Introduction

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.

This Release Notes contain information about downloading and installing Cisco 1x2 / Compact Shelf RPD Software 6.4 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 6.4 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.

Note Cisco 1x2 / Compact Shelf RPD Software 6.4 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.

This chapter includes the following sections:

System Requirements

These sections describe the system requirements for Cisco 1x2 / Compact Shelf RPD Software 6.4 and its maintenance releases:

Memory Requirements for Cisco 1x2 / Compact Shelf RPD Software 6.4

Note Memory is not configurable for the Cisco Remote PHY device.

Table 1: Memory Recommendations for the Cisco Remote PHY Device

Feature Set	Cisco RPHY Processor	Software Image	Fixed Memory	Runs From
CISCO RPHY 6.4	NXP LS1043A	RPD-V6-4.itb.SSA	1G Bytes	Bootflash:

Hardware Supported

For detailed information about the hardware supported in Cisco 1x2 / Compact Shelf RPD Software 6.4 and its maintenance releases, see:

http://www.cisco.com/c/en/us/td/docs/cable/cbr/installation/guide/b_cbr_how_and_what_to_order.html.

Determining the Software Version of Cisco 1x2 / Compact Shelf RPD Software 6.4

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 v6.4, build by rpd-release, on 2019-03-25 22:57:22
Branch information:
        RPD branch: (detached from RPD_V6_4_20190326)
        OpenRPD branch: (detached from RPD_V6_4_20190326)
        SeresRPD branch: (detached from RPD_V6_4_20190326)
```

Note The system image file name of the factory installed image is */bootflash/RPD-V6.4_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-V6-4.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 6.4

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

TACACS+ support

Starting from Cisco 1x2 / Compact Shelf RPD Software 6.4, TACACS+ is supported.

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

Note

1. RPD can configure 8 TACACS servers at the most. All configured servers use the same secret key.
2. If multiple TACACS servers are configured, RPD will try to connect TACACS server in the order in which the servers are configured until the connection is established successfully.
3. RPD and TACACS server must use same address family.

Enabling TACACS+ on RPD

To enable TACACS+, user needs to setup a TACACS server with secret key configured. Then add this TACACS server's IPv4/IPv6 address and key to RPD configuration.

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

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

User can also delete server and change the secret key.

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

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

Displaying configured TACACS server

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

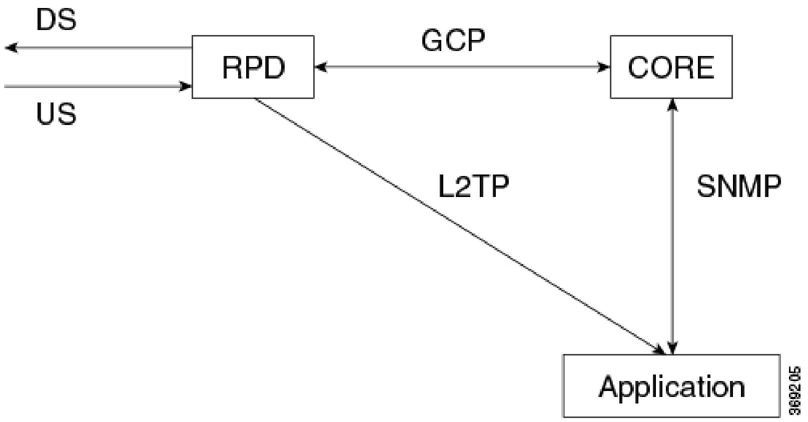
Starting from Cisco 1x2 / Compact Shelf RPD Software 6.4, TLV 100 RpdInfo read count and read by key is supported.

Spectrum capture support

Starting from Cisco 1x2 / Compact Shelf RPD Software 6.4, Spectrum capture is supported.

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



Note 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:

https://www.cisco.com/c/en/us/td/docs/cable/cbr/configuration/guide/b_cbr_docsis_full_book_xe16_10/b_cbr_docsis_full_book_xe16_10_chapter_0100110.html

Note

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.

Verifying spectrum capture on RPD

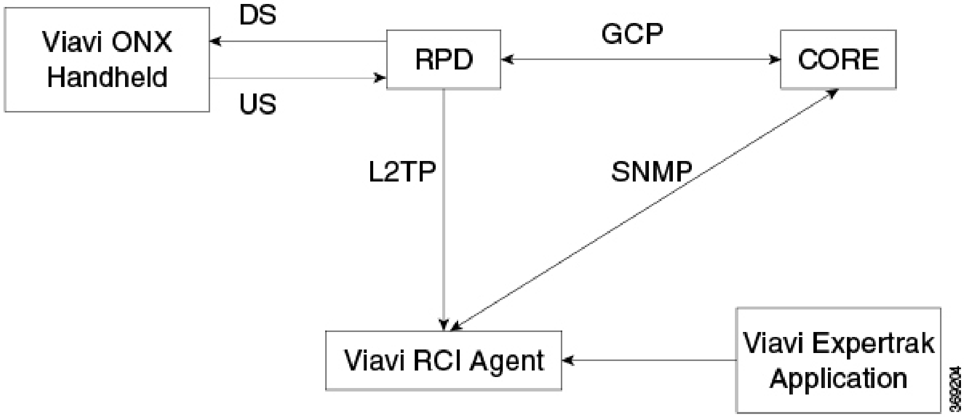
To verify if the spectrum capture is enabled, use **show bcm-register wbfft config** command as shown in the following example. The WBFFT Trigger Mode should be FreeRunning if this feature is enabled.

```
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
WBFFT MIDL WDW CF  [cc00002c]      : 000061E0
WBFFT MAX CTL      [d0000048]      : 33800000
WBFFT Status       [cc000034]      : 00000000

WBFFTS In Ctrl     [d0000044]      : 00000100
WBFFT PKT BYTE                     : 004A0000
WBFFT PKT COUNT                    : 00004A00
```

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



Note

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.

Verifying spectrum capture on RPD

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 Triger 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   [cc000000]     : 00000005
In Control         [cc000004]     : 00472F04
Out Control        [cc00000c]     : 00000099
Timing Ctrl        [cc000010]     : 00000003
WBFFT FIRST WDW CF [cc000024]     : 00000920
WBFFT SCND WDW CF  [cc000028]     : 0000C660
WBFFT MIDL WDW CF  [cc00002c]     : 000061E0
WBFFT MAX CTL      [d0000048]     : 39C00000
WBFFT Status       [cc000034]     : 00000080

WBFFTS In Ctrl     [d0000044]     : 00000100
WBFFT PKT BYTE                    : 01557D00
WBFFT PKT COUNT                   : 0001557D
```

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.
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

Below is the warning event that is triggered when the default password for admin account is used to login RPD:

RPD Priority	Event Message	Event ID
Warning	Rpd default login credentials detected in use - please change password immediately	2148075527

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 2: AnalogTxPower Object

Attribute Name	Type	Access	Type constraints	Units	TLV Type
TxIndex	UnsignedByte	Key			21.13.1
MajorLowTH	UnsignedShort	Write-only			21.13.2
MinorLowTH	UnsignedShort	Write-only			21.13.3
NormalTH	UnsignedShort	Write-only			21.13.4

Attribute Name	Type	Access	Type constraints	Units	TLV Type
MinorHighTH	UnsignedShort	Write-only			21.13.5

Table 3: AnalogRxPower Object

Attribute Name	Type	Access	Type constraints	Units	TLV Type
RxIndex	UnsignedByte	Key			21.14.1
MajorLowTH	UnsignedShort	Write-only			21.14.2
MinorLowTH	UnsignedShort	Write-only			21.14.3
NormalTH	UnsignedShort	Write-only			21.14.4
MinorHighTH	UnsignedShort	Write-only			21.14.5

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

```
R-PHY#show environment table 49
sensor_id: 49
name: TX1_OPT_PWR_MON
type: power
unit: mW
state            low            high
------------------------------------
MAJOR-LOW        N/A            0.00
MINOR-LOW        0.00           0.49
NORMAL           0.50           0.99
MINOR-HIGH       1.00           1.49
MAJOR-HIGH       1.50           N/A
poll_interval: 2
sensor_state: N/A
sensor_value: N/A

Configured Values (Currently Used Values):

state            low            high
------------------------------------
MAJOR-LOW        N/A            0.00
MINOR-LOW        0.00           0.49
NORMAL           0.50           0.99
MINOR-HIGH       1.00           1.49
MAJOR-HIGH       1.50           N/A
sensor_state: N/A
R-PHY#show environment table 50
sensor_id: 50
name: RX1_OPT_PWR_MON
type: power
unit: mW
state            low            high
------------------------------------
MAJOR-LOW        N/A            0.00
MINOR-LOW        0.00           0.49
NORMAL           0.50           1.49
MINOR-HIGH       1.50           1.99
MAJOR-HIGH       2.00           N/A
```

```
poll_interval: 2
sensor_state: N/A
sensor_value: N/A

Configured Values (Currently Used Values):
state            low            high
------------------------------------
MAJOR-LOW        N/A            0.00
MINOR-LOW        0.00           0.49
NORMAL           0.50           1.49
MINOR-HIGH       1.50           1.99
MAJOR-HIGH       2.00           N/A
sensor_state: N/A
```

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 4: Supported events for DHCPv6

Process	Sub-Process	RPD Priority	Event Message	Message Notes and Detail	Error Code Set	Event ID
DHCP		Error	DHCP RENEW sent - No response for <P1><P2><TAGS>	• P1= IPv4 or IPv6 • P2 = RPD interface number (EnetPortIndex)	B703.0	66070300
DHCP		Error	DHCP REBIND sent - No response for <P1><P2><TAGS>	• P1=IPv4 or IPv6 • P2 = RPD interface number (EnetPortIndex)	B703.1	66070301

Process	Sub-Process	RPD Priority	Event Message	Message Notes and Detail	Error Code Set	Event ID
DHCP		Error	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	DHCP RENEW FAILED - Critical field invalid in response<P1><TAGS>	P1 = RPD interface number (EnetPortIndex)	B703.3	66070303
DHCP		Error	DHCP REBIND WARNING - Field invalid in response<P1><TAGS>	P1 = RPD interface number (EnetPortIndex)	B703.4	66070304
DHCP		Critical	DHCP REBIND FAILED - Critical field invalid in response<P1><TAGS>	P1 = RPD interface number (EnetPortIndex)	B703.5	66070305

Table 5: Supported network events

Process	Sub-Process	RPD Priority	Event Message	Message Notes and Detail	Error Code Set	Event ID
Init	Network Authentication	Error	Network Authentication Error; Descr: <P1>; <TAGS>;	P1 = Authentication error description	B701.0	66070104
Init	Network Authentication	Notice	Network Authentication Success; <TAGS>;		B701.4	66070105
Connectivity	CCAP Core	Notice	Successfully connected to Core; Core ID: <P1>; <TAGS>;	P1 = CCAP Core ID to which the connection was completed	B702.19	66070219
Connectivity	CCAP Core	Warning	Connection lost - Auxiliary CCAP Core. Reconnect attempted; Core ID: <P1>; <TAGS>;	P1 = Auxiliary CCAP Core ID to which the connection was lost.	B702.20	66070220

Process	Sub-Process	RPD Priority	Event Message	Message Notes and Detail	Error Code Set	Event ID
Connectivity	CCAP Core	Warning	Connection lost – Principal CCAP Core. Reconnect attempted; Core ID: <P1>; <TAGS>;	P1 = Principal CCAP Core ID to which the connection was lost.	B702.21	66070221
Connectivity	CCAP Core	Notice	Successfully reconnected to Core; Core ID: <P1>; <TAGS>;	P1 = CCAP Core ID to which the connection was completed	B702.22	66070222
Init	IPv4 Address Acquisition	Notice	Successfully obtained IPv4 address; <TAGS>;		B703.24	66070324
Init	IPv6 Address Acquisition	Notice	Successfully obtained IPv6 address; <TAGS>;		B703.25	66070325
Init	TOD	Notice	Successfully obtained ToD; <TAGS>;		B703.26	66070326
Init	Config	Error	Received unknown RCP message from Core; Core ID: <P1>; Descr: <P2>; <TAGS>;	P1 = CCAP Core ID P2 = Error description	B703.27	66070327
Init	Config	Error	Received RCP message from Core, not allowed in current state; Message: <P1>; Core ID: <P2>; State: <P3>; <TAGS>;	P1 = RCP message P2 = CCAP Core ID P3 = Current TopLevelRPDState	B703.28	66070328
Init	IRA	Error	No IRA received after Notify message to Core; Core IP: <P1>; <TAGS>;	P1 = CCAP Core IP address	B703.29	66070329
Init	IRA	Error	No REX received after IRA from Core; Core ID: <P1>; Core IP: <P2>; <TAGS>;	P1 = CCAP Core ID P2 = CCAP Core IP address	B703.30	66070330

Process	Sub-Process	RPD Priority	Event Message	Message Notes and Detail	Error Code Set	Event ID
Init	Initialization	Critical	Failure occurred during local RPD initialization process. RPD reset; Descr: <P1>; <TAGS>;	P1 is optional P1 = Vendor Specific Event or Text	B708.0	66070800

Factory reset support

Starting from Cisco 1x2 / Compact Shelf RPD Software 6.1, factory reset and NVRAM reset via TLV and CLI 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 6.4

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

Leakage Detection Meter

The leakage detection tone's power adjust range is updated from -36.0 to -21.0 dBmV in release 6.3 to -36.0 to -18.0 dBmV in release 6.4.

Enhancement of RPD allows invalid SSH to be written

When user adds SSH public key, RPD checks the format and tries to calculate an MD5 fingerprint from the input SSH-RSA key. For example:

```
R-PHY(config)#ssh pubkey add 1234 1341413431413
Incorrect format of pubkey. It should start with 'ssh-rsa'

R-PHY(config)#ssh pubkey add ssh-rsa ABCDEFGHJKLMNOPQRSTUVWXYZ1234567890 test@test
Exception met while calculating fingerpint: Incorrect padding

R-PHY(config)#ssh pubkey add ssh-rsa
[illegible]
 pyats@sh-cable-vnc-8
Pubkey added. Certificate fingerprint (MD5): 22:14:23:35:94:7e:1b:fa:04:f3:37:4d:99:0d:ca:f8
```

Integrated Software Features in Cisco 1x2 / Compact Shelf RPD Software 6.4

There are no integrated features in Cisco 1x2 / Compact Shelf RPD Software 6.4 release.

New Hardware Features in Cisco 1x2 / Compact Shelf RPD Software 6.4

There are no new hardware features for Cisco 1x2 / Compact Shelf RPD Software 6.4 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:

http://tools.cisco.com/ITDIT/MIBS/servlet/index

To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check verifies that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password is e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

http://tools.cisco.com/RPF/register/register.do

MIBs in Cisco 1x2 / Compact Shelf RPD Software 6.4

There are no new MIBs in Cisco 1x2 / Compact Shelf RPD Software 6.4.

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.