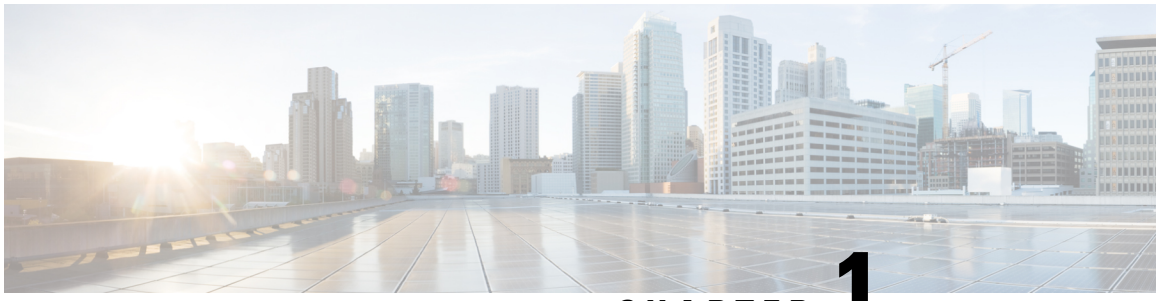
Release Notes for Cisco NCS 4206 and Cisco NCS 4216 Series, Cisco IOS XE Bengaluru 17.4.x

First Published: 2021-11-30

Last Modified: 2020-11-30

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS



CHAPTER 1

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 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.

Cisco NCS 4216 F2B

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 F2B can also be positioned as a Carrier Ethernet aggregation platform.

The Cisco NCS 4216 F2B 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.

NCS 4216 14RU

The Cisco NCS 4216 14RU 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 GigabitEthernet 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 14RU chassis, see the Cisco NCS 4216 14RU 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.

Swapping of Interface Modules

The following Ethernet interface modules support swapping on the Cisco NCS4216-RSP module:

Use the **hw-module subslot default** command before performing a swap of the modules to default the interfaces on the interface module.

- SFP Combo IM—8-port Gigabit Ethernet (8X1GE) + 1-port 10 Gigabit Ethernet (1X10GE)
- 2-port 40 Gigabit Ethernet Interface Module (2X40GE)
- 8/16-port 1 Gigabit Ethernet (SFP/SFP) + 1-port 10 Gigabit Ethernet (SFP+) / 2-port 1 Gigabit Ethernet (CSFP) Interface Module
- 8-port 10 Gigabit Ethernet Interface Module (8X10GE)
- 1-port 100 Gigabit Ethernet Interface Module (1X100GE)
- 2-port 100 Gigabit Ethernet (QSFP) Interface Module (2X100GE)

Use of **hw-module subslot default** command is not supported on the following interface modules.

- OC-192 Interface Module with 8-port Low Rate CEM Interface Module (10G HO / 10G LO)
- 48 T1/E1 TDM Interface Module (48XT1/E1)
- 48 T3/E3 TDM Interface Module (48XT3/E3)
- 1-port OC48 STM-16 or 4-port OC-12/OC-3 / STM-1/STM-4 + 12-Port T1/E1 + 4-Port T3/E3 CEM Interface Module
- NCS 4200 1-Port OC-192 or 8-Port Low Rate CEM 20G Bandwidth Interface Module

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.

Table 3: NCS4216-RSP Supported Interface Modules and Part Numbers

RSP Module	Interface Modules	Part Number	Slot
NCS4216-RSP	SFP Combo IM—8-port Gigabit Ethernet (8X1GE) + 1-port 10 Gigabit Ethernet (1X10GE)	NCS4200-1T8LR-PS	2,5,6,9,10,13,14,15
	1-port 100 Gigabit Ethernet Interface Module (1X100GE)	NCS4200-1H-PK	7,8
	2-port 100 Gigabit Ethernet (QSFP) Interface Module (2X100GE)[5]	NCS4200-2H-PQ	7,8
	2-port 40 Gigabit Ethernet QSFP Interface Module (2X40GE)	NCS4200-2Q-P	3,4,7,8,11,12
	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	All slots
	1-port OC48[6]/ 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	All slots
	8-port 10 Gigabit Ethernet Interface Module (8X10GE)	NCS4200-8T-PS	3,4,7,8,11,12

	1-port OC-192 Interface Module with 8-port Low Rate CEM Interface Module (5G/ 10G HO / 10G LO)	NCS4200-1T8S-10CS	3,4,7,8,11,12 (10G mode)
			0,1,2,5,6,9,10,13,14,15 (5G mode)
			Note To enable this IM on slot 0 or slot 1, do the following and reload the router:
			`Router# configure t`
			`Router(config)# license feature service-offload enable`

	NCS 4200 1-Port OC-192 or 8-Port Low Rate CEM 20G Bandwidth Interface Module	NCS4200-1T8S-20CS	3,4,7,8,11,12 (20G mode)
			0,1,2,5,6,9,10,13,14,15 (10G mode)
			Note To enable this IM on slot 0 or slot 1, do the following and reload the router:
			`Router# configure t`
			`Router(config)# license feature service-offload enable`

	48-port T1/E1 Interface module	NCS4200-48T1E1-CE	2,3,4,5,6,7,8,9,10,13,14,15

RSP Module	Interface Modules	Part Number	Slot
	48-port T3/E3 Interface module	NCS4200-48T3E3-CE	2,3,4,5,6,7,8,9,10,13,14,15

[5] IM supports only one port of 100G with RSP3 as QSFP28 on Port 0 in both slots 7 and 8.
[6] If OC48 is enabled, then the remaining 3 ports are disabled.

Cisco NCS 4216 F2B Supported Interface Modules

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

Swapping of Interface Modules

The following interface modules support swapping on the Cisco NCS4216-RSP module:

- SFP Combo IM—8-port Gigabit Ethernet (8X1GE) + 1-port 10 Gigabit Ethernet (1X10GE)
- 2-port 40 Gigabit Ethernet Interface Module (2X40GE)
- 8-port 10 Gigabit Ethernet Interface Module (8X10GE)
- 1-port 100 Gigabit Ethernet Interface Module (1X100GE)
- 2-port 100 Gigabit Ethernet Interface Module (2X100GE)
- 8/16-port 1 Gigabit Ethernet (SFP/SFP) + 1-port 10 Gigabit Ethernet (SFP+) / 2-port 1 Gigabit Ethernet (CSFP) Interface Module
- 1-port OC-192 Interface Module with 8-port Low Rate CEM Interface Module (10G HO / 10G LO)
- 48-port T1/E1 TDM Interface Module (48XT1/E1)
- 48-port T3/E3 TDM Interface Module (48XT3/E3)
- 1-port OC 482/ 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)
- 1-Port 10 Gigabit MR and 8-Port LR 20 Gigabit CEM and iMSG Interface Module (NCS 4200-1T8S-20CS)

Use the **hw-module subslot default** command before performing a swap of the modules to default the interfaces on the interface module.

See the *Cisco NCS 4216 Router Hardware Installation Guide* for information on Supported Interface Modules on the RSP.

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.

Table 4: Cisco NCS4216-RSP Supported Interface Modules and Part Numbers

RSP Module	Interface Modules	Part Number	Slot
NCS4216-RSP	SFP Combo IM—8-port Gigabit Ethernet (8X1GE) + 1-port 10 Gigabit Ethernet (1X10GE)	NCS4200-1T8LR-PS	2,5,6,9,10,13,14,15
	1-port 100 Gigabit Ethernet Interface Module (1X100GE)	NCS4200-1H-PK	7,8
	2-port 100 Gigabit Ethernet (QSFP) Interface Module (2X100GE)[7]	NCS4200-2H-PQ	7,8
	2-port 40 Gigabit Ethernet QSFP Interface Module (2X40GE)	NCS4200-2Q-P	3,4,7,8,11,12
	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	All slots
	8-port 10 Gigabit Ethernet Interface Module (8X10GE)	NCS4200-8T-PS	3,4,7,8,11,12
	1-port OC-192 Interface Module with 8-port Low Rate CEM Interface Module (5G/ 10G HO / 10G LO)	NCS4200-1T8S-10CS	3,4,7,8,11,12 (10G mode) 0,1,2,5,6,9,10,13,14,15 (5G mode)
	NCS 4200 1-Port OC-192 or 8-Port Low Rate CEM 20G Bandwidth Interface Module	NCS4200-1T8S-20CS	3,4,7,8,11,12 (20G mode) 0,1,2,5,6,9,10,13,14,15 (10G mode)
	48XT1/E1 Interface module	NCS4200-48T1E1-CE	2,3,4,5,6,7,8,9,10,13,14,15
	48XT3/E3 Interface module	NCS4200-48T3E3-CE	2,3,4,5,6,7,8,9,10,13,14,15
	1-port OC48[8]/ 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	All slots

[7] IM supports only one port of 100G with RSP3 as QSFP28 on Port 0 in both slots 7 and 8.
[8] If OC48 is enabled, then the remaining 3 ports are disabled.

Restrictions and Limitations for Cisco NCS 4206 and Cisco NCS 4216

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.

- In the Cisco IOS XE 16.12.1 release, IPSec is not supported on the Cisco RSP3 module.
- VT PMON is not supported.
- APS is supported across interface modules. But it is not supported on the same interface module.
- VT loopback is not supported if T1 is configured for the VT mode.
- DS1/DS3 SF/SD is not supported.
- All zeros BERT pattern on system side does not get in sync on DS3.
- DS3/OCx MDL does not interoperate with legacy Q.921 standards.
- APM is not supported with EPAR on CEP.
- FDL is not supported.
- STS24-c is not supported on 1-port OC-192 or 8-port low rate CEM interface module.
- Port restriction on 1-port OC-192 or 8-port low rate CEM interface module. If you have OC-48 configured on a port, you cannot use the neighboring port.
- Bellcore remote loopbacks are not supported for DS1/DS3. Only T1.403 remote loopbacks are supported.
- CEP MIB is not supported.
- HSPW is not supported on DS3/DS1/OCX card.
- The **ip cef accounting** command is not supported on the chassis.
- 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 chassis. 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 Cisco NCS 4206. A reload of the chassis 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 of T1, T3, and CT3 circuits to UPSR are not supported.
- DCC is supported only on PPP encapsulation. It is not supported on CLNS encapsulation.
- If oversubscription is enabled on 8-port 10 Gigabit Ethernet interface module, PTP is not supported.
- Effective with Cisco IOS XE Everest 16.6.1, the Port-channel (PoCH) scale is reduced to 24 from 48 for Cisco ASR 900 RSP3 module.

Note The PoCH scale for Cisco NCS 4216 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.
- 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.
- One Ternary Content-Addressable Memory (TCAM) entry is utilized for Segment Routing Performance Measurement. This is required for the hardware timestamping to function.
- 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 diskspace of 2 MB is required in the boot flash memory file system for a successful ROMMON auto upgrade process. For a diskspace lesser than 2 MB, ROMMON auto upgrade fails and the router reboots. This is applicable to Cisco NCS 4206 and Cisco NCS 4216 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.
- 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 exhibited by running the pyang tool with the **lint** flag are currently non-critical 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.

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 Cisco IOS XE 3S consolidated packages can be downloaded from Cisco.com; users who want to run the chassis using individual subpackages must first download the image from Cisco.com and extract the individual subpackages from the consolidated package.

ROMMON Version

For software upgrade later than the Cisco IOS XE 16.9.x release, it is mandatory that you upgrade the ROMMON version to 15.6(49r)S.

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 FPGA Versions for NCS 4206-RSP3 and NCS 4216

	Cisco IOS XE Release	48 X T1/E1 CEM Interface Module FPGA	48 X T3/E3 CEM Interface Module FPGA	OC-192 Interface Module + 8-port Low Rate Interface Module FPGA	NCS 4200-1T8S-20CS	NCS4200-3GMS	8x10G FPGA	2x40G FPGA	1x100G FPGA
IM FPGA	17.4.2	1.22	1.22	1.15	0.93	2.0	0.23	0.22	0.20
CEM FPGA		0x52050052	0x52420052	5G mode: 0x10180062 10G mode: 0x10530078	10G mode: 0x60210071 20G mode: 0x10090051	0x60210051 20G mode: 0x10530078	—	—	—
IM FPGA	17.4.1	1.22	1.22	1.15	0.93	2.0	0.23	0.22	0.20
CEM FPGA		0x52050052	0x52420052	5G mode: 0x10180062 10G mode: 0x10530078	10G mode: 0x10770047 20G mode: 0x10090051	0x10320074	—	—	—

Documentation Updates

Rearrangement in the Configuration Guides

- The following are the modifications in the CEM guides.
  - Introduction of the Alarm Configuring and Monitoring Guide:

    This guide provides the following information:
    - Alarms supported for SONET and SDH, and their maintenance
    - Alarm profiling feature
    - Auto In-Service States for cards, ports, and transceivers

    For more information, see the Alarm Configuring and Monitoring Guide, Cisco IOS XE 17 (Cisco NCS 4200 Series).
  - Rearrangement of Chapter and Topics in the Alarm Configuring and Monitoring Guide:
    - The Auto In-Service States Guide is now a chapter inside the Alarms Configuring and Monitoring Guide.

- Alarms at SONET Layers topic in the following CEM guides, is added to the Alarms Configuring and Monitoring Guide:
  - 1-Port OC-48/STM-16 or 4 port OC-12/OC-3 / STM-1/STM-4 + 12 port T1/E1 + 4 port T3/E3 CEM Interface Module Configuration Guide
- The Alarm History and Alarm Profiling chapters are removed from the below CEM Technology guides, and added into the Alarm Configuring and Monitoring Guide:
  - 1-Port OC-48/STM-16 or 4 port OC-12/OC-3 / STM-1/STM-4 + 12 port T1/E1 + 4 port T3/E3 CEM Interface Module Configuration Guide

- Configuring IEEE 802.3ad Link Bundling is now available in Ethernet Channel Configuration Guide, Cisco IOS XE 17 (Cisco NCS 4200 Series).

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)
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)

Supported MIBs		
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:

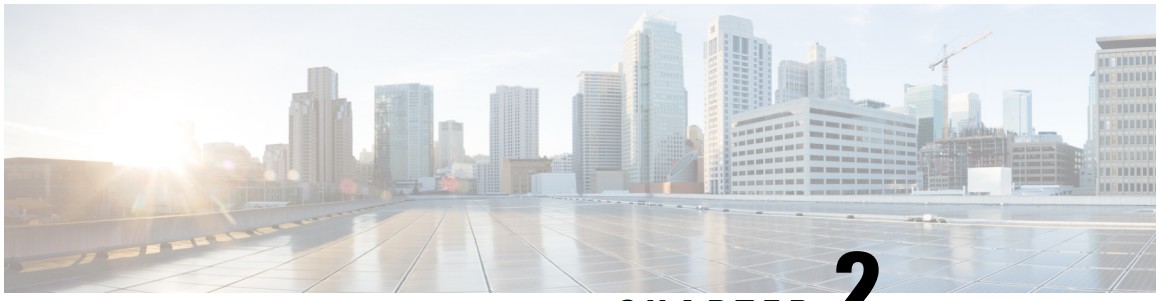
http://www.cisco.com/en/US/products/ps11174/products_licensing_information_listing.html

.

- 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 Bengaluru 17.4.x

This chapter describes the new hardware and software features supported on the Cisco NCS 4206 and Cisco NCS 4216 series routers in Cisco IOS XE Bengaluru 17.4.x.

What's New in Hardware for Cisco IOS XE Bengaluru 17.4.2a

There are no new features introduced for this release.

What's New in Software for Cisco IOS XE Bengaluru 17.4.2a

There are no new features introduced for this release.

What's New in Hardware for Cisco IOS XE Bengaluru 17.4.2

There are no new hardware features for this release.

What's New in Software for Cisco IOS XE Bengaluru 17.4.2

There are no new software features for this release.

What's New in Hardware for Cisco IOS XE Bengaluru 17.4.1

The following optics are supported for the Cisco IOS XE Bengaluru 17.4.1 release:

- OPTICS - QSFP-100G-ER4L-S=

- OPTICS - ONS-SI-100-LX10=
- OPTICS - ONS-SE-100-BX10D=
- OPTICS - ONS-SE-100-BX10U=
- OPTICS - ONS-SI-100-FX=

For more information, see the Cisco NCS 4206-16 Series Aggregation ServicesRouters Feature Optics Matrix.

What's New in Software for Cisco IOS XE Bengaluru 17.4.1

Feature	Description
1 port OC-48/STM-16 or 4 port OC-12/OC-3 / STM-1/STM-4 + 12 port T1/E1 + 4 port T3/E3 CEM Interface Module	
IPv6 VLAN Handoff and 4k iMSG scale	VLAN handoff supports IPv4 and IPv6 local connect and cross connect.
STS1E Framed SAToP Support on IMA3G	Support on clock recovery on STS-1e controller for framed SAToP on the following modes: • T3 • CT3 • VT-15
1-Port OC-192 or 8-Port Low Rate CEM Interface Module	
BERT Error Injection	BERT Error injection enables you to inject errors into the BERT stream on SONET and SDH controllers. You can introduce BERT errors in a range of 1 to 255. This feature is introduced on the following Interface Modules: • 1 port OC-48/STM-16 or 4 port OC-12/OC-3 / STM-1/STM-4 + 12 port T1/E1 + 4 port T3/E3 CEM Interface Module • 1-Port OC-192 or 8-Port Low Rate CEM Interface Module
DCC Termination	Support for DCC Termination on 1 port OC-48/STM-16 or 4 port OC-12/OC-3 / STM-1/STM-4 + 12 port T1/E1 + 4 port T3/E3 CEM Interface Module.
CEM and IP IW Feature Parity for NCS4200-1T8S-20CS and NCS4200-3GMS Interface Module	• APS and non-APS support for SDH and SONET for iMSG IPv6 interworking • NxDS0 iMSG IPv4 and NxDS0 APS iMSG IPv4 • UPSR IPv6 • IPv4 and IPv6 with VLAN handoff for both cross connect and local connect

Feature	Description
Support for all 0s and 1s BERT Patterns	Support for all 0s and 1s BERT patterns on the following Interface Modules: • 48-Port T1 or E1 CEM Interface Module • 48-Port T3 or E3 CEM Interface Module • 1 port OC-48/STM-16 or 4 port OC-12/OC-3 / STM-1/STM-4 + 12 port T1/E1 + 4 port T3/E3 CEM Interface Module • 1-Port OC-192 or 8-Port Low Rate CEM Interface Module • NCS 4200 Combo 8-Port SFP GE and 1-Port 10 GE 20G Interface Module (NCS4200-1T8S-20CS)
IP Multicast: Multicast	
Multicast SLA Measurment with MLDP	Display of aggregated egress multicast stats for BDI interfaces on Head node, which is part of the MLDP core is supported.
IP Routing: Protocol-Independent	
On-Change Notifications for IS-IS State	This feature allows you to externalize the internal state of the router for the operational data and thus enables you to access the internal state of the router. It helps in sending on-change notifications to the receiver for any change of state, for example, when the adjacency goes up or down.
Segment Routing	
L2VPN over SR-TE Preferred Path	This feature allows you to configure an SR policy as the preferred path for a VPWS or VPLS pseudowire. VPWS or VPLS pseudowires between same PEs can be routed over different SR policies based on the requirements. Prior to this release, you could only steer the traffic using the SR policy for routing IPv4 traffic to a destination pseudowire (over IGP or BGP-LU).
PCE Initiated SR Policy with OSPF Autoroute Announce	This feature enables a steering mechanism in which IGPs automatically use the policy for destination's downstream of the policy end point.
Segment Routing Flexible Algorithm support for TI-LFA uLoop Avoidance, SID Leaking, and ODN with Auto-Steering	This feature allows you to compute Loop Free Alternate (LFA) paths, TI-LFA backup paths, and Microloop Avoidance paths for a particular Flexible Algorithm using the same constraints as the calculation of the primary paths for such Flexible Algorithms, for IS-IS. Inter-area leaking of Flexible Algorithm SIDs and prefixes and selectively filtering the paths that are installed to the MFI are also supported.

Feature	Description
Telemetry (Model-Based Telemetry and Event-Based Telemetry) Support for Performance Measurement	This feature enables Model-Based Telemetry (MDT) and Event-Based Telemetry (EDT) that allow the data to be directed to a configured receiver. This data can be used for analysis and troubleshooting purposes to maintain the health of the network. The **sr_5_label_push_enable** SDM template is mandatory for this feature to function.
MPLS Basic	
Re-optimization with Tunnel Bandwidth Modification on Flex-LSP Protect Path	This feature supports Make Before Break (MBB) functionality and thus ensures there is no traffic loss when a MPLS Flex LSP tunnel runs on protect LSP (if working LSP goes down) and the tunnel bandwidth is modified. When the working LSP comes up, use the following command to manually switch from the working to protect LSP: **mpls traffic-eng switch tunnel** *tunnel-ID*.
IP SLAs	
Configurable User-Defined and EMIX Packet Size	This feature allows you to configure user-defined and Enterprise traffic (EMIX) packet sizes. Use the following commands to configure user-defined and EMIX packet sizes: • **packet-size user-defined***packet size* • **packet-size emix sequence** *emix-sequence*[**u-value** *u-value value*]
SAT based support for configurable EMIX traffic pattern in FPGA	Support for EMIX packet size is enhanced. For EMIX traffic, packet sizes of 64, 128, 256, 512, 1024, 1280, 1518, Maximum Transmission Unit (MTU) and user-defined patterns are supported. These packet sizes are forwarded in ratio of 1:1:1:1:1.
IP Routing: BFD	
BFD over G8032 and Multi EFP BDI	Scale numbers for BFD and hardware offload are enhanced for the Cisco RSP2 and Cisco RSP3 modules.
High Availability	
Secondary ROMMON Partition Auto Upgrade	This feature supports secondary ROMMON partition auto upgrade after a successful primary ROMMON partition is complete for NCS 4216 routers.
Cisco NCS 4200 Series Software	
CCP User Secret and Enable Secret masking	To support Common Criteria Policy validation for the masked secret.
Increase Maximum MTU Size	Maximum Transmission Unit (MTU) is increased to a maximum of 9644 bytes on the Cisco RSP3 module. You can configure the MTU bytes using the **mtu bytes** command.

Feature	Description
VLAN Translation for RSP3	VLAN translation provides flexibility in managing VLANs and Metro Ethernet-related services. You can configure 1:1 and 2:1 VLAN translations using the **sdm prefer enable_vlan_translation** command on the Cisco RSP3 module.

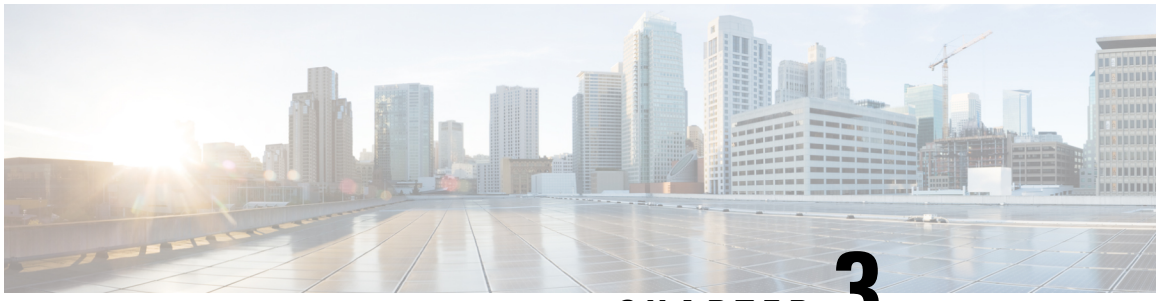
Other Supported Features in this Release

- **Programmability Features**
  - Complete YANG Model for Ethernet EVC Configuration—An Ethernet Virtual Connection (EVC) is defined by the Metro-Ethernet Forum (MEF) as an association between two or more user network interfaces that identifies a point-to-point or multipoint-to-multipoint path within the service provider network. An EVC is a conceptual service pipe within the service provider network.
  - Complete YANG Model for CFM Configuration—Ethernet Connectivity Fault Management (CFM) is an end-to-end per-service-instance Ethernet layer operations, administration, and maintenance (OAM) protocol. It includes proactive connectivity monitoring, fault verification, and fault isolation for large Ethernet metropolitan-area networks (MANs) and WANs.

  YANG Data Models—For the list of Cisco IOS XE YANG models available with this release, navigate to https://github.com/YangModels/yang/tree/master/vendor/cisco/xe/1741

  Revision statements embedded in the YANG files indicate if there has been a model revision. The README.md file in the same GitHub location highlights changes that have been made in the release.

  For more information, see *Programmability Configuration Guide, Cisco IOS XE Bengaluru 17.4.x*.



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 Bengaluru 17.4.2a

Caveat ID Number	Description
CSCvw87264	Micro BFD sessions stays down permanently after detect timer expired.
CSCvx86711	17.6.1:RSP3:uBFD Poch: BFD sessions remain DOWN/INIT after node reload.
CSCvz66437	ISSU between 17.3.x rebuild results in DSx IM reload.
CSCvz49468	APS-ACR impacted during ISSU from 16.12. to 17.3.
CSCvw48885	IM OIR as part of ISSU resulted in IOSD crash for T3/E3 RSP3 IM.

Caveat ID Number	Description
CSCvz10220	DS3 card protection - iosd crash upon no mode t3.
CSCvy46030	RSP3 - While upgrading from 17.03.01(42r) to latest Pol_dev(49r) BinOS Init script failed.

Open Caveats – Cisco IOS XE Bengaluru 17.4.2a

There are no open caveats for this release.

Resolved Caveats – Cisco IOS XE Bengaluru 17.4.2

Caveat ID Number	Description
CSCvu99207	Router: Incorrect STP forwarding state programming in platform
CSCvw56612	LOTR : Router show lic CLI does not show port details
CSCvw59531	Auto negotiation failing when CU SFP connected to 100m port
CSCvw64784	CEM ACR: Not able to reuse same clock id on another controller After deleted clock id.
CSCvw71447	RSP3: interface flaps step-by-step issu procedure post sso
CSCvw71735	Async Line raw-socket packet-length Configure to 0 on Switchover
CSCvw81102	RSP3: copy recent standby logs & corefiles to Active
CSCvw82303	Support for multicast route leaking in Native multicast
CSCvw85511	Router: BDI interface is causing high cpu usage
CSCvw93411	Interface counters not incrementing after 2yrs, 22+ weeks on Router
CSCvx01642	PPPoE tag circuit-id remote-id should not be trusted if the interface is in untrusted mode
CSCvx24923	HS1 2.43 FPGA commit for reload/brom select issue
CSCvx25220	BERT is running cannot remove mode observed while running BERT on unframed mode
CSCvx42987	On XE 17.4.1 , for mode VT1-15 , when counters are enabled on controllers , o/p of LOP is showing IP
CSCvx55831	Ingress Policy with set qos-group action is creating extra TCAM entry with match on Egress Policy

Resolved Caveats – Cisco IOS XE Bengaluru 17.4.2 - Platform Independent

Caveat ID Number	Description
CSCvv79677	Router crashed after BGP flaps
CSCvx19209	ISIS crash in isis_sr_tilfa_compute_protection
CSCvx26650	On configuring route tag under ISIS, TI-lFA is not forming repair path

Open Caveats – Cisco IOS XE Bengaluru 17.4.2

There are no open caveats for this release.

Resolved Caveats – Cisco IOS XE Bengaluru 17.4.1

Caveat ID Number	Description
CSCvn47496	ENH : RSP3C Request for overriding restriction "MVPN-GRE VRF-SM: RP must be at Encap PE"
CSCvt42842	RSP3-400S: Flood of "SKB received from Kernel, and could not find SA" kernel logs
CSCvt58155	rsp3c: Kernel crash bcmINTR rcu_check_callback
CSCvt64706	CPU HOG due to constant soft-parity errors
CSCvt72171	v173 cardprotection after doing im_oir traffic is not happening on NCS4200-48T3E3-CE1
CSCvt74987	v1731: tunnels with more than 1500b certificate is not coming up
CSCvt75327	v1731: Traffic is not happend after doing sso in Imsg_Mixmode
CSCvt76777	[17.3.1 BB]: Adj error object on removing sr-label-preferred.
CSCvt78211	A900-IMA3G-IMSG: Serial interface gets blocked after reaching count of 700 for non acr and non pg
CSCvt82525	ASR 900 crash while IPV6 updating prefixes
CSCvt96614	More than 1 second TI-LFA convergence is seen with 250 PDP and 250 PFP tunnels
CSCvu13886	v174: card protection performing shut/no shut on the CPG sts1e, could see SLOS alarm on the Peer.
CSCvu18276	ASR903 Standby RSP3 crash during IOS upgrade

Caveat ID Number	Description
CSCvu29991	Historic performance intervals are not present for STS1 E interfaces in CLI as well as SNMP MIB
CSCvu30972	ASR903: All readings for Power supply unit reflect as zero though the unit is functional
CSCvu31393	[RSP3-poch-Mcast]: igmp queries are not egressing out of poch in a sequence
CSCvu36636	ASR900 ROMMON region 0 and 1 verification CLI
CSCvu38550	For VCOP configured with type DS3 , Applique type should be Subrate T3 instead of Channelized T3/T1
CSCvu43329	Remote Loopback: Far end did not go into loop for T3 RL in A900-IMA1Z8S-CX
CSCvu45472	A900-IMA3G-IMSG: Serial interface gets blocked after reaching count of 700 for acr and pg
CSCvu45833	ISSU : 1612-173 : CEM Ckt stuck at Setup Failed
CSCvu51472	Support for SAToP payload 64 byte and dejitter 2 ms in LOTR IM's
CSCvu57879	OIR of A900-IMA48T-C IM in bay 12 affects RX traffic of A900-IMA1Z8S-CX IM in bay 0
CSCvu66126	OC192 APS Group Stuck with Signal Fail condition
CSCvu67675	17.3.1:RSP3: >3000ms TI-LFA convergence is seen with SR PFP configured
CSCvu92797	RSP3-VZ: Observing traceback while executing IM-OIR cleanup test.
CSCvv10139	Uea-iomd phase1 IM FPD ugprade Ver-0x4B commit
CSCvv13495	17.1.1. Loopback local not working on T3 card protection physically connected ports
CSCvv18671	RSP3-400S: Kernel crash - arch_cpu_idle+0x30/0xa0 during SSO Soak
CSCvv31617	e2e circuit not pinging serial interface up & line protocol up

Open Caveats – Cisco IOS XE Bengaluru 17.4.1

Caveat ID Number	Description
CSCvv33300	Alarm-profile : APS configured for Au-4 mode t3 , e3 after SSO alarms are removed
CSCvv72192	IMA2Z IM, xfp and sfp+ are present then XFP is removed LED still shows as green
CSCvw15076	16.12.3-75.1/75.2 With VP and Fixed port the ptp state shows freq-locked
CSCvw34109	PTP RX failure due to LSMPI buffer exhaustion

Caveat ID Number	Description
CSCvv43263	17.4.1: RSP3: BGP PIC edge cutover convergence is high for Global prefixes with VPLS_stats enabled
CSCvv40904	RSP3-400S: kernel crash during SSO secfp_MapPolInSA+0x134/0x5f0
CSCvw34109	PTP failure due to LSMPI buffer exhaustion

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