Release Notes for Cisco Remote PHY Device, Cisco 1x2 / Compact Shelf
RPD Software 6.7.1

First Published: 2019-09-13

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
Introduction

Explore the Content Hub, the all new portal that offers an enhanced product documentation experience.

- Use faceted search to locate content that is most relevant to you.
- Create customized PDFs for ready reference.
- Benefit from context-based recommendations.

Get started with the Content Hub at content.cisco.com to craft a personalized documentation experience.

Do provide feedback about your experience with the Content Hub.

This Release Notes contain information about downloading and installing Cisco 1x2 / Compact Shelf RPD Software 6.7.1 and its maintenance releases. It also provides new and changed information, hardware support, limitations and restrictions, and caveats for Cisco 1x2 / Compact Shelf RPD Software 6.7.1 and its maintenance releases.

We recommend that you view the field notices for this release to see if your software or hardware platforms are affected. If you have an account at Cisco.com, you can find the field notices at http://www.cisco.com/en/US/customer/support/tsd_products_field_notice_summary.html.

If you do not have an account at Cisco.com, you can find the field notices at http://www.cisco.com/en/US/support/tsd_products_field_notice_summary.html.

Cisco 1x2 / Compact Shelf RPD Software 6.7.1 is generally available for field deployment. To ensure a smoother, faster, and successful field deployment, we recommend that you validate and qualify the software in a limited field trial.

The versions of Cisco cBR-8 router and RPD must be compatible. If the versions are not compatible, the RPD remains in the init(gep) state. The following list provides information on the compatible cBR-8 and RPD versions:

- Cisco IOS XE Everest 16.6.x works with RPD 2.x
- Cisco IOS XE Fuji 16.7.x works with RPD 3.x
- Cisco IOS XE Fuji 16.8.x works with RPD 4.x
Cisco IOS XE Fuji 16.9.x works with RPD 5.x
Cisco IOS XE Gibraltar 16.10.1c works with RPD 6.1, 6.2 and 6.3
Cisco IOS XE Gibraltar 16.10.1d works with RPD 6.4, 6.5 and 6.7
Cisco IOS XE Gibraltar 16.10.1f works with RPD 6.6 and 6.7
Cisco IOS XE Gibraltar 16.10.1g works with RPD 6.7.1

This chapter includes the following sections:

- System Requirements, on page 2
- New and Changed Information, on page 3
- MIBs, on page 17
- Obtaining Documentation and Submitting a Service Request, on page 18

System Requirements

These sections describe the system requirements for Cisco 1x2 / Compact Shelf RPD Software 6.7.1 and its maintenance releases:

Memory Requirements for Cisco 1x2 / Compact Shelf RPD Software 6.7.1

Memory is not configurable for the Cisco Remote PHY device.

Table 1: Memory Recommendations for the Cisco Remote PHY Device

<table>
<thead>
<tr>
<th>Feature Set</th>
<th>Cisco RPHY Processor</th>
<th>Software Image</th>
<th>Fixed Memory</th>
<th>Runs From</th>
</tr>
</thead>
<tbody>
<tr>
<td>CISCO RPHY 6.7.1</td>
<td>NXP LS1043A</td>
<td>RPD-V6-7-1.itb.SSA</td>
<td>1G Bytes</td>
<td>Bootflash:</td>
</tr>
</tbody>
</table>

Hardware Supported

For detailed information about the hardware supported in Cisco 1x2 / Compact Shelf RPD Software 6.7.1 and its maintenance releases, see:


Determining the Software Version of Cisco 1x2 / Compact Shelf RPD Software 6.7.1

To determine the version of the Cisco 1x2 RPD software running on your Cisco Remote PHY Device, log in and enter the `show version` EXEC command:

```
R-PHY# show version
Cisco RPD Software, version v6.7.1, build by rpd-release, on 2019-09-07 02:10:35
```
Branch information:
- RPD branch: (detached from RPD_V6.7_1_20190906)
- OpenRPD branch: (detached from RPD_V6.7_1_20190906)
- SeresRPD branch: (detached from RPD_V6.7_1_20190906)

Note
The system image file name of the factory installed image is
/bootflash/RPD-V6.7.1_hardware_certificate.itb.rel.sign.SSA. The system image file name of the Secure
Software Download (SSD) from the Cisco software download page is /bootflash/RPD-V6-7-1.itb.SSA.act.

New and Changed Information

The following sections list the new hardware and software features supported on the Cisco Remote PHY
Device in this release:

New Software Features in Cisco 1x2 / Compact Shelf RPD Software 6.7.1

There are no new software features for Cisco 1x2 / Compact Shelf RPD Software 6.7.1 release.

New Software Features in Cisco 1x2 / Compact Shelf RPD Software 6.7

The new software features for Cisco 1x2 / Compact Shelf RPD Software 6.7 release are:

**PTP big jitter packets filter on RPD**

From RPD V6.7 release onwards, RPD will filter PTP big jitter packets and dynamically adjust the delay
threshold to improve PTP stability. This change will help avoid the modem offline issue caused by PTP lose
sync issue caused by the following two scenarios:

- RPD receives a PTP packet with big jigger (bigger than 0.5ms) and then jumps back.
- Network path between RPD and PTP master is switched to another with a different time delay.

Serviceability Improvements

The following serviceability improvements are included with the RPD V6.7 release:

- Add archive and rotation for OFDM related logs.
- Resolve RPD crash issue when bcm regproc component debugs are turned on.
- Enhance show l2tp session CLI for improved debuggability.
- Session and tunnel IDs in show l2tp session table is displayed in both decimal and hex format for quick
  verification.

```
R-PHY#show l2tp session
L2TP Tunnel Information Total tunnels 1 sessions 48
```
Enhance the CLI to display per session detail to accept session/tunnel IDs in both decimal and hex format.

R-PHY# show l2tp session 497498612 4390913

['497498612', '4390913']

NdfPerfStats-TLV 76 support

The RPD 6.7 includes TLV 76(NdfPerfStats) support. Get NDF performance stats through this TLV 76 from RPD or use SNMP MIB table docsRphyStatsRpDsNdfPerfStatsTable to query stats from CMTS/CCAP.

Support PNM-UTSC-SAC channel type

From RPD V6.7 release, add channel type 12(PNM-UTSC-SAC) in TLV 58.3.11.2.2(ChannelType) to alignment latest Remote-PHY Specification I12.
New Software Features in Cisco 1x2 / Compact Shelf RPD Software 6.6.1

There are no new software features for Cisco 1x2 / Compact Shelf RPD Software 6.6.1 release.

New Software Features in Cisco 1x2 / Compact Shelf RPD Software 6.6

The new software features for Cisco 1x2 / Compact Shelf RPD Software 6.6 release are:

**SoftReset support**

SoftReset is supported from RPD V6.6 release. You can softReset RPD by RPD CLI or write TLV 40.1.1(RpdResetCtrl to softReset(1)).

To perform soft-reset by 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
```

**Support NDR/NDF channel in TLV 100.2.21**

RPD V6.6 release provides NDR/NDF channel support in TLV 100.2.21(RPDSessionStats). You can get information on NDR/NDF channel counter by reading this TLV.

**Add ADM1260 PSOC fault log output to log file**

From RPD V6.6 release and later, ADM1260 PSOC fault log will be recorded in the RPD log file.

**Support for Events 66070312, 66070313, 66070323**

RPD V6.6 release provides event support for 66070312, 66070313, 66070323. Information on the event is listed in the following table:

<table>
<thead>
<tr>
<th>Process</th>
<th>Sub-Process</th>
<th>RPD Priority</th>
<th>Event Message</th>
<th>Message Notes and Detail</th>
<th>Error Code Set</th>
<th>Event ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Init</td>
<td>DHCP</td>
<td>Warning</td>
<td>DHCP WARNING - Non-critical field invalid in response; DHCP Server IP: &lt;P1&gt;; Port: &lt;P2&gt;; &lt;TAGS&gt;;</td>
<td>P1 = DHCP server IP address; P2 = Ethernet port number</td>
<td>B703.12</td>
<td>66070312</td>
</tr>
</tbody>
</table>
### Boot-up failure solution

RPD V6.6 also has the Boot-up failure solution enhancement that solves any RPD boot-up failure issues. To implement the enhancement, complete the following steps:

1. Upgrade bootloader to May 03 2019 - 21:56:55-0400 version. The RPD boot retry sequence would change during an RPD boot failure. Boot sequence:

   ```markdown
   primary bootloader > imagea(24 times) > imageb(1 time) > imageg(1 time) >
   golden bootloader > imagea(1 time) > imageb(1 time) > imageg(1 time)
   ```

2. Disable the console port input during RPD boot-up.
3. Change RPD uboot stop autoboot from Ctrl + C to 'shell'.
4. Disable the RPD by using the Ctrl +S key combination.
5. Revert the watchdog timing from 10 minutes to 5 minutes.
6. Add more bootup debug logs in RPD log file.

### New Software Features in Cisco 1x2 / Compact Shelf RPD Software 6.5.1

There are no new software features for Cisco 1x2 / Compact Shelf RPD Software 6.5.1 release.
New Software Features in Cisco 1x2 / Compact Shelf RPD Software 6.5

View Downstream Channel Traffic Rate for Each Downstream Channel

You can view the downstream channel traffic rate for each downstream channel using the `show downstream channel counter dps` command. The downstream channel traffic rate is calculated every 60 seconds for SC-QAM and every 15 seconds for OFDM. This time interval for rate calculation is fixed and is not configurable. The rate for video channels is constant due to NULL padding by RPD.

The downstream channel traffic rate is displayed in the Rate-in-Mbps column.

```
R-PHY#show downstream channel counter dps
Chan  Tx-packets Tx-octets Drop-pkts Tx-sum-pkts Tx-sum-octs Drop-sum-pkts Rate-in-Mbps
 0    4813    312062    0   681977411   1351860818   0   1.056
 1    4813    312062    0   681959934   1350670750   0   1.056
 2    4813    312062    0   681976985   1351570253   0   1.056
 3    4815    312386    0   682030255   1355185470   0   1.057
 4    1     34        0   183779   7268458    0   0.000
 5    1     34        0   183844   7275912    0   0.000
 6    1     34        0   183751   7265430    0   0.000
158  2176627  315605389   0 1774253740  3657047865   0 1187.343
```

New Software Features in Cisco 1x2 / Compact Shelf RPD Software 6.4.1

The new software features for Cisco 1x2 / Compact Shelf RPD Software 6.4.1 release are:

Periodic Unsolicited Neighbor Advertise

User can write TLV 21(VendorSpecificExtension).15(UnsolicitedNA) to enable/disable RPD sending Periodic Unsolicited Neighbor Advertise by specific interval.

RetransTime

This object controls the interval of RPD send Periodic Unsolicited Neighbor Advertise. If set value to 0, means disable RPD send Periodic Unsolicited Neighbor Advertise.

```
Table 2:

<table>
<thead>
<tr>
<th>TLV Type</th>
<th>Length</th>
<th>Access</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>21.15.1</td>
<td>2</td>
<td>R/W</td>
<td>An unsigned short value has a range of 0 to 65535 seconds. Set to 0, means disable RPD send Periodic Unsolicited Neighbor Advertise.</td>
</tr>
</tbody>
</table>
```

You can check “UnsolicitedNA” value in “show DHCP” command for Periodic Unsolicited Neighbor Advertise RetransTime configuration if this feature is enabled.

```
R-PHY#show dhcp
Interface  IP-Address   Subnet-Mask
vbh0      2001:11:1:4::7c06  ffff:ffff:ffff:ffff:
Details:
-------------------------------------------------------------
Interface: vbh0
AddrType: IPv6<Stateful>
TimeServers: 2001:11:1:1::10
```
New Software Features in Cisco 1x2 / Compact Shelf RPD Software 6.4

The new software features for Cisco 1x2 / Compact Shelf RPD Software 6.4 release are:

**TACACS+ support**

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.

1. **Note**
   - RPD can configure 8 TACACS servers at the most. All configured servers use the same secret key.
   - 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.
   - RPD and TACACS server must use same address family.

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.
```

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
```

**RpdInfo read count/read by key support**

Starting from Cisco 1x2 / Compact Shelf RPD Software 6.4, TLV 100 RpdInfo read count and read by key is supported.

**Spectrum capture support**
The upstream triggered spectrum analysis measurement provides a wideband spectrum analyzer function in the CCAP which can be triggered to examine desired upstream transmissions as well as underlying noise or interference during a quiet period. WBFFT stands for Wide Band Fast Fourier Transform. This feature allows all RPD US ports to enable an upstream spectrum analyzer built into the RPD’s front end. RPD supports FreeRunning trigger mode.

Figure 1: Spectrum capture workflow

US FFT data is computed and sent directly from US PHY. RPD firmware does not handle these data. The firmware configures US PHY to send L2TP stream based on GCP TLV messages.

Please refer to below link for cBR8 configuration about this feature:


1. This feature provides a stream of raw spectrum data only.
2. The application that interprets and presents the data in human readable format is not part of this feature.

To verify if the spectrum capture is enabled, use `show bcm-register wbfft config` command as shown in the following example. The WBFFT Trigger Mode should be FreeRunning if this feature is enabled.

```
R-PHY#show bcm-register wbfft config
WBFFT Trigger Mode : FreeRunning
Enable UTSC : TRUE
Sample Num : 4096
Session ID : 44201020
PNM Dest IP : 2001:30:84:0:1:0:66:1
PNM Dest Mac : c414.3c16.d682
R-PHY#show bcm-register wbfft all 0
WBFFT Start Ctrl [cc000000] : 00000001
In Control [cc000004] : 00472F04
Out Control [cc00000c] : 0000009B
Timing Ctrl [cc000010] : 00000003
WBFFT FIRST WDW CF [cc000024] : 00000920
WBFFT SCND WDW CF [cc000028] : 0000C660
```
Viavi integration

In this feature, RPD supports non-CCAP defined MAX-HOLD mode for spectrum capture that work with Viavi RCI Agent.

Figure 2: Viavi integration workflow

1. Communications with core is implemented using SNMP.
2. Before using this feature, the NDF/NDR feature must be configured on cBR-8.
3. Viavi RCI Agent needs to be installed and configured on the system with Linux/Ubuntu operating system.

To verify if the spectrum capture is enabled, use `show bcm-register wbfft config` command as shown in the following example. The WBFFT Trigger Mode should be Other if this feature is enabled.

R-PHY#show bcm-register wbfft config

- **WBFFT Trigger Mode**: Other
- **Enable UTSC**: True
- **Samples Num**: 4096
- **Session ID**: 5f20003c
- **PNM Dest IP**: 91.7.66.171
- **PNM Dest Mac**: 0050.5688.eb3d

R-PHY#show bcm-register wbfft all 0

- **WBFFT Start Ctrl**: 00000005
- **In Control**: 00472f04
- **Out Control**: 00000099
- **Timing Ctrl**: 00000003
- **WBFFT FIRST WDW CF**: 00000920
- **WBFFT SCND WDW CF**: 0000c660
- **WBFFT MIDL WDW CF**: 000061e0
- **WBFFT MAX CTL**: 39c00000
- **WBFFT Status**: 00000080
Soft Enforcement

Soft Enforcement of SEC-AUT-DEFROOT requirement is implemented by printing a warning message and posting warning event 2148075527 during user login process when the default password for admin account is in use.

Below is the warning message that shows up when the default password for admin account is used to login RPD:

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Default login credentials detected in use.
In order to enhance the security of your network, default login credentials must be changed on this RPD.
In a future release, this RPD will disable service until default credentials are changed.
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

The following table lists the warning event that is triggered when the default password for admin account is used to login RPD:

<table>
<thead>
<tr>
<th>RPD Priority</th>
<th>Event Message</th>
<th>Event ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Warning</td>
<td>Rpd default login credentials detected in use - please change password immediately</td>
<td>2148075527</td>
</tr>
</tbody>
</table>

**TLV100.2.21 support for OOB 55-1 and 55-2 channels**

Starting from Cisco Remote PHY for Cisco 1x2 / Compact Shelf RPD Software 6.4, support for TLV 100.2.21 is added in OOB 55-1 and 55-2 channels.

**New Software Features in Cisco 1x2 / Compact Shelf RPD Software 6.3**

The new software feature for Cisco 1x2 / Compact Shelf RPD Software 6.3 release is:

**OOB Support on Compact Shelf**

This release enables support for OOB 55-1 and 55-2 functionality for Cisco Remote PHY Compact Shelf 6 x 12 and Cisco Remote PHY Compact Shelf 3 x 6.

**New Software Features in Cisco 1x2 / Compact Shelf RPD Software 6.2**

The new software features for Cisco 1x2 / Compact Shelf RPD Software 6.2 release are:

**SFP support for 1RU shelf**

The following SFPs are supported:

- SFP-10G-AOC3M(10-2847-01)
- SFP-10G-LR-S(10-3107-01)
• DWDM-SFP10G-C(10-3036-01)

You can change DWDM-SFP10G-C’s Wavelength by using the RPD config CLI:

```
R-PHY(config)#sfp itu [port_no] [channel_no]
```

For more information on the mapping relationship between channel_no with wavelength, go through Cisco 10GBASE Dense Wavelength-Division Multiplexing SFP+ Modules Data Sheet.

**Read count TLV 100.21/22/23/17 support**

Read count TLV 100.21 HostResourcesSystem, TLV 100.22 HostResourcesStorage, TLV 100.23 HostResourcesSwRun and TLV 100.17 IpDefaultRouter is supported in RPD V6.2 Release.

**Read count TLV 74/75 support**

Read count TLV 100.74 DsOob551Perf and TLV 100.75 DsOob552Perf is supported in RPD V6.2 Release

**Analog Tx/Rx modules alarm threshold setting**

You can set Analog Tx/Rx modules alarm threshold by TLV 21 VendorSpecificExtension sub TLV 21.13 AnalogTxPower and TLV 21.14 AnalogRxPower.

- TLV definition:

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>Type</th>
<th>Access</th>
<th>Type constraints</th>
<th>Units</th>
<th>TLV Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>TxIndex</td>
<td>UnsignedByte</td>
<td>Key</td>
<td></td>
<td></td>
<td>21.13.1</td>
</tr>
<tr>
<td>MajorLowTH</td>
<td>UnsignedShort</td>
<td>Write-only</td>
<td></td>
<td></td>
<td>21.13.2</td>
</tr>
<tr>
<td>MinorLowTH</td>
<td>UnsignedShort</td>
<td>Write-only</td>
<td></td>
<td></td>
<td>21.13.3</td>
</tr>
<tr>
<td>NormalTH</td>
<td>UnsignedShort</td>
<td>Write-only</td>
<td></td>
<td></td>
<td>21.13.4</td>
</tr>
<tr>
<td>MinorHighTH</td>
<td>UnsignedShort</td>
<td>Write-only</td>
<td></td>
<td></td>
<td>21.13.5</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>Type</th>
<th>Access</th>
<th>Type constraints</th>
<th>Units</th>
<th>TLV Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>RxIndex</td>
<td>UnsignedByte</td>
<td>Key</td>
<td></td>
<td></td>
<td>21.14.1</td>
</tr>
<tr>
<td>MajorLowTH</td>
<td>UnsignedShort</td>
<td>Write-only</td>
<td></td>
<td></td>
<td>21.14.2</td>
</tr>
<tr>
<td>MinorLowTH</td>
<td>UnsignedShort</td>
<td>Write-only</td>
<td></td>
<td></td>
<td>21.14.3</td>
</tr>
<tr>
<td>NormalTH</td>
<td>UnsignedShort</td>
<td>Write-only</td>
<td></td>
<td></td>
<td>21.14.4</td>
</tr>
<tr>
<td>MinorHighTH</td>
<td>UnsignedShort</td>
<td>Write-only</td>
<td></td>
<td></td>
<td>21.14.5</td>
</tr>
</tbody>
</table>

- You can verify Analog Tx/Rx modules alarm threshold setting on RPD by below CLI:

```
R-PHY#show environment table 49
sensor_id: 49
```
New Software Features in Cisco 1x2 / Compact Shelf RPD Software 6.1

The new software features for Cisco 1x2 / Compact Shelf RPD Software 6.1 release are:

Disable LLDP by TLV

In Cisco 1x2 / Compact Shelf RPD Software 6.1, LldpEnable TLV is introduced to enable or disable the LLDP protocol. The RPD which supports this attribute MUST preserve the value of this attribute in it non-volatile configuration store.

Value is defined as the boolean value to enable/disable LLDP operation on the RPD. The values are:
• 0 – LLDP is disabled.
• 1 – LLDP is enabled.

The selection of a default value is left to vendor’s choice.

New added events

New events are supported for DHCPv6 and supported networks.

Table 5: Supported events for DHCPv6

<table>
<thead>
<tr>
<th>Process</th>
<th>Sub-Process</th>
<th>RPD Priority</th>
<th>Event Message</th>
<th>Message Notes and Detail</th>
<th>Error Code Set</th>
<th>Event ID</th>
</tr>
</thead>
</table>
| DHCP    | Error       | 66070300     | DHCP RENEW sent - No response for <P1><P2><TAGS> | • P1= IPv4 or IPv6  
• P2 = RPD interface number (EnetPortIndex) | B703.0 | 66070300 |
| DHCP    | Error       | 66070301     | DHCP REBIND sent - No response for <P1><P2><TAGS> | • P1=IPv4 or IPv6  
• P2 = RPD interface number (EnetPortIndex) | B703.1 | 66070301 |
| DHCP    | Error       | 66070302     | DHCP RENEW WARNING - Field invalid in response <P1> option field<P2><TAGS> | • P1=v4 or IPv6  
• P2 = RPD interface number (EnetPortIndex) | B703.2 | 66070302 |
| DHCP    | Critical    | 66070303     | DHCP RENEW FAILED - Critical field invalid in response<P1><TAGS> | P1 = RPD interface number (EnetPortIndex) | B703.3 | 66070303 |
| DHCP    | Error       | 66070304     | DHCP REBIND WARNING - Field invalid in response<P1><TAGS> | P1 = RPD interface number (EnetPortIndex) | B703.4 | 66070304 |
| DHCP    | Critical    | 66070305     | DHCP REBIND FAILED - Critical field invalid in response<P1><TAGS> | P1 = RPD interface number (EnetPortIndex) | B703.5 | 66070305 |
Table 6: Supported network events

<table>
<thead>
<tr>
<th>Process</th>
<th>Sub-Process</th>
<th>RPD Priority</th>
<th>Event Message</th>
<th>Message Notes and Detail</th>
<th>Error Code Set</th>
<th>Event ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Init</td>
<td>Network Authentication</td>
<td>Error</td>
<td>Network Authentication Error; Descr: &lt;P1&gt;; &lt;TAGS&gt;;</td>
<td>P1 = Authentication error description</td>
<td>B701.0</td>
<td>66070104</td>
</tr>
<tr>
<td>Init</td>
<td>Network Authentication</td>
<td>Notice</td>
<td>Network Authentication Success; &lt;TAGS&gt;;</td>
<td></td>
<td>B701.4</td>
<td>66070105</td>
</tr>
<tr>
<td>Connectivity</td>
<td>CCAP Core</td>
<td>Notice</td>
<td>Successfully connected to Core; Core ID: &lt;P1&gt;; &lt;TAGS&gt;;</td>
<td>P1 = CCAP Core ID to which the connection was completed</td>
<td>B702.19</td>
<td>66070219</td>
</tr>
<tr>
<td>Connectivity</td>
<td>CCAP Core</td>
<td>Warning</td>
<td>Connection lost - Auxiliary CCAP Core. Reconnect attempted; Core ID: &lt;P1&gt;; &lt;TAGS&gt;;</td>
<td>P1 = Auxiliary CCAP Core ID to which the connection was lost</td>
<td>B702.20</td>
<td>66070220</td>
</tr>
<tr>
<td>Connectivity</td>
<td>CCAP Core</td>
<td>Warning</td>
<td>Connection lost – Principal CCAP Core. Reconnect attempted; Core ID: &lt;P1&gt;; &lt;TAGS&gt;;</td>
<td>P1 = Principal CCAP Core ID to which the connection was lost</td>
<td>B702.21</td>
<td>66070221</td>
</tr>
<tr>
<td>Connectivity</td>
<td>CCAP Core</td>
<td>Notice</td>
<td>Successfully reconnected to Core; Core ID: &lt;P1&gt;; &lt;TAGS&gt;;</td>
<td>P1 = CCAP Core ID to which the connection was completed</td>
<td>B702.22</td>
<td>66070222</td>
</tr>
<tr>
<td>Init</td>
<td>IPv4 Address Acquisition</td>
<td>Notice</td>
<td>Successfully obtained IPv4 address; &lt;TAGS&gt;;</td>
<td></td>
<td>B703.24</td>
<td>66070324</td>
</tr>
<tr>
<td>Init</td>
<td>IPv6 Address Acquisition</td>
<td>Notice</td>
<td>Successfully obtained IPv6 address; &lt;TAGS&gt;;</td>
<td></td>
<td>B703.25</td>
<td>66070325</td>
</tr>
<tr>
<td>Init</td>
<td>TOD</td>
<td>Notice</td>
<td>Successfully obtained ToD; &lt;TAGS&gt;;</td>
<td></td>
<td>B703.26</td>
<td>66070326</td>
</tr>
<tr>
<td>Init</td>
<td>Config</td>
<td>Error</td>
<td>Received unknown RCP message from Core; Core ID: &lt;P1&gt;; Descr: &lt;P2&gt;; &lt;TAGS&gt;;</td>
<td>P1 = CCAP Core ID; P2 = Error description</td>
<td>B703.27</td>
<td>66070327</td>
</tr>
</tbody>
</table>
Factory reset support
Starting from Cisco 1x2 / Compact Shelf RPD Software 6.1, factory reset and NVRAM reset via TLV and CL1 are supported.

- factoryReset: The device restores the factory configuration and performs a hard reset. You can perform a factoryReset by running the following:

  R-PHY>enable
  R-PHY#reboot factory-reset

- nvReset: The device clears non-volatile configuration and performs a hard reset. You can perform a nvReset by running the following:

  R-PHY>enable
  R-PHY#reboot nvreset

Support for Narrowband Digital Forward And Narrowband Digital Return
Narrowband Digital Forward (NDF) refers to the digitizing of an analog portion of the downstream spectrum at the headend, sending the digital samples as payload in [DEPI] packets to the RPD, and then re-creating the original analog stream at the RPD. NDF supports services such as FM Broadcast, DAB+ Broadcast, and OOB signals for Forward Sweep, DS Leakage, and Element management.

Narrowband Digital Return (NDR) refers to the digitizing of an analog portion of the upstream spectrum at the RPD, sending the digital samples as payload in [R-UEPI] packets to the CMTS, and then re-creating the
original analog stream at the headend. NDR supports legacy OOB signals for Reverse Sweep, Return Path Monitoring, FSK based HMS, and other FSK based telemetry signals.

The following commands are introduced on the Cisco 1x2 / Compact Shelf RPD Software 6.1 release:

- **show downstream oob configuration ndf** – Provides the NDF configuration in RPD for each NDF channel configured. It displays PHY information for the NDF session.
- **show upstream oob configuration ndr** – Provides the NDR configuration in RPD for each of NDR channel configured. It displays PHY and L2TP information.
- **show downstream oob counter ndf** – Provides the NDF packet counter from BCM for each NDF channel configured. It is a clear on read counter.
- **show upstream oob counter ndr** – Provides the internal mapping of RPD channels and its corresponding channel configured in core.
- **show oob fpga ndf-status** – Provides the NDF FPGA status for each NDF channel configured.
- **show oob ds-mapping** – Provides the internal mapping of RPD channels and its corresponding channel configured in the core.

For more information, see the Cisco cBR Series Converged Broadband Routers Quality of Services Configuration Guide for Cisco IOS XE Gibraltar 16.10.x and the Cisco CMTS Cable Command Reference Guide.

**Modified Software Features in Cisco 1x2 / Compact Shelf RPD Software 6.7.1**

There are no modified software features for Cisco 1x2 / Compact Shelf RPD Software 6.7.1 release.

**Integrated Software Features in Cisco 1x2 / Compact Shelf RPD Software 6.7.1**

There are no new integrated software features for Cisco 1x2 / Compact Shelf RPD Software 6.7.1 release.

**New Hardware Features in Cisco 1x2 / Compact Shelf RPD Software 6.7.1**

There are no new hardware features for Cisco 1x2 / Compact Shelf RPD Software 6.7.1 release.

**MIBs**

To locate and download MIBs for selected platforms, Cisco IOS XE releases, and feature sets, use Cisco MIB Locator found at the following URL:

https://mibs.cloudapps.cisco.com/ITDIT/MIBS/servlet/index

**MIBs in Cisco 1x2 / Compact Shelf RPD Software 6.7.1**

There are no new MIBs in Cisco 1x2 / Compact Shelf RPD Software 6.7.1.
Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see What’s New in Cisco Product Documentation.

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the What’s New in Cisco Product Documentation RSS feed. The RSS feeds are a free service.
Caveat List

This chapter describes open severity 1 and 2 caveats and select severity 3 caveats:

- The Open Caveats sections list open caveats that apply to the current release and may apply to previous releases. A caveat that is open for a prior release and is still unresolved applies to all future releases until it is resolved.

The bug IDs are sorted alphanumerically.

Note

The Caveats section includes the bug ID and a short description of the bug. For details on the symptoms, conditions, and workaround for a specific caveat you must use the Bug Search Tool.

- Cisco Bug Search, on page 19
- Open Caveats for Cisco 1x2 / Compact Shelf RPD Software 6.7.1, on page 19
- Resolved Caveats for Cisco 1x2 / Compact Shelf RPD Software 6.7.1, on page 20

Cisco Bug Search

Cisco Bug Search Tool (BST), the online successor to Bug Toolkit, is designed to improve effectiveness in network risk management and device troubleshooting. You can search for bugs based on product, release, and keyword, and aggregates key data such as bug details, product, and version. For more details on the tool, see the help page located at http://www.cisco.com/web/applicat/cbsshelp/help.html.

Open Caveats for Cisco 1x2 / Compact Shelf RPD Software 6.7.1

<table>
<thead>
<tr>
<th>Caveat ID Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCvq03023</td>
<td>Duplicate option 32 sent in INFO REQUEST</td>
</tr>
<tr>
<td>CSCvq10038</td>
<td>docsRphyPtpRpdPtpPortStatusPacketsReceived &amp; sent return 0</td>
</tr>
<tr>
<td>CSCvq14646</td>
<td>RPHY: rpd stuck at init(l2tp) after DHCP renew fail and got a new IP address</td>
</tr>
</tbody>
</table>
# Resolved Caveats for Cisco 1x2 / Compact Shelf RPD Software 6.7.1

<table>
<thead>
<tr>
<th>Caveat ID Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCvp53392</td>
<td>Invalid REGPROC caller error due to pilottone code</td>
</tr>
<tr>
<td>CSCvq54296</td>
<td>Invalid Regproc call from ConfigureGLobalOfdm causes OFDM to fail</td>
</tr>
<tr>
<td>CSCvr03413</td>
<td>RPHY: 552 OOB, STBs will not sign-on due to timing failure</td>
</tr>
<tr>
<td>CSCvp71150</td>
<td>Hitting the Traceback message while executing &quot;show upstream oob counter ndr&quot; CLI.</td>
</tr>
<tr>
<td>CSCvp93760</td>
<td>55d2 core DS stuck with unknown trigger</td>
</tr>
</tbody>
</table>