020-01-13 01:30:18  1970-01-01 00:00:00  0            66070212
3     hardReset       2020-01-13 01:19:19  2020-01-13 01:29:26  568          66070212
4     hardReset       2020-01-13 00:57:43  2020-01-13 01:16:23  1099         66070411
5     softReset       2020-01-10 20:02:52  2020-01-11 01:11:40  18527        66070212
6     softReset       2020-01-10 20:00:30  2020-01-10 20:02:29  118          66070212
7     softReset       2020-01-10 19:57:51  2020-01-10 19:59:56  124          66070212
8     softReset       2020-01-10 19:51:30  2020-01-10 19:52:53  82           66070212
9     hardReset       2020-01-10 19:25:23  2020-01-10 19:40:51  898          66070212
10    hardReset       2020-01-10 19:19:39  1970-01-01 00:00:00  0            66070212
11    hardReset       2020-01-10 19:13:51  1970-01-01 00:00:00  0            66070212
…
R-PHY#clear reset-history
```

Use the following command to clear the RPD reset-history: **clear reset-history**:

```
R-PHY#clear reset-history
```

RPD TACACS

The RPD TACACS (Terminal Access Controller Access-Control System) feature is supported from Cisco 1x2 / Compact Shelf RPD Software V7.2 and later. The RPD TACACS feature disables local access if the server is available.

When the TACACS server can be reached from RPD, you can only access the RPD by TACACS account. Local access will be disabled, and you cannot access RPD by local account. But if the TACACS server cannot be reached, for example, due to a wrong server address, network issue, or so on, you can then access RPD by local account.

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

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

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

User can also delete server and change the secret key.

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

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

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

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

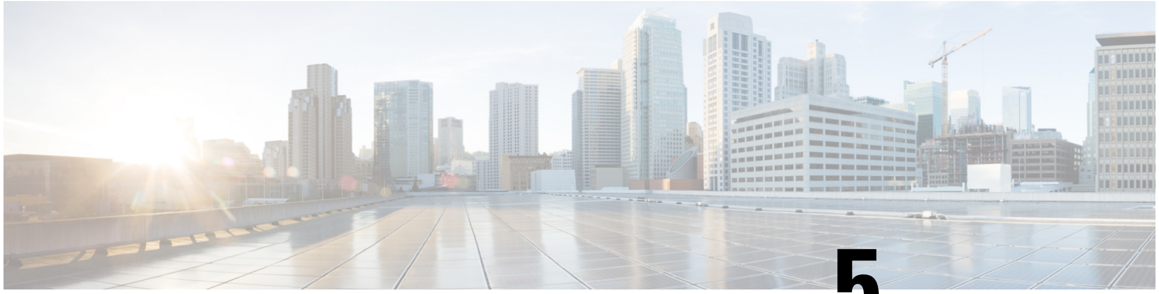
Feature Information for RPD Reset

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

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

Table 7: Feature Information for RPD Reset

Feature Name	Releases	Feature Information
Factory reset support	Cisco 1x2 / Compact Shelf RPD Software 6.1	This feature was introduced on the Cisco Remote PHY Device.
Softreset support	Cisco 1x2 / Compact Shelf RPD Software 6.6	This feature was introduced on the Cisco Remote PHY Device.
RPD TACACS support	Cisco 1x2 / Compact Shelf RPD Software 7.2	This feature was introduced on the Cisco Remote PHY Device.
RPD Reset-history	Cisco 1x2 / Compact Shelf RPD Software 7.7	This feature was introduced on the Cisco Remote PHY Device.



CHAPTER 5

Archiving RPD Logs

Finding Feature Information

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

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 8: 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 Archiving Logs

You can archive logs to the SCP or TFTP server, or RPD itself.

When an RPD SSH session is closed during an RPD logging archive process, the RPD logging temp file is retained in the RPD file system. In this release, only the latest temp file is retained. The legacy temp files are removed.

Archiving Logs Using SCP or TFTP

To archive logs, use the **logging** command.

To transfer files to the TFTP server, use the **logging [provision-archive|1588-archive|corefile-archive] tftp** *server_ip save_path* command.

To transfer files to the SCP server, use the **logging [provision-archive|1588-archive|corefile-archive] scp** *server_ip user save_path* command.

To archive logs created during RPD provisioning to the SCP server, use the **logging provision-archive scp** *server_ip user save_path* command.

Note

- Use **provision-archive** to archive logs created during RPD provisioning.
- Use **1588-archive** to archive PTP logs.
- Use **corefile-archive** to archieve logs created duing system crashes.
- *user* is the username of the SCP or TFTP server account to which files are transferred.
- *save_path* is the relative path of the folder in the SCP or TFTP server. You must have write permission to access the folder. Make sure that the folder has sufficient space.
- *server_ip* can be IPv4 or IPv6 address. The server IP address type must be the same as the RPD IP address.
- For SCP file transfer, type the password of your server account when prompted. For TFTP file transfer, password is not required.
- RPD should be able to successfully ping the SCP or TFTP server. If the ping is unsuccessful, files are not archived.

This is an example of how to archive logs created during RPD provisioning to the SCP server.

```
R-PHY#logging provision-archive scp 198.51.100.1 <user> /tmp
Wait for archiving logs
Collect tech-support info...
```

```
Wait for upload archive to server. It would take 3 minutes or more.
RPD logs will be saved in
<user>@<server_ip>:/<save_path>/RPD_PROV_10049fc20200_LOG_2018-08-20_00_12_22_419798.tar.gz


Host '<server_ip>' is not in the trusted hosts file.
(ssh-rsa fingerprint md5 b6:bb:d4:20:92:47:bb:29:d7:2c:5d:47:7a:a5:c6:8d)
Do you want to continue connecting? (y/n) y
<user>@<server_ip>'s password:
RPD_PROV_10049fc20200_LOG_2018-08-20_00_12_22 100%   61MB   1.9MB/s   00:32
[Done]
```

This is an example of how to archive PTP logs to the SCP server.

```
R-PHY#logging 1588-archive scp 198.51.100.1  <user> /tmp

wait for archiving 1588 logs
Wait for upload archive to server. It would take 3 minutes or more.
RPD logs are saved in
user@198.51.100.1:/tmp/RPD_1588_0027900a0cf8_LOG_1977-01-08_21_26_05_222552.tar.gz

Host '198.51.100.1' is not in the trusted hosts file.
(ssh-rsa fingerprint md5 1d:9d:69:0c:17:1e:66:03:11:7e:ff:a3:c1:55:b1:a7)
Do you want to continue connecting? (y/n) user@198.51.100.1's password:
RPD_1588_0027900a0cf8_LOG_1977-01-08_21_26_05 100%   29     0.0KB/s   00:00
[Done]
```

This is an example of how to archive logs created during system crashes to the SCP server.

```
R-PHY#logging corefile-archive scp 198.51.100.1  <user> /tmp

wait for archiving corefile
Wait for upload archive to server. It would take 3 minutes or more.
RPD logs are saved in
user@198.51.100.1:/tmp/RPD_COREFILE_0027900a0cf8_LOG_1977-01-08_21_27_59_522646.tar.gz
jianyzha@198.51.100.1's password:
RPD_COREFILE_0027900a0cf8_LOG_1977-01-08_21_2 100% 9126KB   8.9MB/s   00:01
[Done]
```

This is an example of how to archive logs created during RPD provisioning to the TFTP server.

```
R-PHY#logging provision-archive tftp 198.51.100.1 .

wait for archiving logs
Collect tech-support info...

wait for upload archive to server
RPD provision logs are saved in
198.51.100.1:$TFTP_DIR/./RPD_0027900a0cf8_LOG_1977-01-08_18_20_10_509660.tar.gz
[Done]
```

This is an example of how to archive PTP logs to the TFTP server.

```
R-PHY#logging 1588-archive tftp 198.51.100.1 .

wait for archiving 1588 logs
Wait for upload archive to server. It would take 3 minutes or more.
RPD logs are saved in
198.51.100.1:$TFTP_DIR/./RPD_1588_0027900a0cf8_LOG_1977-01-08_21_25_26_352484.tar.gz
[Done]
```

This is an example of how to archive logs created during system crashes to the TFTP server.

```
R-PHY#logging corefile-archive tftp 198.51.100.1 .

wait for archiving corefile
Wait for upload archive to server. It would take 3 minutes or more.
RPD logs are saved in
198.51.100.1:$TFTP_DIR/./RPD_COREFILE_0027900a0cf8_LOG_1977-01-08_21_27_37_782555.tar.gz
[Done]
```

Archiving Logs Locally

Starting from Cisco 1x2 / Compact Shelf RPD Software 7.3, user can save a log archive to **/rpd/archive** on the RPD using the command **logging [provision-archive|1588-archive|corefile-archive] local**. This archive can then be transferred or viewed locally.

Note

- Use **provision-archive** to archive logs created during RPD provisioning.
- Use **1588-archive** to archive PTP logs.
- Use **corefile-archive** to archieve logs created duing system crashes.

You can specify a date-range for archiving logs using the `logging` command. This command helps in controlling the size of the log archive if you specify logging only in the specific date range.

Configure logging by running the following commands:

```
logging provision-archive <from_date> <to_date> [scp|tftp|local]
logging 1588-archive <from_date> <to_date> [scp|tftp|local]
logging core-file archive <from_date> <to_date> [scp|tftp|local]
```

Usage

Enter the date range in the logging command and verify the logs locally or through SCP, TFTP. For example:

```
R-PHY#logging provision-archive 2020-07-10 2020-07-20 local
R-PHY#logging 1588-archive 2020-07-10 2020-07-20 local


R-PHY#logging provision-archive local
Collect tech-support info...
Please wait, archiving...
Created archive: /rpd/archive/RPD_PROV_badbad13ac3e_LOG_2019-08-28_11_59_01_898484.tar.gz
Created archive: /rpd/archive/RPD_running_log.tar.gz
Created archive: /rpd/archive/RPD_config_log.tar.gz
[Done]
```

Copying RPD Log Files using SCP

Remotely retrieving log files from the RPD via SCP is supported starting from Cisco 1x2 / Compact Shelf RPD Software 7.3 release. For security reasons, the SCP support would be limited to specific directories that contain the log files and only certain types of files under these directories. Only files from /tmp/, /rpd/, /rpd/archive/, /rpd/log/, and /rpd/log/<logname>.log/ are allowed. Filename must include one of: 'log', '.gz', or '.pcap'. This feature will only allow copying-out of files and will not allow copying-in of files to the RPD.

Feature Information for Archiving Logs

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

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

Table 9: Feature Information for Archiving Logs

Feature Name	Releases	Feature Information
Archiving Logs	Cisco 1x2 / Compact Shelf RPD Software 6.1	This feature was introduced on the Cisco Remote PHY Device.
SCP Support to Copy RPD Logfiles	Cisco 1x2 / Compact Shelf RPD Software 7.3	This feature was introduced on the Cisco Remote PHY Device.
Support for Local Archive	Cisco 1x2 / Compact Shelf RPD Software 7.3	This feature was introduced on the Cisco Remote PHY Device.

CHAPTER 6

SSH Account Management

Finding Feature Information

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

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 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 SSH Account Management

Manage your SSH account for an RPD SSH login. This feature enables you to add, delete, and change password of an SSH account.

Configure SSH Account Management

Add, delete, or modify your SSH account. You can also view your account details.

Add a New SSH Account

Note You can add a maximum of ten accounts at a time.

To add a new SSH account, run the **ssh adduser <newuser>** command. This example shows how to add a new SSH account.

```
R-PHY>enable
R-PHY#configure terminal
R-PHY(config)#ssh adduser <newuser>
Changing password for <newuser>
New password:
Retype password:
Password for <newuser> changed by root
R-PHY(config)#end
```

Delete an SSH Account

Note You cannot delete the last account.

To delete an SSH account, run the **ssh delete <newuser>** command. This example shows how to delete an SSH account.

```
R-PHY>enable
R-PHY#configure terminal
R-PHY(config)#ssh delete <newuser>
Warning: Are you sure to delete this account? [No/Yes]
Yes
delete account '<newuser>' successfully
R-PHY(config)#end
```

Change an SSH Account Password

To change an SSH account password, run the **ssh chpasswd <user>** command. This example shows how to change an SSH account password.

```
R-PHY>enable
R-PHY#configure terminal
R-PHY(config)#ssh chpasswd <user>
Please enter password for '<user>':
Please re-enter your password:
Password for '<user>' changed
R-PHY(config)#end
```

View SSH Account Details

To view an SSH account details, run the **show ssh account** command. This example shows how to view an SSH account details.

```
R-PHY#show ssh account
Account Num: 2
Current SSH Accounts:
admin
user
```

Feature Information for SSH Account Management

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

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

Table 11: Feature Information for SSH Account Management

Feature Name	Releases	Feature Information
SSH Account Management	Cisco 1x2 RPD Software 6.1	This feature was introduced on the Cisco Remote PHY Device.