What's New in Cisco 1x2/Compact Shelf RPD 7.x

Note 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.

Cisco is continuously enhancing the product with every release and this section covers a brief description of key features and enhancements that were added. It also includes links to detailed documentation, where available.

New Software Features in Cisco 1x2 / Compact Shelf RPD Software 7.8.2

There are no new software features for Cisco 1x2 / Compact Shelf RPD Software 7.8.2 release.

New Software Features in Cisco 1x2 / Compact Shelf RPD Software 7.8.1

There are no new software features for Cisco 1x2 / Compact Shelf RPD Software 7.8.1 release.

New Software Features in Cisco 1x2 / Compact Shelf RPD Software 7.8

The new software features for Cisco 1x2 / Compact Shelf RPD Software 7.8 release are the following:

Support for TLV 100.14 InOctets, InDelivers, InMcastOctets, OutMcastPkts, and OutMcastOctets

Supports InOctets TLV100.14.4, InDelivers TLV100.14.16, InMcastOctets TLV100.14.26, OutMcastPkts TLV100.14.27, and OutMcastOctets TLV100.14.28.

- InOctets—Reports the total number of octets received in the input IP datagrams, including those received in the error.
- InDelivers—Reports the total number of datagrams successfully delivered to the IPuser-protocols (including ICMP).
- InMcastOctets—Reports the total number of octets received in the IP multicast datagrams.
- OutMcastPkts—Reports the number of IP multicast datagrams transmitted.
- OutMcastOctets—Reports the total number of octets transmitted in IP multicast datagrams.

Support for Event 66070514-Enclosure Door Opened Condition Cleared

Cisco RPD 7.8 supports the 66070514-Enclosure door opened condition cleared event.

Process	Sub-Process	RPD Priority	Event Message	Message Notes and Detail	Error Code Set	Event ID
Environmental	Security	Notice	Enclosure door opened condition cleared; Time: <P1>; <TAGS>;	P1 = value of HostResourcesSystem Date attribute at time of sensor reading	B705.14	66070514

New Software Features in Cisco 1x2 / Compact Shelf RPD Software 7.7

The new software features for Cisco 1x2 / Compact Shelf RPD Software 7.7 release are the following:

Supports TLV 41.5 UscCalibration

RPD uses this complex TLV to report the current calibration constant for the RF ports associated with the selected SAC. It includes an entry for each RF port with the UscRfPort as a unique key.

The returned value is a signed 16-bit number and is in 1/100th of a dB.

The returned calibration constant should be subtracted from the raw received stream spectral power for any FFT bin.

Supports TLV 100.14.16 OutRequests and TLV 100.14.23 OutTransmits

OutRequests—This attribute reports the total number of IP datagrams that local IP user-protocols (including ICMP) supplied to the IP in requests for transmission.

OutTransmits—This attribute reports the total number of IP datagrams that this entity supplied to the lower layers for transmission.

Enables Strict Enforcement of Password Policy

Important Service Impacting—Update the default RPD SSH password.

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.
```

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.

```
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
R-PHY(config)#ssh password off

Successfully Disabled Password, SoftReset in 10 seconds
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
```

Supports TLV 100.31 ResetHistory

The TLV 100.31 ResetHistory provides a record of the occurrences of a reset of an RPD. The RPD can reset for many reasons, including a loss of Principal Core, loss of IP connection, power failure, hardware or software failure, or reset command from CCAP Core or CLI. This object provides the details of the conditions that cause the RPD to reset and to assist operators with understanding why a service interruption occurs. This object 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 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. No new records are generated for the power cycle reboot.
- About 100.31.7 RecoveryTime:
  - softReset—The recoveryTime of the softReset is the RCP process up-time when the system becomes operational.
  - hardReset/nvReset/factoryReset—The recoveryTime is the system up-time when the system becomes operational.
- It stores up to 100 records.

Use the following command to show or the clear RPD reset-history: **show|clear 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
```

New Software Features in Cisco 1x2 / Compact Shelf RPD Software 7.6.1

There are no new software features for Cisco 1x2 / Compact Shelf RPD Software 7.6.1 release.

New Software Features in Cisco 1x2 / Compact Shelf RPD Software 7.6

The new software features for Cisco 1x2 / Compact Shelf RPD Software 7.6 release are the following:

Support for New Events

This release supports the following events.

Process	Sub-Process	RPD Priority	Event Message	Message Notes and Detail	Error Code Set	Event ID
Init	Config	Notice	Backup Principal Core found; Core ID: <P1>; <TAGS>;	P1 = CCAP Core ID	B703.31	66070331
Init	Config	Notice	Backup Auxiliary Core found; Core ID: <P1>; <TAGS>;	P1 = CCAP Core ID	B703.32	66070332

Process	Sub-Process	RPD Priority	Event Message	Message Notes and Detail	Error Code Set	Event ID
Init	Config	Warning	Core not acting in any role for RPD - Neither active nor backup CCAP Core; Core ID: <P1>; <TAGS>;	P1 = CCAP Core ID	B703.33	66070333
Init	Config	Notice	Upgrade IRA; Core ID: <P1>; <TAGS>;	P1 = CCAP Core ID	B703.36	66070336
Init	Config	Notice	Redirect IRA; Core IP: <P1>; Core ID: <P2>; <TAGS>;	P1 = CCAP Core ID	B703.37	66070337
Init	Config	Notice	Pending IRAs; Core ID: <P1>; <TAGS>;	P1 = CCAP Core IP address P2 = CCAP Core ID	B703.38	66070338

Support for TLV 100.9.21 IfEnetStats OutDiscards

RPD 7.6 supports TLV 100.9.21 IfEnetStats OutDiscards. This attribute provides the number of outbound packets which are chosen to be discarded even though errors were not detected with these packets. The packets are discarded to prevent the system from delivering them to a higher-layer protocol.

Align Current Events to CableLabs RPHY I13 Specification

The following events messages are updated so that they conform to the CM-SP-R-OSSI-I13-190828 Specification: 66070203, 66070220, 66070223, 66070224, 66070320, 66070321, 66070327, 66070335, 66070403, 66070404, 66070215, 66070500, 66070501.

Enhanced Reporting Event 66070504—Enclosure Door Opened

In the earlier RPD releases, the polling interval for the event, 66070504-Enclosure door opened, was two minutes. Opening and closing the enclosure door in two minutes may not generate the event. In this release, this event is detected and reported in 10 seconds. If the enclosure door remains open for more than 10 sec, the event is reported every two minutes.

New Software Features in Cisco 1x2 / Compact Shelf RPD Software 7.5

The new software features for Cisco 1x2 / Compact Shelf RPD Software 7.5 release are the following:

Support for TLV 100.14.1, 100.14.31, 100.14.32

RPD 7.5 supports TLV 100.14.1 Ip version, TLV 100.14.31 DiscontinuityTime, and TLV 100.14.32 RefreshRate.

New Software Features in Cisco 1x2 / Compact Shelf RPD Software 7.4.1

There are no new software features for Cisco 1x2 / Compact Shelf RPD Software 7.4.1 release.

New Software Features in Cisco 1x2 / Compact Shelf RPD Software 7.4

The new software features for Cisco 1x2 / Compact Shelf RPD Software 7.4 release are:

Leakage/Pilot tone generation CW frequency granularity within +/- 0.5 Hz

RPD V7.4 support leakage/pilot tone generation CW frequency granularity within +/- 0.5 Hz. In order to support this granularity, pilot tone configuration need to follow below rules:

- Supported tone numbers: 2/3/4.
- Supported tone index: 0/1/2/3.
- Tone frequency should be large than 50Mhz.
- Valid tones need to be configured “no mute”.
- Frequency spacing should be less than 25MHz in a pair of tone.
- Go through the following possible scenarios:
  - If config 4 tones as two pairs of tones, tone 0 and tone 1 must be a pair, tone 2 and tone 3 must be a pair. For example:

```
R-PHY#show downstream calibration info
 [  0,  on] 137998869.0 Hz -33.0 dB {OFDM scaler=57159, Sine scaler=174}
 [  1,  on] 138001131.0 Hz -33.0 dB {OFDM scaler=57159, Sine scaler=174}
 [  2,  on] 611998717.0 Hz -33.0 dB {OFDM scaler=57159, Sine scaler=162}
 [  3,  on] 612001283.0 Hz -33.0 dB {OFDM scaler=57159, Sine scaler=162}
```

  - If config 2 tones as a pair of tone, support 2 tones at any tone index in (0, 1, 2, 3). For example:

```
R-PHY#show downstream calibration info
  [  0,  on] 611998717.0 Hz -33.0 dB {OFDM scaler=56624, Sine scaler=229}
  [  1,  on] 612001283.0 Hz -33.0 dB {OFDM scaler=56624, Sine scaler=162}
```

- If config 3 tones in CT3 mode, support 3 tones at any tone index in (0, 1, 2, 3). For example:

```
R-PHY#show downstream calibration info
  [  1,  on] 611998717.0 Hz -30.0 dB {OFDM scaler=56897, Sine scaler=229}
  [  2,  on] 612001283.0 Hz -33.0 dB {OFDM scaler=56897, Sine scaler=162}
  [  3,  on] 612000000.0 Hz -31.0 dB {OFDM scaler=56897, Sine scaler=204}
```

New Software Features in Cisco 1x2 / Compact Shelf RPD Software 7.3

The new software features for Cisco 1x2 / Compact Shelf RPD Software 7.3 release are:

TLV Error Handling Support

Cisco 1x2 / Compact Shelf RPD Software 7.3 release supports handling GCP/RCP errors. A number of error scenarios can arise in RCP protocol exchanges. There are two RCP TLVs defined to communicate the information helpful to identify the type of the error and the details of the underlying error condition. These TLVs are ResponseCode (TLV 19) and ErrorMessage (TLV 20). The Response Code provides a numerical identification of the error, while the ErrorMessage provides a human readable description of the error.

Table 1: Defined ResponseCode Values

Code Value	Mnemonic	Description	Example
0	NoError	The RPD reports that no errors occurred during operation.	Operation completed successfully.
1	GeneralError	An error has occurred. This is a catch-all code for all errors that do not fit the description of other specific error conditions. When returning this Error Code the RPD provides ErrorMessage TLV with additional information about the error.	No example is provided.
2	ResponseTooBig	The RPD could not place the results of the requested operation in a single RCP message.	The read request by the CCAP Core has specified a subtree of the RCP schema that results in a response that is over 64 KB, i.e., too big to fit in a single RCP message.

Code Value	Mnemonic	Description	Example
3	AttributeNotFound	The CCAP Core requested a read operation on an attribute or a set of attributes unrecognized by the RPD.	The CCAP Core attempts to read a TLV that the RPD does not recognize. For example the CCAP Core issued a read request for TLV 213, which is not defined.
4	BadIndex	The CCAP Core attempted to write to an attribute but it specified either no index or an index value outside of the range supported by the RPD. This error code can be also returned when the CCAP Core issued a Read request with at least one of the index values outside of the range supported by the RPD. This error code is also applicable when the CCAP Core uses a bad value of a channel, RF port or Ethernet port selector.	The RPD's capabilities indicate support for two DS RF ports. The CCAP Core issues a write request to set the BasePower for a DS RF port with index value of 2, which is outside of the valid range: 0..1.
5	WriteToReadOnly	The CCAP Core attempted to write to a read-only attribute.	A CCAP Core attempts to write to an upstream channel CenterFrequency attribute (TLV 65.4), which is defined as Read-only.
6	InconsistentValue	The value is inconsistent with values of other managed objects.	No example is provided.
7	WrongLength	The CCAP Core attempts to write a value with a TLV length that is inconsistent with the length required for the attribute.	A CCAP Core attempts to write to an Attribute BasePower (TLV 61.3) with TLV indicating a length of 1. The specification defines this attribute with TLV length of 2.

Code Value	Mnemonic	Description	Example
8	WrongValue	The value cannot be assigned to the attribute.	A CCAP Core attempts to write to an attribute RfMute (TLV 61.4) a value of 2, which is invalid.
9	ResourceUnavailable	Assigning the value to the variable requires allocation of resources that are currently unavailable.	A CCAP Core attempts to create or administratively enable OFDM channels that require resources shared with already-created or already-enabled SC-QAM channels.
10	AuthorizationFailure	A CC attempts to write to an attribute it does not own.	An Auxiliary CCAP Core attempted to write to an attribute only writeable by the active Principal Core, e.g., BasePower (TLV 61.3) attribute of the DS RF Port.
11	AttributeMissing	The RPD expected an attribute which was not provided.	The CCAP Core has attempted an AllocateWrite operation but has not included an attribute which is used to mark the table entry as allocated.
12	AllocationFailure	This error code is returned when the AllocateWrite operation fails because the table subject to the operation has no more entries available. No changes are made to any objects included in the sequence.	The CCAP Core attempted to allocate an entry in a table with AllocateWrite access but there are no more entries available.
13	AllocationNoOwner	This error code is returned when the AllocateWrite operation fails because the attribute set does not include a valid owner.	The CCAP Core attempted to allocate an entry in a table with AllocateWrite but did not include the CoreId.

Code Value	Mnemonic	Description	Example
14	ErrorProcessingUCD	The RPD encountered an error when processing a UCD Message sent from the CCAP Core.	A UCD message sent to the RPD is incorrectly formatted.
15	ErrorProcessingOCD	The RPD encountered an error when processing an OCD Message sent from the CCAP Core.	An OCD message sent to the RPD is incorrectly formatted.
16	ErrorProcessingDPD	The RPD encountered an error when processing a DPD Message sent from the CCAP Core.	A DPD message sent to the RPD is missing mandatory DOCSIS TLVs.
17	SessionIdInUse	A Session ID for a static pseudowire is already in use.	A CCAP Core attempts to provision a static pseudowire with a Session ID that is already in use by the RPD for the selected Ethernet port.
18	DoesNotExist	The RPD rejected an attempt to read a single Interface or Array ROT with an index set for an instance that does not exist, or the RPD rejected an attempt to write to a statically configured Interface or Array ROT instance that does not exist.	Example: The CCAP Core attempted to read a dynamically instantiated configuration object that had not been written first.

RPD Event Support

Cisco 1x2 / Compact Shelf RPD Software 7.3 release provides event support for 66070339, 66070226, 66070236, 66070225. Information of these events is listed in the following table:

Process	Sub-Process	RPD Priority	Event Message	Message Notes and Detail	Error Code Set	Event ID
Init	Config	Notice	Pending IRAs; Core ID: <P1>; <TAGS>;	P1 = CCAP Core ID	B703.38	66070339

Process	Sub-Process	RPD Priority	Event Message	Message Notes and Detail	Error Code Set	Event ID
Connectivity	Reconnect		Principal reconnect abandoned; CCAP Core ID: <P1>; CCAP Core IP: <P2>; <TAGS>;	P1 = CCAP Core ID P2 = CCAP Core IP address	B702.26	66070226
Connectivity	Handover		Core initiated handover; Failed Core IP: <P1>; Backup Core IP: <P2>; Requesting Core IP: <P3>; <TAGS>;	P1 = IP address of Failed Core P2 = IP address of Backup Core P3 = IP address of Core sending handover request	B702.36	66070236
Connectivity	Reconnect		Auxiliary reconnect abandoned; Failed Core IP: <P1>; Backup Core IP: <P2>; Requesting Core IP: <P3>; <TAGS>;	P1 = IP address of Failed Core P2 = IP address of Backup Core P3 = IP address of Core sending handover request	B702.25	66070225

SCP Support to Copy RPD Logfiles

Remotely retrieving log files from the RPD via scp is supported in Cisco 1x2 / Compact Shelf RPD Software 7.3 release. Leading to a simpler workflow for the customer and Cisco support teams. 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 copy-out of files and will not allow copying-in of files to the RPD.

Support for Optical Monitoring TLV-100.18

This feature supports a new TLV on RPHY to read the SFP-Plus object on RPD. This object provides detailed information about the SFP+ pluggable transceivers on the RPD Ethernet Interfaces. All the values in TLV 100.18 are supported with the exception of 100.18.34 - DigitalDiagA2Info.

This object is intended to convey information available from Digital Diagnostic Memory Map of the transceiver as defined in [SFP 8472].

- The CCAP Core MUST create an instance of the SfpPlusStatus object for every Ethernet interface on the RPD.
- The CCAP Core reads the SfpPlusStatus object with GCP TLV Type 100.18.

Support for local archive: Added local option to existing CLI

Using the command **logging [1588| corefile| provision]-archive local** can save a log archive to /rpd/archive on the RPD. This archive can then be transferred out or viewed locally.

Example:

```
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]
```

Security MIB Support

Cisco 1x2 / Compact Shelf RPD Software 7.3 release supports RpdCert (TLV 100.26), TrustAnchorCert (100.27) and Ieee8021xPaeSupplicantStatus (100.30) for security MIB.

- RpdCert—TLV100.26: This object describes the set of known Certificate Authority certificates acquired by the RPD, including Signing certificate and Device certificate.
- TrustAnchorCert—TLV100.27: This object describes the set of known Certificate Authority certificates use to validate certificates.
- Ieee8021xPaeSupplicantStatus—TLV100.30: This object reports status information for the IEEE 802.1x PAE RPD supplicant.

New Software Features in Cisco 1x2 / Compact Shelf RPD Software 7.2

The new software features for Cisco 1x2 / Compact Shelf RPD Software 7.2 release are:

RPD P2 Events implementation – Phase 2

RPD V7.2 release provides event support for 66070335, 66070224, 66070234, 66070229, 66070230. Information of these events is listed in the following table:

Process	Sub-Process	RPD Priority	Event Message	Message Notes and Detail	Error Code Set	Event ID
Init	Config	Error	Move to operational timeout; Core ID: <P1>; <TAGS>;	P1 = CCAP Core ID	B703.35	66070335
Connectivity	GCP		TCP failure; CCAP Core IP: <P1>; CCAP Core ID: <P2>; <TAGS>;	P1 = CCAP Core IP address P2 = CCAP Core ID (if known)	B702.24	66070224
Connectivity	Handover		Backup request rejected; Failed Core IP: <P1>; Backup Core IP: <P2>; <TAGS>;	P1 = IP address of Failed Core P2 = IP address of Backup Core	B702.34	66070234
Connectivity	Handover		Auxiliary handover started; Failed Core IP: <P1>; Backup Core IP: <P2>; <TAGS>;	P1 = IP address of Failed Core P2 = IP address of Backup Core	B702.29	66070229
Connectivity	Handover		Principal handover started; Failed Core IP: <P1>; Backup Core IP: <P2>; <TAGS>;	P1 = IP address of Failed Core P2 = IP address of Backup Core	B702.30	66070230

TLV 78.3 support

RPD V7.2 release provides support of TLV 78.3 HcsErrors, which allows the CCAP Core to read the number of bursts with detected HCS error in the DOCSIS header for the selected channel. You can check the HcsError in RPD CLI **show upstream iuc counter**, see the example below.

```
R-PHY#show upstream iuc counter 0 0
```

```
Channel Counters for physical channel 0/0, status valid(1)
+-------+----------+-------+----------+-------+-------+----------+----------+----------+-----+
|IUC    |  Grants  |Collide|  No      |Phy    |No     |   Good   | Corrected|Uncorrectd|
SNR |
|       |          |       |  Energy  |Errors |Preambl|   FEC    | FEC      |FEC       |
   |
+-------+----------+-------+----------+-------+-------+----------+----------+----------+-----+
|1-Req  |1274227   |0      |1274211   |0      |0      |0         |0         |0
|00.00|
|2-ReqD |0         |0      |0         |0      |0      |0         |0         |0
|00.00|
|3-Init |394       |0      |394       |0      |0      |0         |0         |0
|00.00|
|4-Maint|5         |0      |0         |0      |0      |5         |0         |0
|42.00|
|5-Short|0         |0      |0         |0      |0      |0         |0         |0
|00.00|
|6-Long |0         |0      |0         |0      |0      |0         |0         |0
|00.00|
|9-AShrt|7         |0      |0         |0      |0      |7         |0         |0
|42.00|
|10-ALng|63        |0      |0         |0      |0      |83        |0         |0
|43.00|
|11-AUGS|0         |0      |0         |0      |0      |0         |0         |0
|00.00|
+-------+----------+-------+----------+-------+-------+----------+----------+----------+-----+

Physical Channel 0/0 Counters:

DOCSIS 2.0 REQ Count:        0       DOCSIS 3.0 REQ Count:     2539
REQ Overflow Count  :        0       Delete Packet Count :        0       HCS ERR Count :
     115
High Byte Count :        0       Low Byte Count  :  1348846
Last Update Time 51.750970 s ago
```

RPD TACACS - disable local access if the server is available

When the TACACS server can be reached from RPD, user can only access RPD by TACACS account. Local access will be disabled, which means the user cannot access RPD by local account. But if the TACACS server cannot be reached, for example, a wrong server address, network issue, etc. the user can access RPD by local account.

New Software Features in Cisco 1x2 / Compact Shelf RPD Software 7.1

The new software features for Cisco 1x2 / Compact Shelf RPD Software 7.1 release are:

RPD P2 Events implementation – Phase 1

The RPD V7.1 release provides event support for 66070223 and 66070231. Information on these events is listed in the following table:

Process	Sub-Process	Event Message	Message Notes and Detail	Error Code Set	Event ID
Connectivity	GCP	GCP keepalive failure; CCAP Core IP: <P1>; CCAP Core ID: <P2>; <TAGS>;	P1 = CCAP Core IP address P2 = CCAP Core ID	B702.23	66070223
Connectivity	Ethernet Interface	CIN link timeout; Port: <P1>; <TAGS>;	P1 = Ethernet port number	B702.31	66070231

TLV 60.13 and 60.14 support

The RPD V7.1 release provides support of new TLV 60.13 GcpBackupConnectionConfig and 60.14 CandidateBackupCoreTable as described below:

- **60.13 GcpBackupConnectionConfig**: Currently, RPD only support the default value “connection”. The default value always allow a backup mode core to maintain GCP control connection. This TLV can be used to support the MIB items **docsRphyRpdDevCoresConnectedTable** and **docsRphyRpdDevCoresConnectedGcpBackupConnectionConfig**

  .
- **60.14 CandidateBackupCoreTable**: It provides a list of potential backup cores. Index (60.14.1) and BackupCoreIpAddress(60.14.2) of the core based on the Cisco internal TLV 200 **RedundantCoreIpAddress**. It can be used to support the MIB table **docsRphyRpdDevCandidateBackupCoresTable**.

New Hardware Features in Cisco 1x2 / Compact Shelf RPD Software 7.8.2

There are no new hardware features for Cisco 1x2 / Compact Shelf RPD Software 7.8.2 release.

New Hardware Features in Cisco 1x2 / Compact Shelf RPD Software 7.8.1

There are no new hardware features for Cisco 1x2 / Compact Shelf RPD Software 7.8.1 release.

New Hardware Features in Cisco 1x2 / Compact Shelf RPD Software 7.8

There are no new hardware features for Cisco 1x2 / Compact Shelf RPD Software 7.8 release.

New Hardware Features in Cisco 1x2 / Compact Shelf RPD Software 7.7

There are no new hardware features for Cisco 1x2 / Compact Shelf RPD Software 7.7 release.

New Hardware Features in Cisco 1x2 / Compact Shelf RPD Software 7.6.1

There are no new hardware features for Cisco 1x2 / Compact Shelf RPD Software 7.6.1 release.

New Hardware Features in Cisco 1x2 / Compact Shelf RPD Software 7.6

There are no new hardware features for Cisco 1x2 / Compact Shelf RPD Software 7.6 release.

New Hardware Features in Cisco 1x2 / Compact Shelf RPD Software 7.5

There are no new hardware features for Cisco 1x2 / Compact Shelf RPD Software 7.5 release.

New Hardware Features in Cisco 1x2 / Compact Shelf RPD Software 7.4.1

There are no new hardware features for Cisco 1x2 / Compact Shelf RPD Software 7.4.1 release.

New Hardware Features in Cisco 1x2 / Compact Shelf RPD Software 7.4

There are no new hardware features for Cisco 1x2 / Compact Shelf RPD Software 7.4 release.

New Hardware Features in Cisco 1x2 / Compact Shelf RPD Software 7.3

There are no new hardware features for Cisco 1x2 / Compact Shelf RPD Software 7.3 release.

New Hardware Features in Cisco 1x2 / Compact Shelf RPD Software 7.2

There are no new hardware features for Cisco 1x2 / Compact Shelf RPD Software 7.2 release.

New Hardware Features in Cisco 1x2 / Compact Shelf RPD Software 7.1

There are no new hardware features for Cisco 1x2 / Compact Shelf RPD Software 7.1 release.

Behaviour Changes Introduced Features

Modified Software Features in Cisco 1x2 / Compact Shelf RPD Software 7.8.2

There are no modified software features for Cisco 1x2 / Compact Shelf RPD Software 7.8.2 release.

Modified Software Features in Cisco 1x2 / Compact Shelf RPD Software 7.8.1

There are no modified software features for Cisco 1x2 / Compact Shelf RPD Software 7.8.1 release.

Modified Software Features in Cisco 1x2 / Compact Shelf RPD Software 7.8

There are no modified software features for Cisco 1x2 / Compact Shelf RPD Software 7.8 release.

Modified Software Features in Cisco 1x2 / Compact Shelf RPD Software 7.7

There are no modified software features for Cisco 1x2 / Compact Shelf RPD Software 7.7 release.

Modified Software Features in Cisco 1x2 / Compact Shelf RPD Software 7.6.1

There are no modified software features for Cisco 1x2 / Compact Shelf RPD Software 7.6.1 release.

Modified Software Features in Cisco 1x2 / Compact Shelf RPD Software 7.6

There are no modified software features for Cisco 1x2 / Compact Shelf RPD Software 7.6 release.

Modified Software Features in Cisco 1x2 / Compact Shelf RPD Software 7.5

There are no modified software features for Cisco 1x2 / Compact Shelf RPD Software 7.5 release.

Modified Software Features in Cisco 1x2 / Compact Shelf RPD Software 7.4.1

There are no modified software features for Cisco 1x2 / Compact Shelf RPD Software 7.4.1 release.

Modified Software Features in Cisco 1x2 / Compact Shelf RPD Software 7.4

There are no modified software features for Cisco 1x2 / Compact Shelf RPD Software 7.4 release.

Modified Software Features in Cisco 1x2 / Compact Shelf RPD Software 7.3

There are no modified software features for Cisco 1x2 / Compact Shelf RPD Software 7.3 release.

Modified Software Features in Cisco 1x2 / Compact Shelf RPD Software 7.2

There are no modified software features for Cisco 1x2 / Compact Shelf RPD Software 7.2 release.

Modified Software Features in Cisco 1x2 / Compact Shelf RPD Software 7.1

There are no modified software features for Cisco 1x2 / Compact Shelf RPD Software 7.1 release.

Integrated Software Features in Cisco 1x2 / Compact Shelf RPD Software 7.8.2

There are no integrated software features for Cisco 1x2 / Compact Shelf RPD Software 7.8.2 release.

Integrated Software Features in Cisco 1x2 / Compact Shelf RPD Software 7.8.1

There are no integrated software features for Cisco 1x2 / Compact Shelf RPD Software 7.8.1 release.

Integrated Software Features in Cisco 1x2 / Compact Shelf RPD Software 7.8

There are no integrated software features for Cisco 1x2 / Compact Shelf RPD Software 7.8 release.

Integrated Software Features in Cisco 1x2 / Compact Shelf RPD Software 7.7

There are no integrated software features for Cisco 1x2 / Compact Shelf RPD Software 7.7 release.

Integrated Software Features in Cisco 1x2 / Compact Shelf RPD Software 7.6.1

There are no integrated software features for Cisco 1x2 / Compact Shelf RPD Software 7.6.1 release.

Integrated Software Features in Cisco 1x2 / Compact Shelf RPD Software 7.6

There are no integrated software features for Cisco 1x2 / Compact Shelf RPD Software 7.6 release.

Integrated Software Features in Cisco 1x2 / Compact Shelf RPD Software 7.5

There are no integrated software features for Cisco 1x2 / Compact Shelf RPD Software 7.5 release.

Integrated Software Features in Cisco 1x2 / Compact Shelf RPD Software 7.4.1

There are no integrated software features for Cisco 1x2 / Compact Shelf RPD Software 7.4.1 release.

Integrated Software Features in Cisco 1x2 / Compact Shelf RPD Software 7.4

There are no integrated software features for Cisco 1x2 / Compact Shelf RPD Software 7.4 release.

Integrated Software Features in Cisco 1x2 / Compact Shelf RPD Software 7.3

There are no integrated software features for Cisco 1x2 / Compact Shelf RPD Software 7.3 release.

Integrated Software Features in Cisco 1x2 / Compact Shelf RPD Software 7.2

There are no integrated software features for Cisco 1x2 / Compact Shelf RPD Software 7.2 release.

Integrated Software Features in Cisco 1x2 / Compact Shelf RPD Software 7.1

There are no new integrated software features for Cisco 1x2 / Compact Shelf RPD Software 7.1 release.