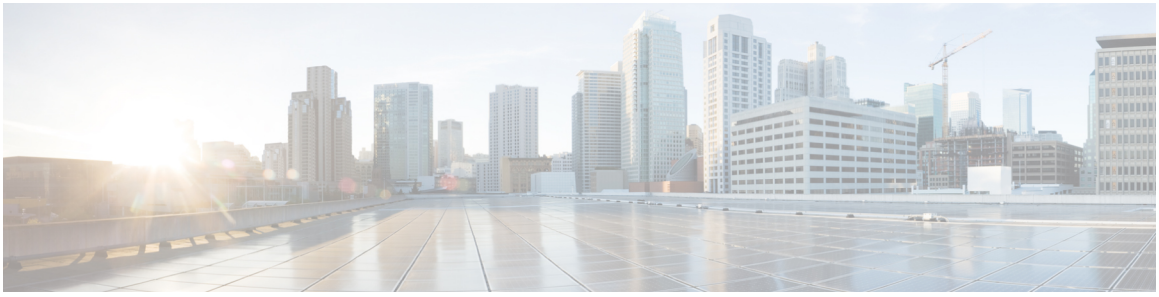
Release Notes for Cisco NCS 4206 and Cisco NCS 4216 Series, Cisco IOS XE Everest 16.6.x

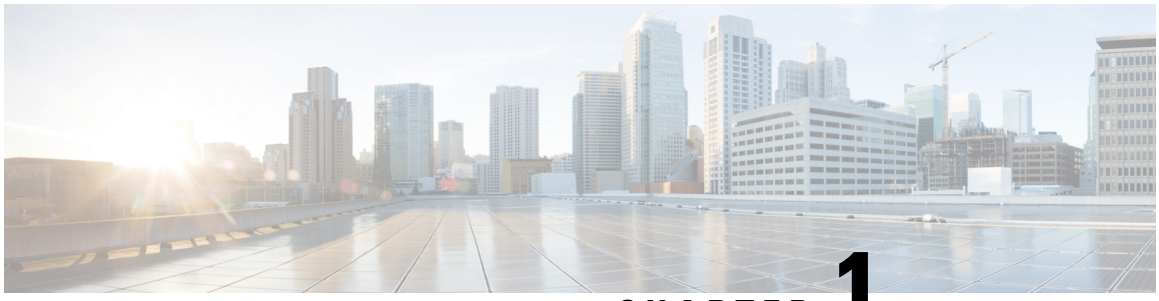
First Published: 2017-08-02

Last Modified: 2018-12-14

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

The Cisco NCS 4206 and Cisco NCS 4216 are full-featured, modular aggregation platforms designed for the cost-effective delivery of converged mobile, residential, and business services.

This document provides information about the IOS XE software release for the Cisco NCS 4206 and Cisco NCS 4216 beginning with Cisco IOS XE Everest 16.5.1, which is the first supported release in the Release 16 Series.

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.

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

The following table lists the supported interface modules for Cisco NCS 4206 chassis:

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 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
	OC-192 Interface module + 8-port Low Rate Interface Module	NCS4200-1T8S-10CS	2,3, 4 and 5
	48 X T1/E1 CEM Interface Module	NCS4200-48T1E1-CE	All
	48 X T3/E3 CEM Interface Module	NCS4200-48T3E3-CE	All

Cisco NCS 4216 RSP Supported Interface Modules

The following table lists the RSP supported interface modules for Cisco NCS 4216 chassis:

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
	1x100G Interface module	NCS4200-1H-PK	7, 8
	2x40G Interface module	NCS4200-2Q-P	3, 4, 7, 8, 11, 12
	8x10G Interface module	NCS4200-8T-PS	3, 4, 7, 8, 11, 12
	OC-192 Interface Module with 8-port Low Rate CEM Interface Module (10G HO / 10G LO)	NCS4200-1T8S-10CS	3, 4, 7, 8, 11, 12
	OC-192 Interface Module with 8-port Low Rate CEM Interface Module (5G HO / 5G LO)	NCS4200-1T8S-10CS	2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15
	48XT1/E1 Interface module	NCS4200-48T1E1-CE	2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15
	48XT3/E3 Interface module	NCS4200-48T3E3-CE	2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15

Restrictions and Limitations for Cisco NCS 4206 and Cisco NCS 4216

- Far end PMON counters are not supported.
- VT PMON is not supported.
- M13 framing (channelized) is not supported on DS3 IM.
- 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.
- Alternate 0's and 1's BERT pattern is not supported for DS1.
- 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 OCx.

- Port restriction on OCx. If you have OC48 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.
- DS3 over CEP is not supported on DS3 IM.
- 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.
- Crash may be observed on the chassis when EoMPLS, CEM, ATM and IMA Pseudowire Redundancy (PW-redundancy) configurations exist while switchover and fail back of the pseudowires are being triggered, and the **show platform hardware pp active pw eompls** command is executed.
- 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.
- UPSR is supported only on VT path and STSnc. It is not supported on T1/T3.
- DCC is supported only on PPP encapsulation. It is not supported on CLNS encapsulation.
- Traffic is dropped when packets of size 64 to 100 bytes are sent on 1G and 10G ports.
  - For 64-byte packets, traffic drop is seen at 70% and beyond of the line rate.
  - For 90-byte packets, traffic drop is seen at 90% and beyond of the line rate.
  - For 95-byte packets, traffic drop is seen at 95% and beyond of the line rate.

  Traffic is dropped when:
  - Traffic is sent on a VRF interface.
  - Traffic is sent across layer 2 and layer 3.

  However, traffic is not dropped when the packet size is greater than 100 bytes, even if the packets are sent bidirectionally at the line rate.
- 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.

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.

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 1: 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	8x10G FPGA	2x40G FPGA	1x100G FPGA
IM FPGA	3.18SP	1.22	1.22	1.12	0.17 (0x1100 H)	0.22 (0x1600 H)	0.19 (0x1300 H)
CEM FPGA		4.6	4.6	6.6	—	—	—

	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	8x10G FPGA	2x40G FPGA	1x100G FPGA
IM FPGA	3.18.1SP	1.22	1.22	1.12	0.17 (0x1100 H)	0.22 (0x1600 H)	0.19 (0x1300 H)
CEM FPGA		4.6	4.6	7.0	—	—	—
IM FPGA	16.5.1	1.22	1.22	1.15	0.21 (0x1500 H)	0.22 (0x1600 H)	0.20 (0x1400 H)
CEM FPGA		0x46310046	0x46310046	5G mode: 0x10070059 10G mode: 0x10050073	—	—	—
IM FPGA	16.6.1	1.22	1.22	1.15	0.21 (0x1500 H)	0.22 (0x1600 H)	0.20 (0x1400 H)
CEM FPGA		0x46310046	0x46310046	5G mode: 0x10070059 10G mode: 0x10050073	—	—	—

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)
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)

Supported MIBs		
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)	

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

Unverified MIBs		
ATM-MIB	CISCO-IETF-DHCP-SERVER-EXT-MIB	EXPRESSION-MIB
CISCO-ATM-EXT-MIB		HC-ALARM-MIB
CISCO-ATM-IF-MIB	CISCO-IETF-PPVPN-MPLS-VPN-MIB	HC-RMON-MIB
CISCO-ATM-PVC-MIB	CISCO-IP-STAT-MIB	IEEE8021-CFM-MIB
CISCO-ATM-PVCTRAP-EXTN-MIB	CISCO-IPSLA-ETHERNET-MIB	IEEE8021-CFM-V2-MIB
CISCO-BCP-MIB	CISCO-L2-CONTROL-MIB	IEEE8023-LAG-MIB
CISCO-CALLHOME-MIB	CISCO-LAG-MIB	INT-SERV-GUARANTEED-MIB
CISCO-CIRCUIT-INTERFACE-MIB	CISCO-MAC-NOTIFICATION-MIB	INTEGRATED-SERVICES-MIB
CISCO-CONTEXT-MAPPING-MIB	CISCO-MEMORY-POOL-MIB	MPLS-L3VPN-STD-MIB (RFC 4382)
CISCO-EIGRP-MIB	CISCO-NHRP-EXT-MIB	MPLS-LDP-ATM-STD-MIB (RFC 3815)
CISCO-ERM-MIB	CISCO-NTP-MIB	MPLS-LDP-MIB
CISCO-ETHER-CFM-MIB	CISCO-PING-MIB	MPLS-TE-STD-MIB
CISCO-ETHERLIKE-EXT-MIB	CISCO-RESILIENT-ETHERNET-PROTOCOL-MIB	MPLS-VPN-MIB
CISCO-EVC-MIB	CISCO-RTTMON-ICMP-MIB	NHRP-MIB
CISCO-HSRP-EXT-MIB	CISCO-RTTMON-IP-EXT-MIB	RFC2006-MIB (MIP)
CISCO-HSRP-MIB	CISCO-RTTMON-RTP-MIB	RMON2-MIB (RFC 2021)
CISCO-IETF-ATM2-PVCTRAP-MIB	CISCO-SNMP-TARGET-EXT-MIB	SMON-MIB
CISCO-IETF-ATM2-PVCTRAP-MIB-EXTN	CISCO-TCP-MIB	VRRP-MIB
CISCO-IETF-BFD-MIB	CISCO-VRF-MIB	
CISCO-IETF-DHCP-SERVER-MIB	ETHER-WIS (RFC 3637)	

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:

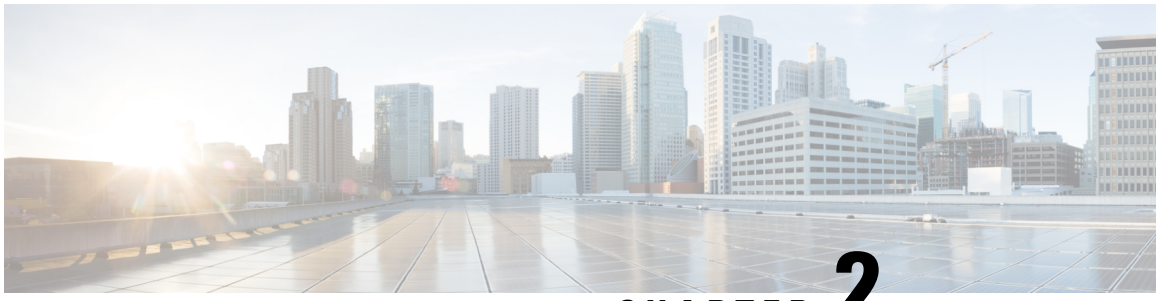
http://www.cisco.com/en/US/products/ps11174/products_licensing_information_listing.html

Communications, Services, and Additional Information

- 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

New Features

This chapter describes the new hardware and software features supported on the Cisco NCS 4200 Series in this release.

New Software Features for NCS 4206 and NCS 4216 in Cisco IOS XE Everest 16.6.9

There are no new software features in Cisco IOS XE Everest 16.6.9.

New Hardware Features for NCS 4206 and NCS 4216 in Cisco IOS XE Everest 16.6.9

There are no new hardware features in Cisco IOS XE Everest 16.6.9.

New Software Features for NCS 4206 and NCS 4216 in Cisco IOS XE Everest 16.6.8

There are no new software features in Cisco IOS XE Everest 16.6.8.

New Hardware Features for NCS 4206 and NCS 4216 in Cisco IOS XE Everest 16.6.8

There are no new hardware features in Cisco IOS XE Everest 16.6.8.

New Software Features for NCS 4206 and NCS 4216 in Cisco IOS XE Everest 16.6.7

There are no new software features in Cisco IOS XE Everest 16.6.7.

New Hardware Features for NCS 4206 and NCS 4216 in Cisco IOS XE Everest 16.6.7

There are no new hardware features in Cisco IOS XE Everest 16.6.7.

New Software Features in Cisco IOS XE Everest 16.6.6

There are no new software features in this release.

New Hardware Features in Cisco IOS XE Everest 16.6.6

There are no new hardware features in this release.

New Software Features for NCS 4206 and NCS 4216 in Cisco IOS XE Everest 16.6.4

There are no new software features in Cisco IOS XE Everest 16.6.4.

New Hardware Features for NCS 4206 and NCS 4216 in Cisco IOS XE Everest 16.6.4

There are no new hardware features in Cisco IOS XE Everest 16.6.4.

New Software Features for NCS 4206 and NCS 4216 in Cisco IOS XE Everest 16.6.3

Card Protection for 48-port T1/E1 CEM Interface Module and 48-port T3/E3 CEM Interface Module

The card protection feature protects traffic when the interface module is out of service, a software failure occurs, or hardware issues are observed. Card protection is supported on primary and backup cards. Traffic is switched to the backup interface module when the primary interface module does not respond and vice versa. A new Y-cable is introduced to support the feature. The following maintenance commands are added in this release:

- lockout
- Force
- Manual

Note This feature does not require any change in the patch panel of the interface modules.

New Hardware Features for NCS 4206 and NCS 4216 in Cisco IOS XE Everest 16.6.3

There are no new hardware features in Cisco IOS XE Everest 16.6.3.

New Software Features for NCS 4206 and NCS 4216 in Cisco IOS XE Everest 16.6.1

- **16K EFP QoS Support**

  Starting Cisco IOS Release 16.6.1, 16K EFPs are supported on the RSP3 module. For more information, see Quality of Service Configuration Guidelines, Cisco IOS XE Everest 16.6.1 (Cisco NCS 4200 Series).

- **Auto In-Service States for Ports**

The Cisco ASR 900 series routers with RSP3 module now support management of equipment and port state model in two modes. These modes are the transport mode and the router mode. For more information, see Auto In-Service States, Cisco IOS XE Everest 16.6.1 (NCS 4200 Series).

- **Configuring Data Communication Channel**

  The Data Communication Channel (DCC) feature uses the SONET or SDH Operation Administration and Maintenance (OAM) channel to manage devices that support SONET or SDH interfaces. SONET or SDH standards support extensive operations, administration, management, and provisioning (OAM&P) capabilities. The following overhead bytes are specified in the standards as the OAM channels that carry management information, alarms, and management commands:

  - D1 to D3 bytes of the Section overhead
  - D4 to D12 bytes of the Line overhead

  These overhead bytes are referred to as the Data Communication Channel (DCC). ITU-G.7712 has defined the following three DCC network domains:

  - OSI DCC network
  - IP DCC network
  - OSI+IP DCC network

  Effective Cisco IOS XE Everest 16.6.1 release, only OSI DCC network and IP DCC network are supported, which implies that same type of network resides on either side of the router.

  For more information, see 1-Port OC-192 or 8-Port Low Rate CEM Interface Module Configuration Guide, Cisco IOS XE Everest 16.6.1 (Cisco NCS 4200 Series).

- **Configuring MSP on 1-Port OC192/STM-64 or 8-Port OC3/12/48/STM-1/-4/-16 Module**

  Multiplex Section Protection (MSP) is a protection mechanism for SDH networks that enables SDH connections to switch to another SDH circuit when a circuit failure occurs. A protection interface serves as the backup interface for the working interface. When the working interface fails, the protection interface quickly assumes its traffic load.

  The SDH protection schemes comply with GR-253 and ITU-T G.783. It allows Optical Interface Module to work seamlessly as SDH Add or Drop Multiplexers (ADMs). The implementation of the above protection schemes allows a pair of SDH lines or paths to be configured for line or path redundancy. In the event of a fiber cut, the active line or path switches automatically to the standby line or path up to 60 milliseconds (2/5/10 millisecond for holdover and 50 millisecond switchovers).

  For more information, see 1-Port OC-192 or 8-Port Low Rate CEM Interface Module Configuration Guide, Cisco IOS XE Everest 16.6.1 (Cisco NCS 4200 Series).

- **Configuring SDH on 1-Port OC192/STM-64 or 8-Port OC3/12/48/STM-1/-4/-16 Module**

  Synchronous Digital Hierarchy (SDH) is used in Europe by the International Telecommunication Union Telecommunication Standardization Sector (ITU-T) that defines optical signals and a synchronous frame structure for multiplexed digital traffic. SDH equipment is accepted everywhere except North America.

  Prior to Cisco IOS XE Everest 16.5.1, Synchronous Optical NETwork (SONET) was supported on 1-Port OC192/STM-64 or 8-Port OC3/12/48/STM-1/-4/-16 Module for NCS 4200 Series Routers. SONET equipment is generally used in North America. 4-Port OC3 STM1 or 1-Port OC12 STM4 Module did not support all possible combinations of the SDH hierarchy.

Effective Cisco IOS XE Everest 16.6.1, SDH is supported on 1-Port OC192/STM-64 or 8-Port OC3/12/48/STM-1/-4/-16 Module along with SONET for NCS 4200 Series Routers. The IM supports the entire SDH hierarchy (except VC-2/C-2).

For more information, see 1-Port OC-192 or 8-Port Low Rate CEM Interface Module Configuration Guide, Cisco IOS XE Everest 16.6.1 (Cisco NCS 4200 Series).

- **Configuring SNCP on 1-Port OC192/STM-64 or 8-Port OC3/12/48/STM-1/-4/-16 Module**

  SNCP is a protection mechanism for SDH networks that enables SDH connections to switch to another SDH circuit when a circuit failure occurs. A protection interface serves as the backup interface for the working interface. When the working interface fails, the protection interface quickly assumes its traffic load.

  The SDH protection schemes comply with GR-253 and ITU-T G.783. It allows Optical Interface Module to work seamlessly as SDH Add or Drop Multiplexers (ADMs). The implementation of the above protection schemes allows a pair of SDH lines or paths to be configured for line or path redundancy. In the event of a fiber cut, the active line or path switches automatically to the standby line or path up to 60 milliseconds (2/5/10 millisecond for holdover and 50 millisecond switchovers).

  For more information, see 1-Port OC-192 or 8-Port Low Rate CEM Interface Module Configuration Guide, Cisco IOS XE Everest 16.6.1 (Cisco NCS 4200 Series).

- **Displaying OBFL Information**

  The following new command is introduced to display any hardware error in the setup:

  show logging onboard hw_errors

  For more information, see System Logging Guide, Cisco IOS XE Everest 16.6.1 (NCS 4200 Series).

- **DS1 and DS3 Card Protection**

  DS1 and DS3 card protection feature is required to protect traffic when the interface module is out of service, there is any software failure, or any hardware issues. Effective Cisco IOS XE Everest 16.6.1, only non-revertive 1:1 switching mode is supported. This feature is only supported on T1 and T3 interface modules. Card protection has primary and backup cards. Traffic is switched to back up the interface module when the primary interface module does not respond and vice versa.

  This feature does not require any change in the patch panel of the interface modules. A new Y-cable is introduced to support the feature. Effective Cisco IOS XE Everest 16.6.1, the virtual controller only supports CEM level configuration and all other configurations are supported on both the physical interface modules.

  For more information, see Cisco NCS 4200 Series Software Configuration Guide, Cisco IOS XE Everest 16.6.1.

- **Routed Psuedowire and VPLS on the RSP3 Module**

  Starting Cisco IOS Release 16.6.1, Routed pseudowire and VPLS is supported on the RSP3 module. For more information, see

  MPLS Layer 2 VPNs Configuration Guide, Cisco IOS XE Everest 16.6.1 (NCS 4200 Series).

- **Split Horizon Enhancements**

  The efp_feat_ext template is introduced on the RSP3 module. This template when enabled allows configuration of two split-horizon groups on the EVC bridge-domain. For more information, see Carrier Ethernet Configuration Guide, Cisco IOS XE Everest 16.6.1 (Cisco NCS 4200 Series).

For information on sdm prefer efp_feat_ext command see Cisco IOS Multiprotocol Label Switching Command Reference.

- **TWAMP MPLS Support**

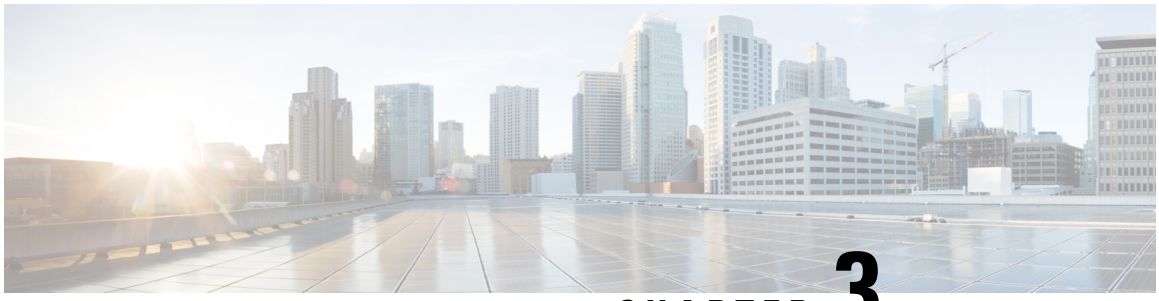
  Effective Cisco IOS-XE Everest 16.6.1, time stamping is supported on MPLS/VPLS interfaces. For more information, see IP SLAs Configuration Guide, Cisco IOS XE Everest 16.6.1 (Cisco NCS 4200 Series).

- **VPLS over IP FRR, rLFA, BGP PIC, RFC 3107 Intra, and Inter AS**

  Effective with Cisco IOS XE Everest 16.6.1, VPLS over IP FRR , rLFA , BGP PIC, RFC 3107 intra, and inter AS is supported. For more information, see MPLS Layer 2 VPNs Configuration Guide, Cisco IOS XE Everest 16.6.1 (NCS 4200 Series).

New Hardware Features for NCS 4206 and NCS 4216 in Cisco IOS XE Everest 16.6.1

There are no new hardware features in Cisco IOS XE Everest 16.6.1.



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.

• Open Caveats – Cisco IOS XE Everest 16.6.1, on page 32
• Resolved Caveats – Cisco IOS XE Everest 16.6.1, on page 34

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

Open Caveats – Cisco IOS XE Everest 16.6.9

Caveat ID Number	Description
CSCve78337	MLP MRAPS convergence is high on Work-Active SSO node
CSCvf08656	Cisco RSP3 module: Traffic fails for few labelled BGP prefixes (BGP label imposed is incorrect)
CSCvn47496	ENH : RSP3C request for overriding restriction "MVPN-GRE VRF-SM: RP must be at Encap PE"
CSCvr54918	MPLS MTU is not correctly derived from interface MTU after reload
CSCvs19041	Traffic sent to the subnets routed over VRF, packets ends up in default class - wrong classification
CSCvw64784	Cisco RSP2 Module CEM ACR: Unable to reuse same clock ID on another controller after clock ID is deleted.

Platform Independent Open Caveats – Cisco IOS XE Everest 16.6.9

Caveat ID Number	Description
CSCvg75709	Unnecessary RIB updates are observed when metric-style transition is configured.
CSCvs15808	VRRPv3 fails on port-channel sub-interface.
CSCvt08609	Secondary IP address is invisible when interface configure with DHCP as primary ip address

Resolved Caveats – Cisco IOS XE Everest 16.6.9

Caveat ID Number	Description
CSCvr69196	Cisco IOS XE software for Cisco ASR 900 Series RSP3 arbitrary code execution vulnerability
CSCvs34482	ISSU is not working on Cisco RSP2 module nodes
CSCvt99095	Traceback: High CPU on standby RSP due to IOMD with A900-IMASER14A/S installed

Platform Independent Resolved Caveats – Cisco IOS XE Everest 16.6.9

Caveat ID Number	Description
CSCvr83128	Cisco IOS and IOS XE software MP-BGP EVPN Denial of Service vulnerability
CSCvt78186	Cisco IOS and IOS XE Software split DNS Denial of Service vulnerability
CSCvu18001	Segmentation fault observed in BGP -"UNIX-EXT-SIGNAL: Segmentation fault(11), Process = BGP Scanner"
CSCvu85572	Dynamic neighbor does not form when peer-group is shutdown in different VRF
CSCvv64633	BGP: advertised community list is malformed due to GSHUT community

Open Caveats – Cisco IOS XE Everest 16.6.8

Caveat ID Number	Description
CSCvf08656	Traffic failure occurs for few labelled BGP prefixes (BGP label imposed is incorrect).
CSCvk68174	Led Indicator shows down after configuring xconnect.

Resolved Caveats – Cisco IOS XE Everest 16.6.8

Caveat ID Number	Description
CSCvk56297	Enhancement request to warn about different software image in Cisco RSP3 Module.
CSCvt15949	Configuration and unconfiguration of ACL with **`running-config`** CLI result in error objects.

Open Caveats – Cisco IOS XE Everest 16.6.7

Caveat ID Number	Description
CSCvq74237	Critical Alarm for serial card reappear after RP switch over
CSCvk68174	Led Indicator on router showing down after configuring xconnect
CSCvq74237	Critical Alarm for serial card reappear after RP switch over

Open Caveats – Platform Independent

Caveat ID Number	Description
CSCvn22199	ISR4K fails to authenticate users via dot1x following interface flap
CSCvo58118	CTS Environment-data is not getting refreshed on the device
CSCvp66281	default ip forward-protocol udp xx changed to no ip forward-protocol udp xx after rollback
CSCvq56114	Cat3k crash in IGMP code due to invalid source count in DNS lookup
CSCvq57996	RADIUS attribute 4 (NAS-IP-Address) is not honored
CSCvq69866	HSRPv2 crash whilst retrieving group from received packet
CSCvq72298	Router crashed on running show policy-map interface <> output command
CSCvq75307	Crash due to watchdog after adding a prefix-list/ Route-map entry to existing route map.
CSCvq78692	mGRE L3VPN broken after reload
CSCvq89252	IP SLA for Path-Jitter returning a value which isn't defined by the MIB
CSCvq91789	When issuing ip helper-addresss x.x.x.x command, "sh run" and "sh run all" show differently
CSCvq97365	2 interfaces of client in different vrf connected to same vlan of server not able to get ip via dhcp
CSCvr00183	AAA accounting issue after router reload when mGRE and L3VPN configured
CSCvr00344	"ip access-list logging hash-generation" removes ACL statements upon reload
CSCvr05406	LISP Map-cache not updated correctly after wired Host-mobility
CSCvr08961	Switch stop responding to CoA
CSCvr10897	Adjacency SIDs not detected in mpls traffic-eng topology (interop issue)

Caveat ID Number	Description
CSCvr26105	ICMP Redirect Message is sending incorrect next-hop in the "gateway address"
CSCvr26693	The order of cEigrpPeerAddrType value and cEigrpPeerAddr value does not follow SNMP Object Navigator
CSCvr31017	ip gratuitous ARP is not VRF aware
CSCvr32292	Router may crash due to segmentation fault after running EEM script

Resolved Caveats – Cisco IOS XE Everest 16.6.7

Caveat ID Number	Description
CSCvj00222	Intermittent packet drops for small size vrf ping (64-72)
CSCvp24919	ToD UBX Format - Incorrect header and checksum calculation
CSCvp67001	Secure FPGA

Resolved Caveats - Platform Independent

Caveat ID Number	Description
CSCvd55092	C3650 traffic will not be block although hit deny ACL entry
CSCvd67904	4500X does not run dot1x when a laptop wakes from sleep mode
CSCve57810	Amur failing over w/o 'fail next-method' or 'no-response next method'
CSCvg32153	"show interface port-channel" falsely reports output drops when there are no actual output drops
CSCvh26032	ICMP Redirect Message is sending incorrect next-hop in the'"gateway address"
CSCvh49874	FNF monitor download to DP failed after changing netflow record
CSCvi22263	Crash when IOS is adapting shaping with Adaptive QoS over DMVPN configured
CSCvj41876	Prefixes are stuck indefinitely in the BGP pending-prefixes list
CSCvj76866	Partial Power Failure in Stack Causes Interfaces to Become "shutdown"
CSCvk51939	SSS Manager Traceback observer when test MLPPP
CSCvm10850	Crash after CPUHOG in ISDN L2D SRQ Process
CSCvm47690	Addition/Edits to numbered OG ACL using "access-list <>" command does not re-expand the ACL.

Caveat ID Number	Description
CSCvn00104	Software crash due to memory corruption after packet trace was enabled.
CSCvn23906	DHCP Server sends Renew ACKs to Clients with 00:00:00:00:00:00 MAC in L2 frame
CSCvn45732	Device crashing if we unconfigure the NTP on the device
CSCvn78961	Subscribers cannot re-login due to CoA time-out (lite-sessions in routed mode)
CSCvo06817	Router crash while executing show commands using '|' (pipe) to filter the output.
CSCvo10145	Memory overlay crash when using include-cui
CSCvo10491	PnP Agent should detect image upgrade scenario and configure dialer to bring up cellular interface
CSCvo17287	ASR1001-X crashed upon receiving Radius Access-Accept message
CSCvo21122	Memory leak at hman process
CSCvo36031	WSMA crash formatting show command output
CSCvo55194	After RSP switchover label imposition was not programmed in Software on APS standby router
CSCvo58098	CTS PACS not downloading to the devices
CSCvo65415	ASR1k crashes by handling DHCP packet
CSCvo71721	When sending account-logon ISG do not reply with ACK nor NACK.
CSCvo87827	Crash when polling IPForwarding MIB
CSCvo90060	Wrong label programming leading to traffic drop
CSCvp24981	When FQDN used for APN, IOS DNS resolves FQDN to IP, but GTP stays in DNS pending and IP 0.0.0.0
CSCvp27220	Tail drops on IPSLA sender when using scaled udp-jitter probes
CSCvp38407	"Radius-server attribute 31" command broken on LNS when LAC sends Remote-Id string
CSCvp70443	isdn cause-location command support for switch-type primary-ntt
CSCvp72379	ip dns primary command does not get removed
CSCvp74674	QoS fails to apply to tunnel2 when underlying tunnel1 reachability change
CSCvp84831	name-ip_address mapping is bypassed when the ip domain command is configured on Cisco C1111X Router
CSCvp87488	no login on-success log CLI does not persist across device reloads
CSCvq00263	Device crashed @ radius_io_stats_timer_handler due to dynamic-author

Caveat ID Number	Description
CSCvq04828	VRF aware reverse DNS lookup not working
CSCvq04989	ping between 2 Interfaces is not working , dialer interface is interferring in the ARP Processs
CSCvq20005	SRMS tries to build a snapshot when there are no SIDs
CSCvq50202	Class-attributes duplicated after EAP reauthen. in ISG radius proxy scenario
CSCvq58265	ASR1K BGP PIC Repair path broke after link flap
CSCvq65283	VXLAN EVPN BGP NEXTHOP not correctly changed with Route-map

Open Caveats – Cisco IOS XE Everest 16.6.6

Caveat ID Number	Description
CSCvp12102	New MPLS entry caused the router to crash
CSCvj33102	[SVSP-215]-AINS card type profile not working post router reload for DS1 card

Resolved Caveats – Cisco IOS XE Everest 16.6.6

Caveat ID Number	Description
CSCvj50537	ISSU Failure
CSCvk54023	Convergence delay in active RSP removal
CSCvk75941	Interface comes out of PoCH on IM OIR followed by RP OIR.
CSCvn08456	Giant counters incremented for packets bigger than 1500 bytes

Open Caveats – Cisco IOS XE Everest 16.6.5a

Caveat ID Number	Description
CSCvc38475	Serdes not locking with ISSU and reload
CSCvd44667	RSP3: PREFIX Object Errored Objects on Local Core Flaps and in Parallel on Other Routers in the Core
CSCve10095	Traffic is getting dropped in both direction due to hw programming went for toss
CSCve16996	Ingress classification misbehaves after removing set qos-group statement from a class.

Caveat ID Number	Description
CSCve22604	RSP3:QOSMGR-4-QUEUE_EXCEEDING_HW messages are seen on port-channel remove and re-config
CSCve37392	RSP3: with ingress dscp (1k tcam scale)policy-map scale and remove, stale TCAM entry found
CSCve63423	Egress Policy-map stats(Output packet counts) accounting twice with policy at Port and EFP
CSCve86912	[Counter]: Giant/Runt/Pause Frame counters issue.
CSCvf08656	RSP3 : Traffic failure for few Labelled BGP prefixes (BGP label imposed is incorrect)
CSCvf45267	RSP3 - Loadbalance map not getting deleted (IM OIR)
CSCvg76895	VID.116-ONS-SI-2G-L1 SFP is rejected by Sonet Module - OC48 SFP Init failure image
CSCvj33102	[SVSP-215]-AINS card type profile not working post router reload for DS1 card
CSCvj75078	RSP3: IOMD crash @ iomd_bsess_open_callback_retry on new active after RP SSO
CSCvk54023	Convergence delay in active RSP removal
CSCvn08456	RSP3: Giant counters incremented for packets bigger than 1500 bytes
CSCvn43045	[RSP3] DHCP packets dropped over the split horizon VPLS EFP
CSCve64323	RSP1:MPLS MTU programming fails on standby with latest image
CSCve72906	RSP3:ECMP LB seen when flags field is changed in ip header with l4 header in 4 label scenario
CSCvg43968	CRETE:Cylon Mgr crash @ adjmgr_get_fid_index
CSCvi21714	ASR907 showing alarms of power supply 3 missing
CSCvi53346	RSP3 : BFD packets not sent out towards 9K after timer change and link flap
CSCvi79409	ENM flaps/hangs on configuring CEM interface
CSCvi92596	ISSU: interface module delay calculation needs to be enhanced for TDM IMs
CSCvj50335	SERDES lock issue on DS1 IM in slot15
CSCvj60379	RSP3: ARP Request Not Generated when IPv4 Routable Packets with L4 Header are Punted
CSCvk07960	RSP3_400 - silent reload - Last reload reason: Critical process smand fault on rp_0_0 (rc=0)
CSCvk62834	16101:cylon_mgr crash@nile_cef_prefix_v4u_get_adj_info seen in soak run on 16th July Polaris image

Caveat ID Number	Description
CSCvm96368	non-Cisco USB is not recognized in rommon while it shows up in IOS-XE
CSCvh05072	Cem Sys : LOF/AIS are set on T3 under STS in arrive but not asserted in IOS
CSCvi40742	Configuration change on E&M interface results in xconnect failure
CSCvm84355	[SVSP-299]-'linkDown' trap should not be sent when the port is in AINS mode-[SVSPE-570]
CSCvk47892	ASR900-RSP3C-400:For ONS-SC+-10G-Z SFP , intf doesnt come up aftr "hw-module subslot <>stop/start"
CSCvd58289	IPC buffer leak during error conditions

Resolved Caveats – Cisco IOS XE Everest 16.6.5a

Caveat ID Number	Description
CSCvd58289	IPC buffer leak during error conditions
CSCve64323	RSP1:MPLS MTU programming fails on standby with latest image
CSCve72906	RSP3:ECMP LB seen when flags field is changed in ip header with l4 header in 4 label scenario
CSCvi21714	ASR907 showing alarms of power supply 3 missing
CSCvi53346	RSP3 : BFD packets not sent out towards 9K after timer change and link flap
CSCvi92596	ISSU: interface module delay calculation needs to be enhanced for TDM IMs
CSCvj50335	SERDES lock issue on DS1 IM in slot15
CSCvj60379	RSP3: ARP Request Not Generated when IPv4 Routable Packets with L4 Header are Punted
CSCvk07960	RSP3_400 - silent reload - Last reload reason: Critical process smand fault on rp_0_0 (rc=0)
CSCvm96368	non-Cisco USB is not recognized in rommon while it shows up in IOS-XE
CSCvh06656	Malformed OSPF packet causes crash
CSCvg28351	VPLS with Segment Routing not flowing traffic.
CSCvi21308	RSP3_400 : Tx bias values are high on CPAK-100G and QSFP-40G SFP's
CSCvi67694	100Gig link is up in one node and down in peer side after multiple reloads with CPAK-SR-10 optics
CSCvk20779	APS switch times exceed 50ms in Rx direction for T3 SATOP with Eomer

Open Caveats – Cisco IOS XE Everest 16.6.4

Caveat ID Number	Description
CSCui87222	IP directed-broadcast functionality not working on RSP1/RSP2
CSCve73831	THS:After SSO/ISSU observed AIS Alarm in SYSTEM THS with XE318SP Image
CSCvf55327	CLNS interop with ONS not working
CSCvg21899	Traffic forwarding not happening for VLANs added via "encap dot1q add" command in TEFP
CSCvh52244	Uni-directional communication failure with IOT Legacy IMs
CSCvh55384	Need to Accept User Configurable 4Wire E&M CEM Payload and Dejitter Buffer Values
CSCvh55399	T1 Service Latency is Asymmetric in a Simple Linear Topology
CSCvh69270	RSP2_MLDP-Rentry chunk memory leak when zapping the multicast channels
CSCvh76761	A900-RSP3C-200-S RSP module crashes while MPLS TE tunnel interfaces comes up
CSCvh79267	RSP3: Hundredgig interface goes down with reload with SR10 H/W settings
CSCvi21134	C37.94 port change leads to controller flap
CSCvi25653	TDM-IOT: observing uni-directional traffic failure after replacing TDM IM with IOT IM
CSCvi32766	9400: entSensorThreshold traps are generated even when temperature threshold isn't crossed
CSCvi41087	E&M:Payload size other than multiple of 48(96,192...) bytes never work in TO mode
CSCvi55229	ENM Type 3 doesnt work on port 4 , if port 0 is also configured for ENM Type TO
CSCvi70138	Adptive Clock Rec and master CEM is chosen automatically on the CEM circuit in IMA8D
CSCvi85693	Mac Flap Syslog Notification not working after reload
CSCvj43887	Type TO is not working for different payload sizes
CSCvd99581	RSP3-400: In polaris Fan speeds are not set properly according to the temperature
CSCvi21308	RSP3_400 : Tx bias values are high on CPAK-100G and QSFP-40G SFP's
CSCvg92065	PTP session stuck in HOLDOVER in RSP2 Timing WRT - 1588_Transparent <Vz>
CSCvi71909	G.8265.1- T3 packets getting stopped while adding and deleting clock source multiple times.

Caveat ID Number	Description
CSCvj57301	[VF-PT] Slave not locking on a specific port (IMA8T Gi0/5/0)
CSCuy78963	FNF CLIs are visible for templates other than netflow-video in Striker

Resolved Caveats – Cisco IOS XE Everest 16.6.4

Caveat ID Number	Description
CSCuy84775	Slow response when typing in CLI on telnet session
CSCvb96943	Offset from master jumps to Huge value with SPAN
CSCve53492	IOT: For Serial(with RS232) interface IfType comes as other instead of serial/RS232
CSCvg70409	IOT: For Serial IM, flowcontrol is not applicable
CSCvh32219	Require Environmental Syslog message during Recovery of temperature and voltage Threshold Violation
CSCvi40742	Configuration change on E&M interface results in xconnect failure
CSCvi53346	RSP3 : BFD packets not sent out towards 9K after timer change and link flap
CSCvi72770	Unpredictable asymmetry across the port on C37.94 IM
CSCvi79409	ENM flaps/hangs on configuring CEM interface
CSCvj05472	Running line rate traffic on an internal loopback impacts BFD session
CSCvj10722	CEM Pseudo wire flap on SSO
CSCvj22030	ACR fails with -/+ 50 ppm tolerance
CSCvj61645	Incorrect Tx/Rx optical power thresholds for QSFP-40G-LR4
CSCvj43887	Type TO is not working for different payload sizes
CSCve43412	RSP3: CFM stats are not working on latest polaris images
CSCvi79552	HSRP and VRRP didnt converge with Multi Active portchannel Template
CSCvj13676	ENM IM : remove signal command from Type TO mode
CSCvi85693	Mac Flap Syslog Notification not working after reload
CSCvi70138	Adptive Clock Rec and master CEM is chosen automatically on the CEM circuit in IMA8D

Open Caveats – Cisco IOS XE Everest 16.6.3

Caveat ID Number	Description
CSCuz24819	Crash seen when WAN-PHY mode is enabled in RSP3
CSCvd38391	Standby Router: uea_mgr crashed @ ml2vpn_provision_pw_and_ac
CSCvd44667	RSP3: PREFIX Object Errored Objects on Local Core Flaps and in Parallel on Other Routers in the Core
CSCvd50734	RSP3-200:Router Crash while trying to delete label uea_oce_base_delete uea_mpls_label_delete_async
CSCvd77735	RSP3 - Small loss (6-10ms) observed for VPLS traffic when BGP backup peer is powered down
CSCve10095	Traffic is getting dropped in both direction due to hw programming went for toss
CSCve72906	RSP3:ECMP LB seen when flags field is changed in ip header with l4 header in 4 label scenario
CSCvf08656	RSP3 : Traffic failure for few Labelled BGP prefixes (BGP label imposed is incorrect)
CSCvf45267	RSP3 - Loadbalance map not getting deleted (IM OIR)
CSCvg28351	VPLS with Segment Routing not flowing traffic.

Resolved Caveats – Cisco IOS XE Everest 16.6.3

Caveat ID Number	Description
CSCvc94414	RSP3: Incorrect traffic rate recieved with specific values of CIR/PIR in HQOS policy
CSCve37398	RSP3-L2VPN: Load balancing is happening based on wrong fields in P node when CW is enabled
CSCve53479	LOTR OCx: SNCP - CEM-PG controller is DOWN after PG shut/no shut
CSCve55240	LOTR OCx: SNCP - PG CEM group is not attached to physical leg for 2nd cem-group on same port
CSCve75491	TE auto-bw: Incorrect bandwidth requested on soaking with traffic
CSCve87759	RSP3: Link flaps on configuring G8275.1
CSCvf03157	RSP3:PC stays in suspended state on IM OIR
CSCvf72154	RSP3 - PIM neighborship down on BDI interface due to packets ASIC loop
CSCvf72165	RSP3 - Router crash after "debug platform condition" command is applied

Caveat ID Number	Description
CSCvf82589	MPLSoRPW: Traceroute not working over Routed PW interface
CSCvg01577	LineStatusChange notification with not proper for clear event and problem event
CSCvh06657	spa_entity_sensor_xcvr_get_data during SFP/IM OIR
CSCvh08220	RSP3: Crash in IOSD chasfs task on Defaulting and Removing IMA-1X
CSCvh10730	BFD stuck at init state for Sessin ID 1023 alone on RSP3C after link flap
CSCvh51026	Router unresponsive and hangs during boot-up while loading router with package image file
CSCvh67319	Router unresponsive during bootup with the packages.conf file

Open Caveats – Cisco IOS XE Everest 16.6.2

Caveat ID Number	Description
CSCuz24819	Crash seen when WAN-PHY mode is enabled in RSP3
CSCvb96943	Offset from master jumps to Huge value with SPAN
CSCvb99102	MH BFD session flaps on shutting interface of no relevance to BFD session.
CSCvc38475	Serdes not locking with ISSU and reload
CSCvd38391	Standby Router: uea_mgr crashed @ ml2vpn_provision_pw_and_ac
CSCvd44667	RSP3: PREFIX Object Errored Objects on Local Core Flaps and in Parallel on Other Routers in the Core
CSCvd77735	RSP3 - Small loss (6-10ms) observed for VPLS traffic when BGP backup peer is powered down
CSCve05859	Exxx EIN: G.8275.1 testing: Clock loop forming between synce and ptp
CSCve10095	Traffic is getting dropped in both direction due to hw programming went for toss
CSCve37398	RSP3-L2VPN: Load balancing is happening based on wrong fields in P node when CW is enabled.
CSCve53479	LOTR OCx: SNCP - CEM-PG controller is DOWN after PG shut / no shut
CSCve72906	RSP3:ECMP LB seen when flags field is changed in ip header with l4 header in 4 label scenario
CSCve75491	TE auto-bw: Incorrect bandwidth requested on soaking with traffic
CSCve86912	[Counter]: Giant/Runt/Pause Frame counters issue.

Caveat ID Number	Description
CSCve87759	RSP3: Link flaps on configuring G8275.1
CSCvf03157	RSP3:PC stays in suspended state on IM OIR
CSCvf08656	RSP3 : Traffic failure for few Labelled BGP prefixes (BGP label imposed is incorrect)
CSCvf17498	100BASE EX showing wrong PID in all UEA platforms
CSCvf45267	RSP3 - Loadbalance map not getting deleted (IM OIR)
CSCvf72154	RSP3 - PIM neighborship down on BDI interface due to packets ASIC loop.
CSCvf72165	RSP3 - Router crash after "debug platform condition" command is applied.
CSCvf76091	FP fails to bootup with mac security configurations
CSCvf79693	RSP3: BGP support over Router PW
CSCvf82663	RSP3C crashed at dl_callback
CSCvg01577	LineStatusChange notification with not proper for clear event and problem event
CSCvg08224	G8265.1: PTP flaps between HOLDOVER and LOCKED with 64/64 packet rate and HOTSTANDBY
CSCvg22098	Dev_pluggable inconsistent console log seen in THS
CSCvg30892	License: observing ptp command failure error as part of moving from CSL to SL
CSCvg31244	RSP3C corrupts MGCP transaction ID
CSCvg36086	100G driver switchover failure on forced SSO crash scenario causing serdes lock/ping failures
CSCvg36641	Dying gasp snmp trap not seen
CSCve64341	Mid Point LSP creation failure after reload with latest polaris Image
CSCvc59505	Member link of Port channel gets removed on doing a SSO on the peer end

Resolved Caveats – Cisco IOS XE Everest 16.6.2

Caveat ID Number	Description
CSCvc29551	1x100G port not coming up on few reloads
CSCvd97704	RSP3-400:In polaris Fan speed is set to 100% at -40C
CSCvd89421	RMEP failure due to CFM HW table corruption
CSCve10269	RSP3 unable to route(drops) unicast dhcp packets with giaddr field as 0.0.0.0

Caveat ID Number	Description
CSCve12246	RSP3 which is locked to GNSS VP is not giving better accuracy
CSCve15834	BGP PIC-E: Double dip traffic loss on recovering primary ABR for CEM And EOMPLS VC
CSCve42430	[SH] Invalid MC_TYPE in LIF update
CSCve43278	MVPN-GRE : Free the nmdt when core prefix goes away
CSCve45078	RSP3-CFM: MA number is not working with ID NULL for offloaded sessions
CSCve45870	Observing obj download with CFM configs
CSCve56992	Traffic loss seen with L2 Xconnect on 10G
CSCve61214	G8275.1: Master disqualified even though packets are flowign fine
CSCve70271	OCx:SDH:MSP:VC1x:On create default txpsl set as 0x02 in ios it set as 0x01
CSCve73883	RSP3 Ping is not successful after IP moved to different EFP
CSCve77231	RSP3:traffic failure on VRRP session and traces @ vrrp_comms_process_pak
CSCve81377	RSP3:CFMoVPLS scale:VPLS PD entry missing for few neighbors upon Soak
CSCve83541	RSP3: IOSd Crash on Deleting PTP Loopbacks during ISSU SOAK
CSCve87122	Frequency Traceable Flag is set to false on downstream routers when 1pps is made down on TGM
CSCve87327	Tx SS bit should be set to 2 for SDH mode
CSCve90377	Active and standby RSP hang just after booting because of thermal shutdown
CSCve92481	After PTP reconfiguration, slave 903 stuck in freq-lock state.
CSCve93405	RSP3 : RPW ping failure on VPLS PWs with Auto Discovery enabled
CSCvf05587	RSP3 : 2 KBP entries created for ingress vpnv4 label - Label swap case
CSCvf06625	Programming mismatch between Active & STBY after STBY reload for L3VPN prefix
CSCvf19017	RSP3_GNSS: ToD down after reload on G8275.1T-BC
CSCvf21127	2 ACs in a VFI, when one interface is shutdown, traffic is not flood to other interface
CSCvf21487	L2VPN attachment circuit is going down after SSO on the line card A900-IMA8S1Z
CSCvf33429	APS UNI ADM mode: APS reverts back on clearing the shut from inactive controller
CSCvf33518	On SSO L3VPN prefix is programmed with LFA backup interface as primary interface in PD.

Caveat ID Number	Description
CSCvf38857	RSP3 PTP BC is not locking to the Master via intermediate PTP aware nodes with tagging enabled.
CSCvf40845	Alarms are not generating values at Path level for concatenated STS(12C and 48C)
CSCvf46100	Tracebacks on configuring interface PoCh
CSCvf50635	Dynamic stream are getting deleted on router with G8275.2 profile <POLARIS> Timing THS
CSCvf57056	T3 framed satop reporting parity errors on L-bit instead of AIS
CSCvf60263	APS-ACR Scale Issue:For 8K Scale Config, PW-GROUP not bound on Arrive CEM FPGA during Copy Config
CSCvf64035	Few BFD v4 sessions staying in down/init after ip address removal/addition
CSCvf66464	ISSU failing between 16.5.X/16.6.Y CCO builds
CSCvf68040	Labels not programmed on standby RSP for T1 circuits for denether IM
CSCvf76449	Observing Object Download Failure on Shut/NO shut with CFM Config
CSCvf90854	Configured priority2 under ptp clock is not sent downstream when T- BC selected VP
CSCvf91208	Unable to retrieve stream with G8275.2 profile Timing THS
CSCve64336	RSP1-Continous ESMC tracebacks observed after IMA8T OIR followed by SSO
CSCve98223	Two PW-Group switchover notifications are triggered from PI to PD for a single event
CSCvf05616	Traffic drop, on reconfiguring l2vpn sessions after SSO on peer
CSCvf33489	ISIS FRR : FRR ReOpt Issue, FRR state pointing to Label backup even with primary link up

Open Caveats – Cisco IOS XE Everest 16.6.1

Caveat ID Number	Description
CSCve52155	BFD Session Between 2 RSP3s Down on Reloading 1 RSP3
CSCvd11229	Some of BFD sessions are flapped after changing the BFD timer
CSCvb01668	Convergence time is taking more than 50 ms (7 secs) after SS0 with IPV6
CSCvb99102	MH BFD session flaps on shutting interface of no relevance to BFD session
CSCvf06625	Programming mismatch between Active and STBY after STBY reload for L3VPN prefix

Caveat ID Number	Description
CSCve73883	RSP3 ping is not successful after IP moved to different EFP
CSCvd36139	40G interface down on changing mode from LAN to OTN
CSCve63289	Micro flaps are seen in interface when an xconnect is made down
CSCve65904	10 Gig port going down after few reloads
CSCvf02136	VLAN untagged traffic wrongly punted to CPU when service instance is deleted
CSCve15834	BGP PIC-E: Double dip traffic loss on recovering primary ABR for CEM and EOMPLS VC
CSCvd73294	L2VPN : Traffic drop on recovery of PIC- primary peer
CSCve63937	RSP2 ODN: pending and error objects pile up on stby RSP2 with ODN auto-tunnel
CSCvf05386	RSP2: Standby RP Get AToM Forwarding Context Cylon_Mgr Crash on Core Gigs Flap SOAK on RRs
CSCvd34677	RSP3 : 30-40sec traffic loss for MPLS TE tunnels on performing SSO @ TE midpoint
CSCve93405	RSP3 : RPW ping failure on VPLS PW's with Auto Discovery enabled
CSCve45288	RSP3-L2VPN: ECMP LB is not working based on PE node in 3 label scenario when PIC core disabled
CSCve37398	RSP3-L2VPN: Load balancing is happening based on wrong fields in P node when CW is enabled.
CSCve72876	RSP3: LB is not working on P node based on Source/destination ipv6 addresses in 3 label scenario
CSCvd81439	RSP3: VPLS HW stale entries are present although PW is down
CSCve72906	RSP3: ECMP LB seen when flags field is changed in ip header with l4 header in 4 label scenario
CSCva63048	RSP3: Traffic Drop,IP FRR Primary is program'd with wrong Out going intf
CSCve81377	RSP3: VPLS prgrm'g missing for some neighbors after reload
CSCvd38391	Standby Router: uea_mgr crashed @ ml2vpn_provision_pw_and_ac
CSCvd13823	Storm control - L3 Mcast Traffic :: Not all packets are dropped
CSCve05859	Exxx EIN: G.8275.1 testing: Clock loop forming between synce and ptp
CSCve49550	IOX: OOS issue seen with 100Mbps sfp inserted on a SFP combo IM
CSCve43404	PTP Clock Creation Fails for Specific Sequence of Triggers
CSCve39547	PTP PI counters were not shown properly.

Caveat ID Number	Description
CSCve58737	RSP2 : PTP hybrid BC failed as config appiled before netsync locked REF alarm cleared
CSCve83541	RSP3: IOSd Crash on Deleting PTP Loopbacks during ISSU SOAK
CSCve87759	RSP3: Link flaps on configuring G8275.1
CSCve12246	RSP3: RSP3 which is locked to GNSS VP is not giving better accuracy
CSCve16996	Ingress classification misbehaves after removing set qos-group statement from a class.
CSCvc94414	RSP3: Incorrect traffic rate recieved with specific values of CIR/PIR in HQOS policy
CSCva23389	RSP3: Upon double SSO, LDP neighborship is not coming up on POCH (act-stby)
CSCvb22120	cCocks state is freeruning after SSO
CSCve20630	RSP2 TDM THS : Core generate during reload : unable to initialize the bipc manager
CSCvc50710	RSP2: Standby RP Crash in HA-IDB-SYNC Process on SOAK of Delete Reconfig CEM and ACR
CSCve01357	DCC: DCC check not available in 1+1 APS
CSCvc34890	OCx APS-ACR : RTP is not enabled on FPGA with config copy
CSCve53479	LOTR OCx: SNCP - CEM-PG controller is DOWN after PG shut / no shut
CSCve55240	LOTR OCx: SNCP - PG cem group is not attached to physical leg for 2nd cem-group on same port
CSCvf03668	Mid-chain object stuck to pending state on TE tunnel interfaces and core Gig flap SOAK

Resolved Caveats – Cisco IOS XE Everest 16.6.1

Caveat ID Number	Description
CSCvc25416	UMMT Automated Regression :: Active RSP3-200 crashes after interface shutdown between AG1 and AG2
CSCvd12231	Unicast ARP resolution fails in VRRP master state
CSCve22853	Improper SIGDET register setting could cause traffic failure and link down conditions
CSCvc44999	Pending objects seen Tx Channel and Interface after disabled IM and FP stuck init
CSCva16169	DS1:Traffic not resuming after Ctrl shut then SSO and No shut
CSCvc27318	DS3 Path/Line Level PMON issues for DS3 Port

Caveat ID Number	Description
CSCvc54203	Post ISSU : DCR remains in UNKNOWN state
CSCuz89518	T3 AIS: Implementing structure aware DS3 SATOP
CSCvb45433	SLOS reported when we shutdown ais-shut enabled in SDH and SONET mode
CSCvc40326	HSPW : pw programming going for toss and traffic gets dropped after int flap
CSCva24546	MPLS TE : 1-2 ms traffic loss when backup interface state is toggled
CSCvd22428	HSPW traffic failure after SSO/IM OIR (FEC programmed as 0)
CSCvd96938	RSP3 crashes @ tbm_lookup, uea_cef_get_leaf
CSCvd12082	RSP3-mlacp: %FMFP-3-OBJ_DWNLD_TO_DP_FAILED: SIP0: fman_fp_image: atom_xconnect xid 0x408110
CSCvd57077	Traffic Fails on FRR backup path while primary is active.
CSCvb67543	uea mgr crash @"uea_mpls_atom" upon flapping core A/A Poch interface of peer box
CSCvd55076	UMMT: RLFA FRR - High convergence on shutting the core link
CSCvb55216	VPLS: LDP flap after SSO leads to 100% traffic loss
CSCvc53687	Crash @cmm_link_mldp_extranet_metchain
CSCvc39154	[inband] RCY in met chain on bud
CSCvd28433	By removing and adding auto neg at Cu interfaces leads to PTP malfunction
CSCvd12047	G8275.1: syncE drift when PTP is removed from G8275.1 TBC.
CSCvd69590	G8275.1_RSP3: accuracy is ~500nsec when it uses to 10GE IM on first time boot
CSCvc53794	PTP over MPLS support
CSCvd00614	BFD is flapping when removing PTP config
CSCve14324	Port level shaper is counting packets twice
CSCvd34788	Might crash with reason bulk sync failure
CSCvc95602	SDH counter errors
CSCvd38689	Memory leak found @ dsx3_init_t1, cx3_init_e1
CSCvc67481	cpwCTDMPerfCurrentTable not dumping with ACR configuration
CSCvc74964	IPC channel hogging due to alarm flooding on cable looping for APS ports
CSCvb53371	License OIR issue: failed port is coming UP and accessible
CSCvc79065	UPSR - Error message seen when PG is unconfigured and reconfigured again

Caveat ID Number	Description
CSCvd17937	UPSR - PUNEQ seen on UPSR intf of PE2(remote) upon unconfig/config PG e2e after SSO of PE1
CSCvd46410	OCx: ACR/UPSR - Virtual Controller Shut/No-Shut not working due to License rejection
CSCvb78285	OCx: Iomd crash on Active RSP post SSO of admin down IM
CSCvb55300	Port-lic: Port licensing cmds Not synced to HA when IM is shut
CSCuy11711	TIM-S,TIM-P, TIM-V, B1, B2, B3 fields are not showing on show controller output
CSCvc21158	Traffic is flapping on channel when W port is deleted from ACR group