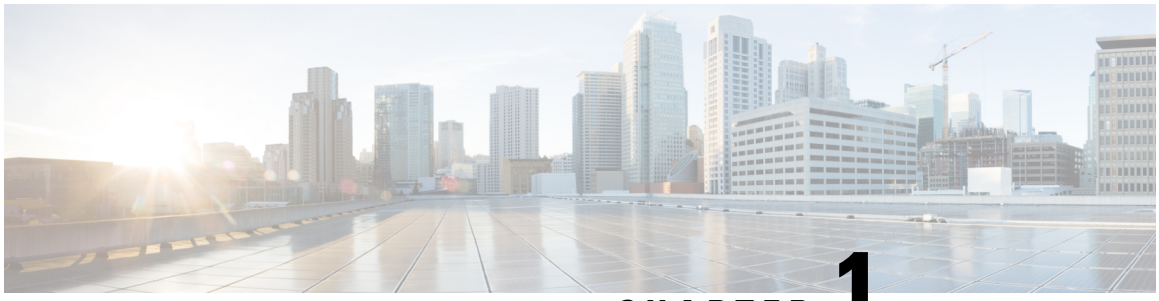
# Release Notes for Cisco NCS 4206 and Cisco NCS 4216 Series, Cisco IOS XE 17.15.x

**First Published:** 2024-08-14

**Last Modified:** 2025-05-29

**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

# CONTENTS



CHAPTER 1

# Introduction

This document provides information about the IOS XE software release for the Cisco NCS 4206 and Cisco NCS 4216 beginning with Cisco IOS XE Release 3.18SP.



# Overview of Cisco NCS 4206 and NCS 4216

## Cisco NCS 4206

The Cisco NCS 4206 is a fully-featured aggregation platform designed for the cost-effective delivery of converged mobile and business services. With shallow depth, low power consumption, and an extended temperature range, this compact 3-rack-unit (RU) chassis provides high service scale, full redundancy, and flexible hardware configuration.

The Cisco NCS 4206 expands the Cisco service provider product portfolio by providing a rich and scalable feature set of Layer 2 VPN (L2VPN) and Layer 3 VPN (L3VPN) services in a compact package. It also supports a variety of software features, including Carrier Ethernet features, Timing over Packet, and pseudowire.

For more information on the Cisco NCS 4206 Chassis, see the Cisco NCS 4206 Hardware Installation Guide.

## Cisco NCS 4216

The Cisco NCS 4216 is a seven-rack (7RU) unit chassis that belongs to the Cisco NCS 4200 family of chassis. This chassis complements Cisco's offerings for IP RAN solutions for the GSM, UMTS, LTE and CDMA. Given it's form-factor, interface types and Gigabit Ethernet density the Cisco NCS 4216 can also be positioned as a Carrier Ethernet aggregation platform.

The Cisco NCS 4216 is a cost optimized, fully redundant, centralized forwarding, extended temperature, and flexible pre-aggregation chassis.

For more information about the Cisco NCS 4216 Chassis, see the Cisco NCS 4216 Hardware Installation Guide.

#### NCS 4216 14RU

The Cisco NCS 4216 F2B is a 14-rack unit router that belongs to the Cisco NCS 4200 family of routers. This router complements Cisco's offerings for IP RAN solutions for the GSM, UMTS, LTE, and CDMA. Given its form-factor, interface types, and Gigabit Ethernet density the Cisco NCS 4216 14RU can also be positioned as a Carrier Ethernet aggregation platform.

The Cisco NCS 4216 14RU is a cost optimized, fully redundant, centralized forwarding, extended temperature, and flexible pre-aggregation router.

For more information about the Cisco NCS 4216 F2B Chassis, see the Cisco NCS 4216 F2B Hardware Installation Guide.

# Feature Navigator

You can use Cisco Feature Navigator to find information about feature, platform, and software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on cisco.com is not required.

# Hardware Supported

The following sections list the hardware supported for Cisco NCS 4206 and Cisco NCS 4216 chassis.

## Cisco NCS 4206 Supported Interface Modules

### Supported Interface Modules

**Note** If the **license feature service-offload enable** command is configured, then the NCS4200-1T8LR-PS IM is not supported in the router for RSP3.

**Note** There are certain restrictions in using the interface modules on different slots in the chassis. Contact Cisco Sales/Support for the valid combinations.

**Note** FAN OIR is applicable every time the IM based fan speed profile is switched to NCS4200-1H-PK= and NCS4200-2Q-P interface modules. Even though the IMs remain in the Out-of-Service state, they are still considered as present in the chassis.

*Table 1: NCS420X-RSP Supported Interface Modules and Part Numbers*

| RSP Module | Supported Interface Modules | Part Numbers | Slot |
|---|---|---|---|
| NCS420X-RSP | 8-port 10 Gigabit Ethernet Interface Module (8X10GE) | NCS4200-8T-PS | All |
| | 1-port 100 Gigabit Ethernet Interface Module (1X100GE) | NCS4200-1H-PK= | 4 and 5 |
| | 2-port 40 Gigabit Ethernet QSFP Interface Module (2X40GE) | NCS4200-2Q-P | 4 and 5 |
| | 8/16-port 1 Gigabit Ethernet (SFP/SFP) + 1-port 10 Gigabit Ethernet (SFP+) / 2-port 1 Gigabit Ethernet (CSFP) Interface Module | NCS4200-1T16G-PS | 0,3,4, and 5 |
| | 1-port OC-192 Interface module or 8-port Low Rate Interface Module | NCS4200-1T8S-10CS | 2,3,4, and 5 |
| | NCS 4200 1-Port OC-192 or 8-Port Low Rate CEM 20G Bandwidth Interface Module | NCS4200-1T8S-20CS | 2,3,4, and 5[1] |
| | 48-port T1/E1 CEM Interface Module | NCS4200-48T1E1-CE | All |
| | 48-port T3/E3 CEM Interface Module | NCS4200-48T3E3-CE | All |
| | 2-port 100 Gigabit Ethernet (QSFP) Interface Module (2X100GE)[2] | NCS4200-2H-PQ | 4,5 |
| | 1-port OC48[3]/ STM-16 or 4-port OC-12/OC-3 / STM-1/STM-4 + 12-port T1/E1 + 4-Port T3/E3 CEM Interface Module | NCS4200-3GMS | 2,3,4, and 5 |

1 These slots are supported on 10G or 20G mode.
2 IM supports only one port of 100G with RSP3 as QSFP28 on Port 0 in both slots 4 and 5.
3 If OC48 is enabled, then the remaining 3 ports are disabled.

*Table 2: NCS420X-RSP-128 Supported Interface Modules and Part Numbers*

| RSP Module | Supported Interface Modules | Part Numbers | Slot |
|---|---|---|---|
| NCS420X-RSP | SFP Combo IM—8-port Gigabit Ethernet (8X1GE) + 1-port 10 Gigabit Ethernet Interface Module (1X10GE) | NCS4200-1T8LR-PS | All |
| | 8-port T1/E1 CEM Interface Module | NCS4200-8E1T1-CE | All |
| | 1-port OC48[4]/ STM-16 or 4-port OC-12/OC-3 / STM-1/STM-4 + 12-port T1/E1 + 4-Port T3/E3 CEM Interface Module | NCS4200-3GMS | 2,3,4, and 5 |

4 If OC48 is enabled, then the remaining 3 ports are disabled.

# Cisco NCS 4216 Supported Interface Modules

For information on supported interface modules, see Supported Interface Modules.

# Cisco NCS 4216 F2B Supported Interface Modules

For information on supported interface modules, see Supported Interface Modules.

# Restrictions and Limitations

**Note** The error message "PLATFORM-1-NOSPACE: SD bootflash : no space alarm assert" may occur in the following scenarios:

- Any sector of SD Card gets corrupted
- Improper shut down of router
- power outage.

This issue is observed on platforms which use EXT2 file systems.

We recommend performing a reload of the router. As a result, above alarm will not be seen during the next reload due to FSCK(file systems check) execution.

However, If the error persists after a router reload, we recommend to format the bootflash or FSCK manually from IOS.

- Embedded Packet Capture (EPC) is not supported on ASR 900 routers.
- From the Cisco IOS XE 16.6.1 releases, In-Service Software Upgrade (ISSU) is not supported on the router to the latest releases. For more information on the compatible release versions, see ISSU Support Matrix.
- ISSU is not supported between a Cisco IOS XE 3S release and the Cisco IOS XE Bengaluru 17.6.x release.
- The port restriction on 1-port OC-192 or 8-port low rate CEM interface module is on port pair groups. If you have OC48 configured on a port, the possible port pair groups are 0–1, 2–3, 4–5, 6–7. If one of the ports within this port group is configured with OC48 rate, the other port cannot be used.
- RS422 pinout works only on ports 0–7.
- The **ip cef accounting** command is *not* supported on the router.
- Configuration sync does *not* happen on the Standby RSP when the active RSP has Cisco Software Licensing configured, and the standby RSP has Smart Licensing configured on the router. If the active RSP has Smart Licensing configured, the state of the standby RSP is undetermined. The state could be pending or authorized as the sync between the RSP modules is not performed.
- Evaluation mode feature licenses may not be available to use after disabling, and enabling the smart licensing on the RSP2 module. A reload of the router is required.

- Ingress counters are not incremented for packets of the below format on the RSP3 module for the 10-Gigabit Ethernet interfaces, 100-Gigabit Ethernet interfaces, and 40-Gigabit Ethernet interfaces:

  **Packet Format**

  MAC header---->VLAN header---->Length/Type

  When these packets are received on the RSP3 module, the packets are not dropped, but the counters are not incremented.

- T1 SAToP, T3 SAToP, and CT3 are supported on an UPSR ring only with local connect mode. Cross-connect configuration of T1, T3, and CT3 circuits to UPSR are not supported.
- PTP is not supported when 8-port 10-Gigabit Ethernet interface module is in oversubscribed mode.
- Port channel 61–64 is not supported in the 16.11.1a release. The range of configurable port channel interfaces has been limited to 60.
- Effective with Cisco IOS XE Everest 16.6.1, the VPLS over Port-channel (PoCH) scale is reduced from 48 to 24 for Cisco ASR 903 RSP3 module.

**Note** The PoCH scale for Cisco ASR 907 routers is 48.

- The frame drops may occur for packets with packet size of less than 100 bytes, when there is a line rate of traffic over all 1G or 10G interfaces available in the system. This restriction is applicable only on RSP2 module, and is not applicable for RSP3 module.
- One Ternary Content-Addressable Memory (TCAM) entry is utilized for Segment Routing Performance Measurement. This is required for the hardware timestamping to function.
- While performing an auto upgrade of ROMMON, only primary partition is upgraded. Use the **upgrade rom-mon filename** command to upgrade the secondary partition of the ROMMON during the auto upgrade. However, the router can be reloaded during the next planned reload to complete the secondary ROMMON upgrade. This is applicable to ASR 903 and ASR 907 routers.
- In the Cisco IOS XE 17.1.1 release, the EVPN EVI type is VLAN-based by default, and while configuring for the EVPN EVI type, it is recommended to configure the EVPN EVI type as VLAN-based, VLAN bundle and VLAN aware model.
- For Cisco IOS XE Gibraltar Release 16.9.5, Cisco IOS XE Gibraltar Release 16.12.3, and Cisco IOS XE Amsterdam 17.1.x, a minimum disk space of 2 MB is required in the boot flash memory file system for a successful ROMMON auto upgrade process. For a disk space lesser than 2 MB, ROMMON auto upgrade fails and the router reboots. This is applicable to Cisco ASR 903 and Cisco ASR 907 routers.
- In the Cisco IOS XE 16.12.1, 17.1.1, and 17.2.1 releases, IPsec is not supported on the Cisco RSP3 module.
- CEM circuit provisioning issues may occur during downgrade from Cisco IOS XE Amsterdam 17.3.1 to any lower versions or during upgrade to Cisco IOS XE Amsterdam 17.3.1 from any lower versions, if the CEM scale values are greater than 10500 APS/UPSR in protected CEM circuits. So, ensure that the CEM scale values are not greater than 10500, during ISSU to or from 17.3.1.
- Some router models are not fully compliant with all IETF guidelines as exemplified by running the pyang tool with the **lint** flag. The errors and warnings that are exhibited by running the pyang tool with the **lint** flag are currently noncritical as they do not impact the semantic of the models or prevent the models

from being used as part of the toolchains. A script has been provided, "check-models.sh", that runs pyang with **lint** validation enabled, but ignoring certain errors. This allows the developer to determine what issues may be present.

As part of model validation for the Cisco IOS XE Amsterdam 17.3.1 release, "LEAFREF_IDENTIFIER_NOT_FOUND" and "STRICT_XPATH_FUNCTIONS" error types are ignored.

- Test Access Port (TAP) is not supported when the iMSG VLAN handoff feature is enabled on the same node.
- Data Communication Channel (DCC) is not supported in the NCS4200-1T8S-20CS interface module for the Cisco IOS XE Cupertino 17.8.1 release.
- In Cisco IOS XE Dublin 17.12.1, for mLDP Partitioned multicast distribution tree (MDT) to work with PIM-Sparse Mode (SM) traffic, configure only a single ingress PE and ensure that the **strict-rpf interface** command is disabled. Configuring multiple PE ingress is not allowed.
- SF and SD alarms are not supported on T1 and T3 ports for the following interface modules:
  - NCS4200-3GMS
  - NCS4200-48T3E3-CE
  - NCS4200-48T1E1-CE
- In RSP2 and RSP3 modules, during In-Service Software Upgrade (ISSU), interface modules undergo FPGA upgrade.

  The following table details the IM Cisco IOS XE versions during ISSU with respect to FPGA upgrade and the impact of traffic flow for these IMs:

***Table 3: Impact on IM during ISSU and FPGA Upgrade***

| IM | IM Version During ISSU | Pre-ISSU FPGA Upgrade | Post-ISSU Impact on IM | FPGA Version post ISSU |
|---|---|---|---|---|
| Phase 1 | Cisco IOS XE 17.3.x or earlier version to Cisco IOS XE 17.4.x | FPGA upgrade completes and IM starts after the reload process.<br>FPGA version (phase -1) - 0.47 | Traffic is impacted during upgrade. | 0.75 |
| Phases 1 and 2 | Version earlier to Cisco IOS XE 17.8.x | FPGA upgrade completes and IM starts after the reload process.<br>• FPGA version (Phase 1)— 0.47<br>• FPGA version (Phase 2)<br>• NCS4200-8T-PS—69.22<br>• Combo IM: 69.24 | Traffic is impacted during upgrade. | • FPGA version (Phase 1)—0.75<br>• FPGA version (Phase 2)<br>• NCS4200-8T-PS—69.24<br>• Combo IM: 69.32 |

| IM | IM Version During ISSU | Pre-ISSU FPGA Upgrade | Post-ISSU Impact on IM | FPGA Version post ISSU |
|---|---|---|---|---|
| Phase 1 | Cisco IOS XE 17.4.1 or later versions to Cisco IOS XE 17.8.1 | IM FPGA already upgraded with the latest version and reload is not required. | Traffic is not impacted. | 0.75 |

For more information on the FPGA versions, see Supported FPGA Versions.

Refer the following table for supported IMs:

***Table 4: NCS 4200 Supported Ethernet Interface Module***

| Phase 1 IM | Phase 2 IM | Phase 3 IM |
|---|---|---|
| NCS4200-1T8LR | NCS4200-1T8LR-PS | NCS4200-8T-PS |
| | | NCS4200-2Q-P |
| | | NCS4200-2H-PQ |

# Determining the Software Version

You can use the following commands to verify your software version:

- Consolidated Package—**show version**
- Individual sub-packages—**show version installed** (lists all installed packages)

# Upgrading to a New Software Release

Only the latest consolidated packages can be downloaded from Cisco.com; users who want to run the router using individual subpackages must first download the image from Cisco.com and extract the individual subpackages from the consolidated package.

For information about upgrading to a new software release, see the Upgrading the Software on the Cisco NCS 4200 Series Routers .

### Upgrading the FPD Firmware

FPD Firmware packages are bundled with the software package. FPD upgrade is automatically performed ont the router.

If you like to manually change the FPD Firmware software, use the **upgrade hw-module subslot 0/0 fpd bundle** to perform FPD frmware upgrade.

# Supported FPGA Versions for NCS 4206 and NCS 4216

Use the **show hw-module all fpd** command to display the IM FPGA version on the chassis.

Use the **show platform software agent iomd** [*slot/subslot*] **firmware cem-fpga** command to display the CEM FPGA version on the chassis.

The table below lists the FPGA version for the software releases.

**Note** During ISSU, TDM interface modules are reset for FPGA upgrade.

***Table 5: Supported TDM IM and CEM FPGAs for NCS 4206-RSP3 and NCS 4216***

| Category | Cisco IOS XE Release | 48 X T1/E1 CEM Interface Module FPGA (NCS 4200-48T1E1-CE) | 48 X T3/E3 CEM Interface Module FPGA (NCS 4200-48T3E3-CE) | OC-192 Interface Module + 8-port Low Rate Interface Module FPGA (NCS4 200-1T8S-10CS) | NCS 4200-1T8S-20CS | NCS4200-3GMS |
|---|---|---|---|---|---|---|
| IM FPGA | 17.15.3b | 1.22 | 1.22 | 1.15 | 0.95 | 2.1 |
| CEM FPGA | | 70160070 | CAS: 72020072<br>Non-CAS: 56030056 | 5G mode:<br>10090065<br>10G mode:<br>10070079 | 20G mode - CAS: 10330075<br>10G and 20G - Non-CAS: 12290074 | CAS: 10930095<br>Non-CAS: 11060093 |
| IM FPGA | 17.15.2 | 1.22 | 1.22 | 1.15 | 0.95 | 2.1 |
| CEM FPGA | | 70160070 | CAS: 72020072<br>Non-CAS: 56030056 | 5G mode:<br>10090065<br>10G mode:<br>10070079 | 20G mode - CAS: 10330075<br>10G and 20G - Non-CAS: 12290074 | CAS: 10930095<br>Non-CAS: 11060093 |
| IM FPGA | 17.15.1b | 1.22 | 1.22 | 1.15 | 0.95 | 2.0 |
| CEM FPGA | | 70160070 | CAS: 72020072<br>Non-CAS: 56030056 | 5G mode:<br>10090065<br>10G mode:<br>10070079 | 20G mode - CAS: 10330075<br>10G and 20G - Non-CAS: 12290074 | CAS: 10930095<br>Non-CAS: 11060093 |

| Category | Cisco IOS XE Release | 48 X T1/E1 CEM Interface Module FPGA (NCS 4200-48T1E1-CE) | 48 X T3/E3 CEM Interface Module FPGA (NCS 4200-48T3E3-CE) | OC-192 Interface Module + 8-port Low Rate Interface Module FPGA (NCS4 200-1T8S-10CS) | NCS 4200-1T8S-20CS | NCS4200-3GMS |
|---|---|---|---|---|---|---|
| IM FPGA | 17.15.1 | 1.22 | 1.22 | 1.15 | 0.95 | 2.0 |
| CEM FPGA | | 70160070 | CAS: 72020072<br>Non-CAS: 56030056 | 5G mode:<br>10090065<br>10G mode:<br>10070079 | 20G mode - CAS: 10330075<br>10G and 20G - Non-CAS: 12290074 | CAS: 10930095<br>Non-CAS: 11060093 |
| IM FPGA | 17.13.1 | 1.22 | 1.22 | 1.15 | 0.95 | 2.0 |
| CEM FPGA | | 70140070 | CAS: 72010072<br>Non-CAS: 56020056 | 5G mode:<br>10090065<br>10G mode:<br>10070079 | 20G mode - CAS: 10240075<br>10G and 20G - Non-CAS: 11160074 | CAS: 10810095<br>Non-CAS: 10950093 |
| IM FPGA | 17.12.1 | 1.22 | 1.22 | 1.15 | 0.95 | 2.0 |
| CEM FPGA | | 7.0 | 7.2 | 5G mode:<br>6.5<br>10G mode:<br>7.9 | 10G mode:<br>7.4<br>20G mode:<br>7.5 | 9.5 |
| IM FPGA | 17.11.1a | 1.22 | 1.22 | 1.15 | 0.95 | 2.0 |
| CEM FPGA | | 7.0 | 5.6 | 5G mode:<br>6.5<br>10G mode:<br>7.9 | 10G mode:<br>7.4<br>20G mode:<br>7.5 | 9.3 |
| IM FPGA | 17.10.1 | 1.22 | 1.22 | 1.15 | 0.95 | 2.0 |
| CEM FPGA | | 6.0 | 5.2 | 5G mode:<br>6.5<br>10G mode:<br>7.9 | 10G mode:<br>7.3<br>20G mode:<br>7.3 | 9.3 |

| Category | Cisco IOS XE Release | 48 X T1/E1 CEM Interface Module FPGA (NCS 4200-48T1E1-CE) | 48 X T3/E3 CEM Interface Module FPGA (NCS 4200-48T3E3-CE) | OC-192 Interface Module + 8-port Low Rate Interface Module FPGA (NCS4 200-1T8S-10CS) | NCS 4200-1T8S-20CS | NCS4200-3GMS |
|---|---|---|---|---|---|---|
| IM FPGA | 17.9.2 | 1.22 | 1.22 | 1.15 | 0.95 | 2.0 |
| CEM FPGA | | 6.0 | 5.2 | 5G mode:<br>6.5<br>10G mode:<br>7.9 | 10G mode:<br>7.2<br>20G mode:<br>7.2 | 9.1 |
| IM FPGA | 17.9.1 | 1.22 | 1.22 | 1.15 | 0.93 | 2.0 |
| CEM FPGA | | 6.0 | 5.2 | 5G mode:<br>6.5<br>10G mode:<br>7.9 | 10G mode:<br>7.2<br>20G mode:<br>7.2 | 9.1 |
| IM FPGA | 17.8.1 | 1.22 | 1.22 | 1.15 | 0.93 | 2.0 |
| CEM FPGA | | 6 | 5.2 | 5G mode:<br>6.5<br>10G mode:<br>7.9 | 10G mode:<br>7.0<br>20G mode:<br>6.0 | 9.0 |
| IM FPGA | 17.7.1 | 1.22 | 1.22 | 1.15 | 0.93 | 2.0 |
| CEM FPGA | | 0x52110052 | 0x52520052 | 5G mode:<br>0x10090065<br>10G mode:<br>0x10070079 | 10G mode:<br>0x10290051<br>20G mode:<br>0x10290051 | 0x10030076 |
| IM FPGA | 17.6.2 | 1.22 | 1.22 | 1.15 | 0.93 | 2.0 |
| CEM FPGA | | 0x52110052 | 0x52520052 | 5G mode:<br>0x10090065<br>10G mode:<br>0x10070079 | 10G mode:<br>0x10290051<br>20G mode:<br>0x10290051 | 0x10030076 |

| Category | Cisco IOS XE Release | 48 X T1/E1 CEM Interface Module FPGA (NCS 4200-48T1E1-CE) | 48 X T3/E3 CEM Interface Module FPGA (NCS 4200-48T3E3-CE) | OC-192 Interface Module + 8-port Low Rate Interface Module FPGA (NCS4 200-1T8S-10CS) | NCS 4200-1T8S-20CS | NCS4200-3GMS |
|---|---|---|---|---|---|---|
| IM FPGA | 17.6.1 | 1.22 | 1.22 | 1.15 | 0.93 | 2.0 |
| CEM FPGA | | 0x52110052 | 0x52520052 | 5G mode: 0x10090065 10G mode: 0x10070079 | 10G mode: 0x10290051 20G mode: 0x10290051 | 0x10030076 |
| IM FPGA | 17.5.1 | 1.22 | 1.22 | 1.15 | 0.93 | 2.0 |
| CEM FPGA | | 0x52050052 | 0x52420052 | 5G mode: 0x10210063 10G mode: 0x10530078 | 10G mode: 0x10090051 20G mode: 0x10090051 | 0x10020076 |

*Table 6: Supported Ethernet IM FPGA/FPD versions for NCS 4206-RSP3 and NCS 4216*

| Cisco IOS XE Release | NCS4200-1T16G -PS | NCS4200-1T8LR -PS | NCS4200-8T -PS | NCS4200-2Q -P | NCS4200-1H -PK | NCS4200-2H -PQ | NCS4200 -1T16LR |
|---|---|---|---|---|---|---|---|
| 17.15.3b | 1.129 | 69.32 | 0.21 | 0.21 | 0.20 | 0.20 | 69.24 |
| 17.15.2 | 1.129 | 69.32 | 0.21 | 0.21 | 0.20 | 0.20 | 69.24 |
| 17.15.1 | 1.129 | 69.32 | 0.21 | 0.21 | 0.20 | 0.20 | 69.24 |
| 17.15.1b | 1.129 | 69.32 | 0.21 | 0.21 | 0.20 | 0.20 | 69.24 |
| 17.13.1 | 1.129 | 69.32 | 0.21 | 0.21 | 0.20 | 0.20 | 69.24 |
| 17.12.1 | 1.129 | 69.32 | 0.21 | 0.21 | 0.20 | 0.20 | 69.24 |
| 17.11.1a | 1.129 | 69.32 | 0.21 | 0.21 | 0.20 | 0.20 | 69.24 |
| 17.10.1 | 1.129 | 69.32 | 0.21 | 0.21 | 0.20 | 0.20 | 69.24 |
| 17.10.1 | 1.129 | 69.32 | 0.21 | 0.21 | 0.20 | 0.20 | 69.24 |
| 17.9.2 | 1.129 | 69.32 | 0.21 | 0.21 | 0.22 | 0.20 | 69.24 |
| 17.9.1 | 1.129 | 69.32 | 0.21 | 0.21 | 0.22 | 0.20 | 69.24 |
| 17.8.1 | 1.129 | 69.32 | 0.21 | 0.21 | 0.22 | 0.20 | 69.24 |
| 17.7.1 | 1.129 | 1.129 | 0.21 | 0.21 | 0.22 | 0.20 | 69.24 |

| Cisco IOS XE Release | NCS4200-1T16G-PS | NCS4200-1T8LR-PS | NCS4200-8T-PS | NCS4200-2Q-P | NCS4200-1H-PK | NCS4200-2H-PQ | NCS4200-1T16LR |
|---|---|---|---|---|---|---|---|
| 17.6.1 | 1.129 | 1.129 | 0.21 | 0.21 | 0.22 | 0.20 | 69.24 |
| 17.5.1 | 1.22 | 1.22 | 1.15 | 0.93 | 2.0 | 0.23 | 0.20 |
| 17.4.1 | 1.129 | 69.24 | 0.21 | 0.22 | 0.20 | 3.4 | 1.129 |

*Table 7: FPGA, HoFPGA, and ROMMON Versions for Cisco IOS XE 17.15.1, 17.15.2, and 17.15.3b Releases*

| Platform | Interface Module | FPGA Current Version | FPGA Minimum Required Version | RSP HoFPGA Active | RSP HoFPGA Standby | ROMMON |
|---|---|---|---|---|---|---|
| NCS420X-RSP-128 | NCS4200-1T8LR-PS | 69.32 | 69.32 | 69.32 | 69.32 | 15.6(57r)S |
| NCS4206-RSP | NCS4200-1H-PK | 0.20 | 0.20 | 69.32 | 69.32 | 15.6(57r)S |
| | NCS4200-8T-PS | 0.22 | 0.21 | | | |
| | NCS4200-1T8LR-PS | 69.32 | 69.32 | | | |
| NCS4216-RSP | NCS4200-1H-PK | 0.20 | 0.20 | 20040034 | 20040034 | 15.6(57r)S |

# Additional References

### Deferrals

Cisco IOS software images are subject to deferral. We recommend that you view the deferral notices at the following location to determine whether your software release is affected: http://www.cisco.com/en/US/products/products_security_advisories_listing.html.

### Field Notices and Bulletins

- Field Notices—We recommend that you view the field notices for this release to determine whether your software or hardware platforms are affected. You can find field notices at http://www.cisco.com/en/US/support/tsd_products_field_notice_summary.html.
- Bulletins—You can find bulletins at http://www.cisco.com/en/US/products/sw/iosswrel/ps5012/prod_literature.html.

### MIB Support

The below table summarizes the supported MIBs on the Cisco NCS 4206 and Cisco NCS 4216.

| Supported MIBs | | |
|---|---|---|
| BGP4-MIB (RFC 1657) | CISCO-IMAGE-LICENSE-MGMT-MIB | MPLS-LDP-STD-MIB (RFC 3815) |
| CISCO-BGP-POLICY-ACCOUNTING-MIB | CISCO-IMAGE-MIB | MPLS-LSR-STD-MIB (RFC 3813) |

| Supported MIBs | | |
|---|---|---|
| CISCO-BGP4-MIB | CISCO-IPMROUTE-MIB | MPLS-TP-MIB |
| CISCO-BULK-FILE-MIB | CISCO-LICENSE-MGMT-MIB | MSDP-MIB |
| CISCO-CBP-TARGET-MIB | CISCO-MVPN-MIB | NOTIFICATION-LOG-MIB (RFC 3014) |
| CISCO-CDP-MIB | CISCO-NETSYNC-MIB | OSPF-MIB (RFC 1850) |
| CISCO-CEF-MIB | CISCO-OSPF-MIB (draft-ietf-ospf-mib-update-05) | OSPF-TRAP-MIB (RFC 1850) |
| CISCO-CLASS-BASED-QOS-MIB | CISCO-OSPF-TRAP-MIB (draft-ietf-ospf-mib-update-05) | PIM-MIB (RFC 2934) |
| CISCO-CONFIG-COPY-MIB | CISCO-PIM-MIB | RFC1213-MIB |
| CISCO-CONFIG-MAN-MIB | CISCO-PROCESS-MIB | RFC2982-MIB |
| CISCO-DATA-COLLECTION-MIB | CISCO-PRODUCTS-MIB | RMON-MIB (RFC 1757) |
| CISCO-EMBEDDED-EVENT-MGR-MIB | CISCO-PTP-MIB | RSVP-MIB |
| CISCO-ENHANCED-MEMPOOL-MIB | CISCO-RF-MIB | SNMP-COMMUNITY-MIB (RFC 2576) |
| CISCO-ENTITY-ALARM-MIB | CISCO-RTTMON-MIB | SNMP-FRAMEWORK-MIB (RFC 2571) |
| CISCO-ENTITY-EXT-MIB | CISCO-SONET-MIB | SNMP-MPD-MIB (RFC 2572) |
| CISCO-ENTITY-FRU-CONTROL- MIB | CISCO-SYSLOG-MIB | SNMP-NOTIFICATION-MIB (RFC 2573) |
| CISCO-ENTITY-SENSOR-MIB | DS1-MIB (RFC 2495) | SNMP-PROXY-MIB (RFC 2573) |
| CISCO-ENTITY-VENDORTYPE-OID-MIB | ENTITY-MIB (RFC 4133) | SNMP-TARGET-MIB (RFC 2573) |
| CISCO-FLASH-MIB | ENTITY-SENSOR-MIB (RFC 3433) | SNMP-USM-MIB (RFC 2574) |
| CISCO-FTP-CLIENT-MIB | ENTITY-STATE-MIB | SNMPv2-MIB (RFC 1907) |
| CISCO-IETF-ISIS-MIB | EVENT-MIB (RFC 2981) | SNMPv2-SMI |
| CISCO-IETF-PW-ATM-MIB | ETHERLIKE-MIB (RFC 3635) | SNMP-VIEW-BASED-ACM-MIB (RFC 2575) |
| CISCO-IETF-PW-ENET-MIB | IF-MIB (RFC 2863) | SONET-MIB |
| CISCO-IETF-PW-MIB | IGMP-STD-MIB (RFC 2933) | TCP-MIB (RFC 4022) |
| CISCO-IETF-PW-MPLS-MIB | IP-FORWARD-MIB | TUNNEL-MIB (RFC 4087) |
| CISCO-IETF-PW-TDM-MIB | IP-MIB (RFC 4293) | UDP-MIB (RFC 4113) |
| CISCO-IF-EXTENSION-MIB | IPMROUTE-STD-MIB (RFC 2932) | CISCO-FRAME-RELAY-MIB |
| CISCO-IGMP-FILTER-MIB | MPLS-LDP-GENERIC-STD-MIB (RFC 3815) | |

### MIB Documentation

To locate and download MIBs for selected platforms, Cisco IOS and Cisco IOS XE releases, and feature sets, use Cisco MIB Locator found at the following location: 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 will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at the following location: http://tools.cisco.com/RPF/register/register.do

### Open Source License Notices

For a listing of the license notices for open source software used in Cisco IOS XE 3S Releases, see the documents accessible from the License Information page at the following location:

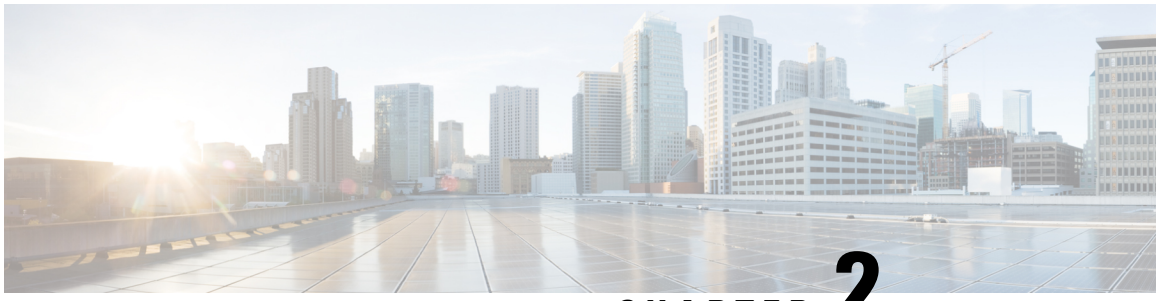
http://www.cisco.com/en/US/products/ps11174/products_licensing_information_listing.html

.

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

### Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.



CHAPTER 2

# What's New for Cisco IOS XE 17.15.x



## What's New in Hardware for Cisco IOS XE 17.15.3b

There are no new hardware features introduced for this release.

## What's New in Software for Cisco IOS XE 17.15.3b

| Feature | Description |
|---|---|
| **IP Addressing** | |
| Optimizing security and CPU utilization using software ACL in VRF traffic management | The Software ACL (SW ACL) is a platform-specific feature designed to control Layer 3 VRF traffic, such as ICMP, SSH, and Telnet, by managing traffic punted to the CPU. This feature enhances security and optimizes CPU utilization by allowing only explicitly permitted traffic to reach the CPU. The software ACLs enhances reliable and secure VRF-based services in enterprise networks and service provider networks.<br>Command introduced:<br>**platform sw_acl enable interface {icmp \| ssh \| telnet}** |
| **MPLS** | |
| Support for Co-routed Inter-area Flex-LSP Tunnels in Point-to-Point OSPF network | Co-routed Flex LSP tunnels now support an inter-area and multiple areas in a Point-to-Point OSPF network. For example, in an inter-area OSPF network, both the head-end or tail-end for a bidirectional LSPs that are in different areas learn the network topology and perform the automatic path redundancy when there is a network link failure. |

# What's New in Hardware for Cisco IOS XE 17.15.2

There are no new hardware features introduced for this release.

# What's New in Software for Cisco IOS XE 17.15.2

| Feature | Description |
|---|---|
| **Chassis** | |
| Alarms to Monitor Unsupported Slot Compatibility in IM | When an interface module (IM) is inserted into an unsupported slot, an **IM_NOT_SUPPORTED** syslog message is generated. Additionally, new unsupported alarms such as **IM_NOT_SUPPORTED**, **INVALID_COMBINATION**, **INVALID_MODE**, and**SPA_MISMATCH** are asserted when an IM is inserted into a router slot that is not supported.<br>You can view the alarm status and unsupported slot information using the<br>**show facility-alarm status** CLI command.<br>This enhancement ensures administrators are promptly alerted to any compatibility issues, enabling them to take corrective action and maintain network stability. |
| Suppressing Extraneous Alarms for Admin-Down Interfaces | Extraneous alarms along with SNMP traps, can be generated on TDM or Ethernet interfaces even when these interfaces are in an administratively down state. These unnecessary alarms can lead to redundant monitoring and troubleshooting efforts. These alarms are suppressed by default. To mitigate this issue, you can disable this feature or unsuppress these alarms using the following command the router:<br>**platform enable-transceiver-sensor-alarm-on-admin-down**<br>This ensures that only relevant alarms are captured and displayed. This helps streamline network management and improves operational efficiency. |
| **Performance Routing** | |
| Hardware Resource and Scale Monitoring | A new command has been introduced for hardware resource and scale monitoring.<br>You can now view the current utilizations and the maximum capacities available in the hardware for various resources.<br>Command: show platform hardware pp active resource-usage monitor |

# What's New in Hardware for IOS XE 17.15.1b

There are no new hardware features introduced for this release.

# What's New in Software for IOS XE 17.15.1b

| Feature | Description |
|---|---|
| **Alarms** | |
| New APS Alarms and Conditions | New APS alarms and conditions have been introduced to enhance network monitoring and management. These alarms are raised or cleared during APS manual, forced, and lockout switch actions, providing real-time alerts on network changes. This advanced alerting mechanism ensures that network operators are immediately informed of any alterations, enabling them to swiftly respond to and manage network conditions, thereby maintaining optimal performance and reliability. |
| SONET Alarms for APS | In APS scenarios, the existing SONET alarms follow the GR-253 standard for alarm soaking. This standardization helps filter out transient conditions by defining specific assertion and clearing times for alarms. |
| SD-BER and SF -BER Alarms for T1/E1 and T3/E3 services | Signal Failure-Bit Error Rate (SF-BER) and Signal Degrade-BER (SD-BER) alarms are declared when there is a signal failure or signal degradation that happens in the traffic.<br>These alarms may be raised when the error rate of a given entity exceeds the user configured BER threshold value.<br>This helps administrator to take corrective actions. |
| **CEM** | |
| DDS DS0 Remote Latching Loopback | DS0 loopback is used for testing and troubleshooting the T1 or E1, T3 or E3, and OCx channel over PSN. You can configure DS0 loopback on these controllers for remote devices. |
| Protected TAP on FRR Protected Core | You can now monitor CEM traffic through protected TAP and split TAP sessions on the protected Fast Reroute (FRR) core interface. During events such as link failure or connectivity issues, the automatic switching happens from active to standby path.<br>Thus, you can monitor and debug the issue without affecting the traffic on these FRR protected core interfaces. |
| Protection Switching Count for Protected SONET Interface | In SONET networks with redundancy, Automatic Protection Switching (APS) seamlessly transitions traffic between working and standby protection links, typically due to circuit failures or other disruptions.<br>Each switching event is tracked using the Protection Switching Count (PSC) parameter. This parameter allows network operators to monitor and analyze the frequency of these switches in real-time. By examining the PSC count, users can diagnose the network to identify the root causes of frequent switching events and implement necessary corrective actions.<br>This advanced capability significantly enhances network reliability and performance, offering users a robust and efficient solution for maintaining optimal service quality. |

| Feature | Description |
|---|---|
| Clear Counters command | • Unlike the previous release, where the **clear counters** command reset the old dataset, from this release onwards, the command resets all the PMON datasets, including the current dataset.<br>• You can clear the PMON data for a specific interface module on the device using the **clear controller hw-module** command |
| GR-820-CORE specific Performance Monitoring | The **show controller tabular** enables you to view the performance monitoring details in tabular form as per GR-820-Core standards. |
| **Chassis** | |
| Alarms to Monitor Standby RSP Upgrade During IOS Version Mismatch | During an upgrade, for a high availability setup, if the IOS version of the active Route Switch Processor (RSP) does not match the IOS version of the standby RSP, a Syslog message, **IPC: IOS versions do not match** is printed on the console. The upgrade process is aborted and there are no alarms to notify the IOS version mismatch or the progress of the standby upgrade.<br>From Cisco IOS XE 17.15.1, show commands have been enhanced to display Syslog messages for any active and standby RSP version mismatch, and the IOS XE image from the active RSP is copied to the standby RSP.<br>You can execute the following show commands on the active RSP to monitor the progress of the upgrade:<br>• **show facility-alarm status**<br>• **show facility-condition status**<br>The NCS 4206/16-RSP3 module supports this feature. See the High Availability Configuration Guide for the upgrade process. |
| Alarm for Incompatible SFP | When an incompatible SFP is used in Ethernet interface modules on the RSP3 node, a *Transceiver NOT_COMPATIBLE* alarm is raised. |
| **High Availability** | |
| Monitoring alarms for standby RSP management interface | In addition to Active RSP, alarms are now generated for the management interface of the Stand-by RSP. You can monitor these alarms in Cisco's Evolved Programmable Network Manager (EPNM) and take the appropriate action to fix the problem. |
| In-Service Software Upgrade (ISSU) Enhancements | During the ISSU upgrade, the system verifies if the new software image is already available in the active and standby boot flash before the binary image expansion. This helps to reduce the ISSU upgrade time on multiple devices.<br>Syslog messages are generated during this ISSU upgrade for each stage. If alarms are generated, they are captured at each stage and sent to SNMP. You can monitor the ISSU process using the show facility-alarm status CLI command.<br>These enhancements are supported only on RSP3 modules. |
| **QoS** | |

| Feature | Description |
|---|---|
| Displaying ASIC QoS Policer Values for Egress Traffic | In addition to Ingress traffic, you can now view the programmed hardware (ASIC) values of the QoS features configured for Egress traffic.<br>Use the following command to enable ASIC values:<br>**platform qos-egress-hw-param enable**<br>The programmed hardware (ASIC) value may differ from the configured software value due to hardware limitations. Now, you can compare the actual QoS policer value programmed in the hardware with the value you configured in the software for egress traffic. |
| **Timing and Synchronization** | |
| Improved Network Synchronization Redundancy with an External BITS Clock | The T4 PLL in the route processor can now send a SyncE signal through the BITS port to an external clocking device. If equipped with a high-quality oscillator, the external clocking device can clean up the timing signal to reduce the jitter. When returned to the T0 PLL through the same BITS port, the cleaned-up signal can be sent to other nodes to propagate network synchronization.<br>This functionality is useful when an external BITS clock cannot receive timing inputs from a Primary Reference Source (PRS). The system can fall back on using the SyncE signal received from a peer router to provide redundancy to the network synchronization operation.<br>Command introduced:<br>**network-clock timing-source** bits<br>Compliance: BITS implementation and SyncE recommendations from GR-436 and G.8264 standards<br>Supported Interface Module: RSP3 |

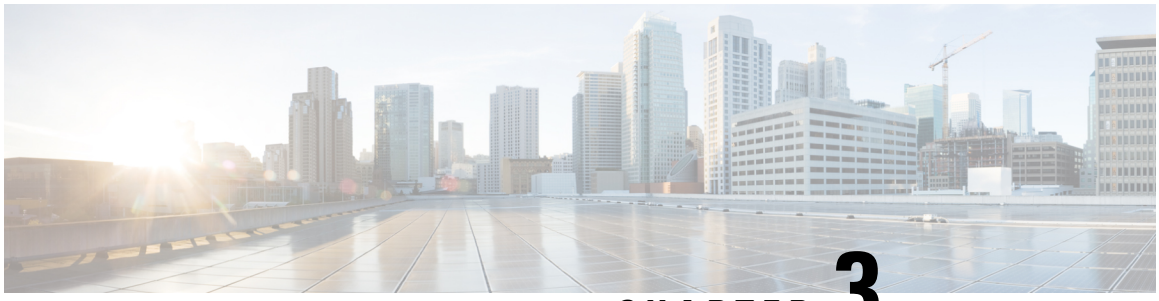
# What's New in Hardware for Cisco IOS XE 17.15.1

There are no new hardware features introduced for this release.

# What's New in Software for Cisco IOS XE 17.15.1

| Feature | Description |
|---|---|
| **Alarms** | |
| SONET Alarms for APS | • With Automatic Protection Switching (APS), SONET alarms soaking as per the recommendation from GR-253.<br>• Alarm is raised or cleared during APS manual, force, and lock out switch actions.<br>• When traffic is switched to an alternate link in the APS group, the severity of the alarms is affected based on service impact. |

| Feature | Description |
|---|---|
| SD-BER and SF -BER Alarms for T1/E1 and T3/E3 services | Signal Failure-Bit Error Rate (SF-BER) and Signal Degrade-BER (SD-BER) alarms are declared when there is a signal failure or signal degradation that happens in the traffic.<br>These alarms may be raised when the error rate of a given entity exceeds the user-configured BER threshold value.<br>This helps the administrator to take corrective actions. |
| **CEM** | |
| DDS DS0 Remote Latching Loopback | DS0 loopback is used for testing and troubleshooting the T1 or E1, T3 or E3, and OCx channel over PSN. You can configure DS0 loopback on these controllers for remote devices. |
| Protection Switching Count for Protected SONET Interface | In SONET with redundancy, an Automatic protection switching (APS) occurs between working and standby protection links due to reasons like a circuit failure. Whenever the switching happens, the switching count is tracked using a Protection Switching Count (PSC) parameter.<br>Depending on the PSC count, you can debug the network to identify the reason for extensive switching and work on the corrective actions. |
| **TCAM and NFT Commands** | |
| TCAM and NFT Commands | New commands have been introduced for the Ternary Content-Addressable Memory (TCAM) and NFT.<br>**TCAM**<br>You can now view the Ternary Content-Addressable Memory (TCAM) utilization for each control plane TCAM entry.<br>Command: show platform hardware pp active tcam utilization control-plane-sessions<br>**NFT**<br>• You can now enable the collection of the packets punted to the CPU from the NFT hash table.<br>Command: platform nft-summarization enable<br>• Once the above command is enabled, you can use a timer to clean up the NFT hash table.<br>Command: platform nft-summarization timer-value<br>• You can view a summary of the packets punted to the CPU from the NFT hash table.<br>Command: show platform hardware pp active infrastructure pi nft summary |



CHAPTER 3

# Caveats

This chapter describes open and resolved 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 "Resolved Caveats" sections list caveats resolved in a specific release, but open in previous releases.

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.



# Resolved Caveats – Cisco IOS XE 17.15.3b

| Identifier | Headline |
|---|---|
| CSCwm82342 | Post reload HSRP is stuck in Init state and shows interface down |
| CSCwm04031 | 17.9.2a/Both active and standby RSP's OAM/CFM configs automatically changed after a reload. |
| CSCwn12822 | Discrepancy with counters on SONET controller during BERT test. |
| CSCwn94246 | XCVR incompatible alarm missing without Sonet controller configurations. |

| Identifier | Headline |
|---|---|
| CSCwn41240 | Observed unframed T1 as none and not shown in running-config under T3 controller. |
| CSCwn38105 | SSH process goes down with a segmentation fault. |
| CSCwo10841 | XCVR incompatible alarm not asserted in Bay0 sonet controller cards |
| CSCwn88535 | ISSU : Missing alarms for Software distribution |
| CSCwm99575 | Trap interval support for Ethernet OAM |
| CSCwn57972 | XCVR incompatible alarms are not generated with Telcordia profile |
| CSCwn53341 | Fan failure alarm does not display correct module name or description with hard OIR |
| CSCwn42612 | With the T3 CTRL shut operation, if the mode T3 is not configured, then the line side connected device receives LOS |
| CSCwn22679 | When standby RSP management interface goes down, there is no alarm generated on active node |

# Open Caveats – Cisco IOS XE 17.15.3b

There are no open caveats in this release.

# Resolved Caveats – Cisco IOS XE 17.15.2

| Identifier | Headline |
|---|---|
| CSCwj72178 | (RSP3) - OSPF not coming on G8032 VLAN after a reload. |
| CSCwk78043 | Double description under CPG STS1E mode. |
| CSCwk87121 | Ports on router remain down after ISSU operation with RSP3. |
| CSCwm91197 | Silent reload of 3GMS IM due to PCI transaction failure. |
| CSCwm86214 | LDP session flap causes memory leak for EMPLS3LD which leads to RSP crash. |

# Open Caveats – Cisco IOS XE 17.15.2

| Identifier | Headline |
|---|---|
| CSCwk02087 | 17.6.3-BFD stuck in INIT state for interface Te0/0/0 & Te0/4/3 |
| CSCwm04031 | 17.9.2a-Both active and standby RSP's OAM or CFM configurations automatically changed after a reload. |

# Resolved Caveats - Cisco IOS XE 17.15.1b

The list of resolved caveats for the RSP3 module.

| Identifier | Headline |
|---|---|
| CSCwi33111 | Eomer T1: Sev changes back from major to minor after IM OIR. |
| CSCwj06370 | Serial cease traffic when configuring module other port |
| CSCwj05647 | 3GMS Serial interface protocol down with specific Modem |
| CSCwj12451 | Update 2^20-O151 QRSS bert help string with QRSS Keyword in NCS42xx platform |
| CSCwj44502 | DCR clocking fails to get acquired on the with sts1-E mode |
| CSCwj99522 | Need to support dtr not-used CLI in RS232 transparent mode |
| CSCwi92203 | Channelized DS3: RAI is propagating to all DS1's when DS3 RAI is asserted |
| CSCwk58917 | L-bit propogation not enabled for LOF alarm after framing change with framed SAToP |

# Open Caveats - Cisco IOS XE 17.15.1b

The list of open caveats for the RSP3 module.

| Identifier | Headline |
|---|---|
| CSCwk02087 | 17.6.3-BFD stuck in INIT state for interface Te0/0/0 & Te0/4/3 |
| CSCwj60760 | Confd process not in Started State in 5 mins after netconf-yang config is done |
| CSCwk27810 | After reconfiguring second synce source the QL-failed for that source interface and ranking also 254 |

# Resolved Caveats - Cisco IOS XE 17.15.1

The list of resolved caveats for the RSP2 module.

| Identifier | Headline |
|---|---|
| CSCwi76112 | Message to be displayed for M13 framing when configured with clear-channel |
| CSCwi60730 | Speed LED status is not correct when sonet/sdh mode is configured |

# Open Caveats - Cisco IOS XE 17.15.1

The list of open caveats for the RSP2 module.

| Identifier | Headline |
|---|---|
| CSCwh75614 | Increased CPU after upgrading router to 17.6.3 from 16.9.4 when 1000 SLM/DMM sessions are configured |
| CSCwj38216 | BDI ARP is not learning but peer side BDI MAC is learning through VC |

# Cisco Bug Search Tool

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