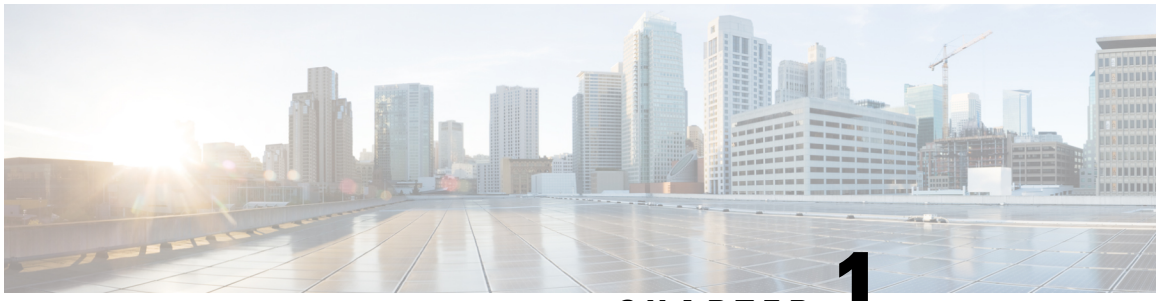
Release Notes for Cisco NCS 4201 and Cisco NCS 4202 Series, Cisco IOS XE Bengaluru 17.6.x

First Published: 2021-07-29

Last Modified: 2024-04-05

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 4201 and Cisco NCS 4202 beginning with Cisco IOS XE Release 3.18SP.

Documentation Updates

IPv4 Unicast Generic Routing Encapsulation Tunnel Overview is now available in the IP Routing: GRE Configuration Guide, Cisco IOS XE 17 (Cisco NCS 4200 Series). The chapter is moved from the MPLS: Layer 3 VPNs Configuration Guide.

Cisco NCS 4201 and Cisco NCS 4202 Overview

The Cisco NCS 4201 and NCS 4202 Network Convergence Systems are full-featured, compact one-RU high converged access platforms designed for the cost-effective delivery of TDM to IP or MPLS migration services.

These temperature-hardened, high-throughput, small-form-factor, low-power-consumption systems are optimized for circuit emulation (CEM) and business applications. NCS 4201 and NCS 4202 chassis allow service providers to deliver dense scale in a compact form factor and unmatched CEM and Carrier Ethernet (CE) capabilities. They also provide a comprehensive and scalable feature set, supporting both Layer 2 VPN (L2VPN) and Layer 3 VPN (L3VPN) services in a compact package .

For more information on the Cisco NCS 4201 Chassis, see the Cisco NCS 4201 Hardware Installation Guide.

For more information on the Cisco NCS 4202 Chassis, see the Cisco NCS 4202 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

NCS4201 is a fixed router and does not have any field replaceable units.

The following table lists the hardware supported for Cisco NCS 4202 chassis.

Chassis	Supported Interface Modules	Part Numbers
NCS 4202	8 port T1/E1 CEM Interface Module	NCS4200-8E1T1-CE
	1 port OC-48/STM-16 or 4 port OC-12/OC-3 / STM-1/STM-4 + 12 ports T1/E1 + 4 ports T3/E3	NCS4200-3GMS
	8-Port 1GE RJ45 and 1-Port 10GE SFP+ module	NCS4200-1T8LR-PS

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)

ROMMON Version

- NCS4201—15.6(48r)S
- NCS4202—15.6(46r)S

Upgrading to a New Software Release

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

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

Upgrading the FPD Firmware

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

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

Bundled FPGA Versions

The following are HoFPGA versions bundled in the IOS:

- NCS4201—0X00030015
- NCS4202
  - BFD—0X0003001B
  - Netflow—0X00020008

The following is the CEM FPGA version:

- NCS4202—0x10050071

The following are HoFPGA versions bundled in the IOS for 17.6.1 release:

- NCS4201—0X0004001b
- NCS4202
  - BFD—0X0003001e
  - Netflow—0X00020008

The following is the CEM FPGA version:

- NCS4202—NA

The following are HoFPGA versions bundled in the IOS for 17.6.2 release:

- NCS4201—0X0004001b
- NCS4202
  - BFD—0X0003001e

- Netflow—0X00020008

The following is the CEM FPGA version:

- NCS4202—0x10020076

The following are HoFPGA versions bundled in the IOS for 17.6.3 release:

- NCS4201—0X0004001b
- NCS4202
  - BFD—0X0003001e
  - Netflow—0X00020008

The following is the CEM FPGA version:

- NCS4202—0x10020076

The following are HoFPGA versions bundled in the IOS for 17.6.4 release:

- NCS4201—0X0004001b
- NCS4202
  - BFD—0X0003001e
  - Netflow—0X00020008

The following is the CEM FPGA version:

- NCS4202—0x10020076

The following are HoFPGA versions bundled in the IOS for 17.6.5 release:

- NCS4201—0X0004001b
- NCS4202
  - BFD—0X0003001e
  - Netflow—0X00020008

The following is the CEM FPGA version:

- NCS4202—0x10020076

The following are HoFPGA versions bundled in the IOS for 17.6.6a release:

- NCS4201—0X0004001b
- NCS4202
  - BFD—0X0003001e
  - Netflow—0X00020008

The following is the CEM FPGA version:

- NCS4202—0x10020076

The following are HoFPGA versions bundled in the IOS for 17.6.7 release:

- NCS4201—0X0004001b
- NCS4202
  - BFD—0X0003001e
  - Netflow—0X00020008

The following is the CEM FPGA version:

- NCS4202—0x10020076

Limitations and Restrictions on the Cisco NCS 4201 and Cisco NCS 4202 Series

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.

- The **default** *command-name*command is used to default the parameters under that interface. However, when speed is configured on the interface, the following error is displayed:

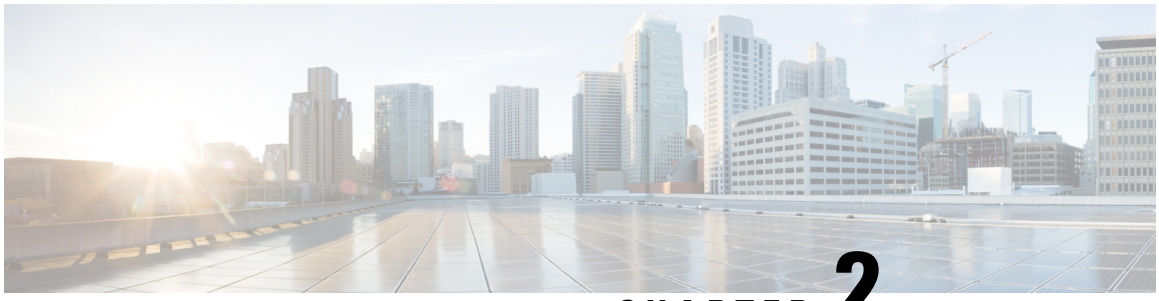
```
Speed is configured. Remove speed configuration before enabling auto-negotiation
```

- For VCoP, only SFP-T3F-SATOP-I is supported.
- Virtual services should be deactivated and uninstalled before performing replace operations.
- IPSec is not supported on the Cisco NCS 4201 and Cisco NCS 4202 routers.
- On Cisco NCS 4202 Series, the following restrictions apply for IPSec:
  - Interface naming is from right to left. For more information, see the Cisco NCS 4200 Series Software Configuration Guide, Cisco IOS XE 17.

  - Packet size greater than 1460 is not supported over IPsec Tunnel.
  - Minimal traffic drop might be seen for a moment when higher rate traffic is sent through the IPsec tunnels for the first time.
  - IPsec is only supported for TCP and UDP and is not supported for SCTP.

- One Ternary Content-Addressable Memory (TCAM) entry is utilized for Segment Routing Performance Measurement. This is required for the hardware timestamping to function.
- Before installing the Cisco IOS XE Amsterdam 17.3.1, you *must* upgrade the ROMMON to version 15_6_43r_s or higher to avoid bootup failure. This is applicable to Cisco NCS 4202 routers. This workaround is not applicable to devices installed with ROMMON version 15.6(9r)S.
- 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. However, the router can be reloaded during the next planned reload to complete the secondary ROMMON upgrade.
- For Cisco IOS XE Amsterdam 17.3.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.
- Some router models are not fully compliant with all IETF guidelines as exemplified by running the pyang tool with the lintflag. 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 is provided, **check-models.sh**, which runs pyang with lint validation enabled, but ignoring certain errors. This allows the developer to determine what issues may be present.

  As part of the model validation for this Cisco IOS XE Amsterdam 17.3.1 release, "LEAFREF_IDENTIFIER_NOT_FOUND" and "STRICT_XPATH_FUNCTIONS" error types are ignored.
- Starting with Cisco IOS XE Bengaluru Release 17.5.1, if IPv6 Global IP is configured as the BFD peer, and if the interface goes down, a VRRP flap may occur. This may occur because, VRRP works on the basis of Link-local IP and not global IP. As a result, VRRP flaps on the previously backed up device and prints a DAD message.



CHAPTER 2

What's New for Cisco IOS XE Bengaluru 17.6.x

This chapter describes the new hardware and software features that are supported on the Cisco NCS 4201 and Cisco NCS 4202 Series routers.

For information on features supported for each release, see Feature Compatibility Matrix.

What's New in Hardware for Cisco IOS XE Bengaluru 17.6.7

There are no new hardware features in this release.

What's New in Software for Cisco IOS XE Bengaluru 17.6.7

There are no new software features in this release.

What's New in Hardware for Cisco IOS XE Bengaluru 17.6.6a

There are no new hardware features in this release.

What's New in Software for Cisco IOS XE Bengaluru 17.6.6a

There are no new features in this release. This release provides a fix for CSCwh87343: Cisco IOS XE Software Web UI Privilege Escalation Vulnerability. For more information, see cisco-sa-iosxe-webui-privesc-j22SaA4z.

What's New in Hardware for Cisco IOS XE Bengaluru 17.6.6

There are no new hardware features in this release.

What's New in Software for Cisco IOS XE Bengaluru 17.6.6

There are no new software features in this release.

What's New in Hardware for Cisco IOS XE Bengaluru 17.6.5

There are no new hardware features in this release.

What's New in Software for Cisco IOS XE Bengaluru 17.6.5

There are no new software features in this release.

What's New in Hardware for Cisco IOS XE Bengaluru 17.6.4

There are no new hardware features in this release.

What's New in Software for Cisco IOS XE Bengaluru 17.6.4

There are no new software features in this release.

What's New in Hardware for Cisco IOS XE Bengaluru 17.6.3

There are no new hardware features in this release.

What's New in Software for Cisco IOS XE Bengaluru 17.6.3

There are no new software features in this release.

What's New in Hardware for Cisco IOS XE Bengaluru 17.6.2

There are no new hardware features in this release.

What's New in Software for Cisco IOS XE Bengaluru 17.6.2

There are no new software features in this release.

What's New in Hardware for Cisco IOS XE Bengaluru 17.6.1

There are no new hardware features in this release.

What's New in Software for Cisco IOS XE Bengaluru 17.6.1

Feature	Description
First Hop Redundancy Protocols	
Support for BFD, sub-second fast hello for VRRPv3 convergence and re-convergence	This feature supports VRRP failover such that the fault is detected by the VRRP-BFD client within the configured value – when the connection to the remote interface IP address fails.
High Availability	
Upgrading Power Supply Monitoring Firmware	This feature allows you to manually upgrade the firmware of the power supply monitoring device in a router. The firmware upgrade reduces unplanned hardware-related downtime caused by input voltage transients during a power outage.
IP Routing	
Establish GRE Tunnel over VRF Routes	This feature establishes GRE tunnels over Virtual Route Forward (VRF) routes.
MPLS Layer 2 VPNs	
Remote LFA for MLDP	Remote Loop-Free Alternate (RLFA) based Fast Reroute (FRR) improves LFA coverage. When used with Multicast Label Distribution Protocol (MLDP) for IPv4, there is no need for an extra protocol in the control plane.

Feature	Description
Network Management	
Ingress and Egress Flexible NetFlow	Flexible NetFlow allows you to monitor the traffic from access circuit on an L2VPN and L3VPN network. In addition to monitoring traffic in routed and ethernet service interfaces, you can now monitor traffic in VRF enabled L2 VFI (virtual forwarding interfaces) and cross-connect services.
Programmability	
YANG Model Support for **show mpls tr tunnel** Command	This feature enables you to verify the **show mpls traffic engineering tunnel** command to check the status from YANG models.
YANG Model Support for RSVP Commands	You can use the **interface BDI 10** and **ip rsvp bandwidth percent 4** commands to configure the RSVP bandwidth on a BDI interface from YANG. You can configure, modify, and verify different bandwidth values using these commands.
YANG Model Support for IPSLA Operating Model for Y1731	You can check the history interval statistics of delay operations like DMM, DMMv1 and 1DM, and loss operations like LMM and SLM using the NETCONF-YANG command to enable YANG data collection.
YANG Model Support for QoS Overhead Accounting	QoS Overhead Accounting feature enables a particular port to consider a particular number of bits that are removed from the packet when the egress packet is re-edited. The traffic scheduler allows more bits than the configured rate at the port, without exceeding the number of bytes that is configured on a port. YANG QOS Overhead accounting configuration model supports the configuration on the router accounting on router from YANG/NETCONF protocol.
YANG Model Support for Alarm Profile Configurations	This feature enables you to configure the alarm profile on the interface through native YANG models that run on Cisco IOS XE.
YANG Model Support for Shared Risk Link Groups (SRLG) Group Identification (GID) Configurations	Shared Risk Link Groups (SRLG) Group Identification (GID) configurations can be enabled on YANG using the **srlg gid** command. Multiple groups and interfaces can be enabled on the interface mode.
Segment Routing	
EVPN-IRB DHCP v4 and v6 Relay over Segment Routing	This feature introduces a specialised implementation of DHCP packets to support DHCPv4 and DHCPv6 in an EVPN Fabric with Distributed Anycast Gateways (DAGs) on the same Virtual Routing and Forwarding (VRF). It also avoids DHCP discovery packet floods across the fabric. The flooding suppression feature is also enhanced to intercept multicast or broadcast DHCP packets when DHCP relay is configured on the DAG to perform the required action and localize the scope of the service.

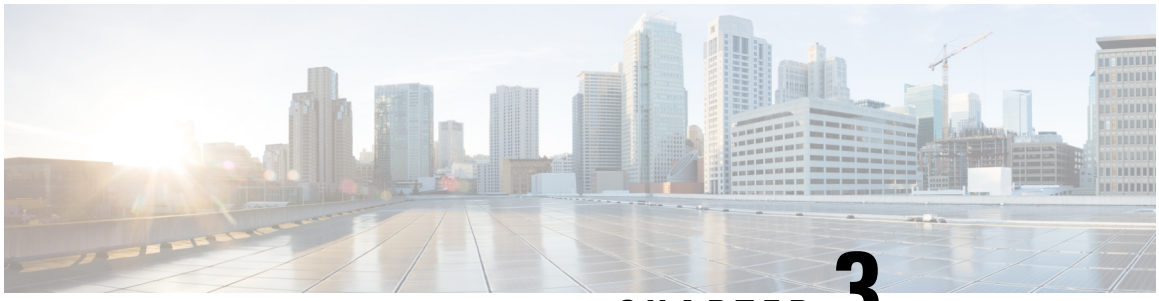
Feature	Description
IS-IS Flexible Algorithm Include Affinity Support	This feature supports "include-any" and "include-all" affinities in IS-IS. Prior to Cisco IOS XE Bengaluru 17.6.1 release, only Flexible Algorithm affinity "exclude-any" was supported.
OSPF Flexible Algorithm (Ph2): Topology-Independent Loop-Free Alternate (TI-LFA) path	This feature allows you to configure the Loop-Free Alternate (LFA) and TI-LFA backup or repair paths for a Flexible Algorithm. The backup path is computed based on the constraints and metrics of the primary path. Prior to Cisco IOS XE Bengaluru 17.6.1, OSPF Flexible Algorithm supported only the primary path.
SR-PCE: Enabling SR PM Delay or Liveness for PCE-Initiated Policies	This feature enables the Path Computation Element (PCE) that can provision a Segment Routing Traffic Engineering (SR-TE) policy to mitigate link congestion. Prior to this release, you could only enable PM link and delay measurement using CLI-based policies. Starting with this release, you can also use PCE to enable PM link and delay measurement.
Stitching of Subnet Route from EVPN to L3VPN	This feature introduces the collpased spine and border leaf node in the network topology of single homing DAGs with symmetric IRB, inter-subnet layer 3 traffic within fabric and inter-subnet layer 3 stitching through layer 3 border gateway. The hosts participating in fabric IRB are directly attached with the collapsed spine and border leaf node.
System Management	
Cisco Secure Development Lifecycle—Factory Reset	This feature removes all the customer-specific data that stored on the device since the time of its shipping. Data erased includes configurations, log files, boot variables, core files, and credentials like FIPS-related keys. Cisco Secure Development Lifecycle (CSDL) is a repeatable and measurable proces designed to increase Cisco product resiliency and trustworthiness. The following new commands are introduced: • **factory-reset all** • **factory-reset keep-licensing-info** • **factory-reset all secure 3-pass DoD 5220.22-M** For information on the commands, Cisco IOS Configuration Fundamentals Command Reference.
Time Division Multiplexing	

Feature	Description
Support for E1 framed Smart TPoP pluggable	You can configure the following features for E1 in framed and unframed modes: • Loopback, framing, line code encoding, cable length, and jitter buffer • BERT • Performance monitoring counters and alarms • Alarm profiling • Clock recovery modes These features that are configured on framed and unframed E1 interfaces help you to monitor the traffic and troubleshoot errors or failures efficiently.
Support for T1 framed Smart TPoP pluggable	You can configure the following features for T1 in framed and unframed modes: • Loopback, framing, line code encoding, cable length, and jitter buffer • BERT • Performance monitoring counters and alarms • Alarm profiling • Clock recovery modes These features that are configured on framed and unframed T1 interfaces help you to monitor the traffic and troubleshoot errors or failures efficiently.

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/1761.

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 17.6.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 17.6.7

Identifier	Headline
CSCwi75499	Lost CEM circuit configuration after reboot

Open Caveats – Cisco IOS XE Bengaluru 17.6.7

There are no open caveats in this release.

Resolved Caveats – Cisco IOS XE Bengaluru 17.6.6a

Identifier	Headline
CSCwh87343	Cisco IOS XE Software Web UI Privilege Escalation Vulnerability

Open Caveats – Cisco IOS XE Bengaluru 17.6.6a

There are no open caveats in this release.

Resolved Caveats – Cisco IOS XE Bengaluru 17.6.6

Identifier	Headline
CSCwd78618	IMASER14A/S does not boot on router.
CSCwe38959	The RS232 ASYNC pseudowire service with full scale seeing packet and byte drops intermittently.
CSCwf40953	DS3_ADMIN_DOWN gets cleared after IM OIR.
CSCwf86864	CEM traffic flow is dropped in one direction due to DEI bit set from router.
CSCwf49426	PAIS alarm get reported after IM OIR.
CSCwe54549	SFP not detected due to checksum error.
CSCwe27336	Error logs during reload in ASR920-24SZ-M variant.
CSCwh02460	With x.21 configured observing underruns in cem counters.

Identifier	Headline
CSCvy81362	Controllers are down due to LP-LOP alarm After CE reboots.
CSCwf07736	CEM interface counters momentarily report error when x21 xconnect is cleared and re-established.
CSCwd46121	Time stamp issue on Transparent clock for 1G PORTS.
CSCwd67723	In IMA32D/IMA8D card, sometimes change in E1 controller config(after ctrlr flap)results in IM reboot.
CSCwf71463	With traffic ON, when speed lowered on ASYNC port, SYNC port CEM traffic gets impacted.
CSCwe98227	The **show version** does not display details of T1/E1 interfaces for 8D and 32D IMs.

Open Caveats – Cisco IOS XE Bengaluru 17.6.6

Identifier	Headline
CSCwh12668	Standard loopback is not working when applied on both the ends on a back to back link.
CSCwa40025	IMA3G card high temperature due to dynamic fan algorithm.

Resolved Caveats – Cisco IOS XE Bengaluru 17.6.5

Identifier	Headline
CSCwc41135	Continuous assertion and clear of LAIS on protect channel causing IPC failure
CSCwc80493	APS - K2 byte not reflecting proper value during LRDI and LAIS conditions.
CSCwd04198	A900-IMASER14A/S: when configurations are pasted in a specific order, line config is missing
CSCwc41115	APS 1+1 Uni - Tx K2 to reflect Rx K1 channel number
CSCwc84627	ASR-920-12SZ-IM - EOMER IM goes continous reboot for a PCIE bus error
CSCwd48164	EVPN statd resource leak after protocol flaps
CSCwc93296	ASR-920-10SZ-PD /16.9.4/port Te0/0/10 went admin down after in successive reload
CSCvy09725	Software solution to detect the BAD PSU
CSCwc79322	Memory leak on ptpd_uea process

Identifier	Headline
CSCwd26357	rs485 with half-duplex configuration when reloaded, it gets into default full-duplex mode

Resolved Caveats – Cisco IOS XE Bengaluru 17.6.5 - Platform Independent

Identifier	Headline
CSCwd66936	UDP pseudowire stuck in Activating
CSCwc21402	Invalid BGP update when add-paths negotiated only for label (SAFI 4) and not unicast (SAFI1)
CSCwb91762	RSP3: MSPW VC down points to Error Local access circuit is not ready for label advertise
CSCwb77093	A BGP speaker may advertise a next-hop set to self when advertising an eBGP route to an iBGP peer.

Open Caveats – Cisco IOS XE Bengaluru 17.6.5

Identifier	Headline
CSCwd90840	Multicast data traffic is getting dropped over vpls
CSCwc77502	Unexpected reload due to MLDPv6
CSCwd67723	In IMA32D/IMA8D cards, any changes in the E1 interface configs (after interface flapping) results in IM crash and reboot
CSCwd16666	The Bit Error Rate Testing (BERT) pattern does not sync while configuring network loop in 3GMS OC-3 ports

Open Caveats – Cisco IOS XE Bengaluru 17.6.5 - Platform Independent

Identifier	Headline
CSCwc55520	Traceback and IDB leak noticed when a RSP3 setup performs a switchover
CSCvy94083	NCS4216:Running configuration syn to the NETCONF running data store takingmor time .

Identifier	Headline
CSCvy87800	Remote LInk Failure notification is disabled when configuring through YANG
CSCwb43369	ASR920::Traceback seen when default made on all core intfs.

Resolved Caveats – Cisco IOS XE Bengaluru 17.6.4

Identifier	Headline
CSCwb01284	ASR 900 Series PTP Sync degraded on Tester after primary PTP source failover to secondary

Resolved Caveats – Cisco IOS XE Bengaluru 17.6.4 - Platform Independent

There are no resolved caveats in this release.

Open Caveats – Cisco IOS XE Bengaluru 17.6.4

Identifier	Headline
CSCwc60168	Traffic drop in primary/active path when changes are made on backup path

Open Caveats – Cisco IOS XE Bengaluru 17.6.4 - Platform Independent

Identifier	Headline
CSCwa30653	MVPN Profile 14 : Data MDT traffic not flowing with 2 paths when OSPF cost configured on 1 path

Resolved Caveats – Cisco IOS XE Bengaluru 17.6.3

Identifier	Headline
CSCvz42622	TPOP T1 SATOP : Cable length range needs to be changed to be consistent with the IMA48D/IMA3G
CSCvy78284	ASR920 will crash when zeroised RSA key is regenerated

Identifier	Headline
CSCwa35351	Raw-socket config-event use all the iomem when L1 is down
CSCwa59045	Need to support few line level CLIs with "no" even without any cable attached.
CSCwa79398	rs232 service on port8 gives SLIP errors when databits is set on other ports
CSCwa09302	iMSG serial interfaces bitrate/sec data is displayed incorrectly in show command output
CSCwa04795	Interfaces are showing up in SNMP polling while associated Hardware Does not Exists on System
CSCvy92074	MTU programming for mpls l2 vc may fail after interface flaps
CSCvz27117	linux_iosd_image crash seen during router reload
CSCwa41638	ASR920 MAC Table and L2VPN EVPN Table out of sync

Resolved Caveats – Cisco IOS XE Bengaluru 17.6.3 - Platform Independent

Identifier	Headline
CSCwa37283	RSP failover on NCS4200 showing several seconds of outage for L2VPN services

Open Caveats – Cisco IOS XE Bengaluru 17.6.3

There are no open caveats for this release.

Open Caveats – Cisco IOS XE Bengaluru 17.6.3 - Platform Independent

Identifier	Headline
CSCwb04551	FRR not calculating backup route due to "primary_update_complete_pending:" flag set to 1
CSCwa30653	MVPN Profile 14 : Data MDT traffic not flowing with 2 paths when OSPF cost configured on 1 path
CSCwa36608	ICCP stuck on CONNECTING state after RSP SO on Active PoA

Resolved Caveats – Cisco IOS XE Bengaluru 17.6.2

Caveat ID Number	Description
CSCvy64788	LLC frames get looped back due to autonomic networking
CSCvy91436	Egress QoS classification issues are seen with Service instance 2 configuration on CE facing interfaces
CSCvz07477	DWDM SFPs threshold value set to 0.0 dbm for RX/TX and -0.0 C for temperature.
CSCvz26979	DHCP packets are not forwarded from client to server when DHCP snooping is enabled globally
CSCvz79672	HQoS on egress TenGig interface does not work properly

Resolved Caveats – Cisco IOS XE Bengaluru 17.6.2 - Platform Independent

Caveat ID Number	Description
CSCvz66346	New Bridge-Domain are not added dynamically to POCH when TEFP-encap from-bd is configured
CSCvz25471	NSO config push failure seen due to getconf on BD gives additional value mac learning

Open Caveats – Cisco IOS XE Bengaluru 17.6.2

Caveat ID Number	Description
CSCvy78284	Router crashes when zeroised RSA key is regenerated
CSCvz52848	Raw-socket config-event use all the iomem if connected device L1 signals are down

Resolved Caveats – Cisco IOS XE Bengaluru 17.6.1

Caveat ID Number	Description
CSCvs50029	Interface flaps and input errors seen with optics GLC-FE-100BX-D
CSCvu78738	T3 counter names to be as per GR-820 standard names
CSCvv21542	Command to change from dynamic to static FAN algorithm for the router

Caveat ID Number	Description
CSCvv42595	REP flapping is seen randomly and frequently due to port down
CSCvv47918	Block SATOP when controller is looped remotely (far end) for ACR/UPSR/CPG/STS1e
CSCvv55842	DEI bit on C-TAG is not being preserved for Double tag to Double tag svc even if there is no rewrite
CSCvv74638	RSP2-128: IMA1X frequent link down
CSCvv62123	FPGA TX tables are not programmed for microbfd session after router reload in 17.4.1 release
CSCvv73275	Applique type, syslog are misleading when a path configured with t3 is over-written with STSnC mode
CSCvv74342	VPLSoBKPW: MAC is not flushed or withdrawn in remote peer on VC swichover from active to standby
CSCvv99456	ACL entries with FRAGMENT keywords are not working on the router
CSCvw08879	EVPN-IRB: Complete traffic drop seen in one direction after intf flap on spine or leaf with XE-XR interop
CSCvw32263	Router is not going for shutdown when device booted without fan tray
CSCvw56612	LOTR : **show lic** command does not show port details
CSCvw64784	RSP2 CEM ACR: Not able to reuse same clock ID on another controller after you delete clock ID
CSCvw82333	Continuous PCI role logging to trace file
CSCvx41010	Failed to marshal xcvr_sync message: Bad address
CSCvr43362	NCS 4202: Fan speed control measures for overheating router

Open Caveats – Cisco IOS XE Bengaluru 17.6.1

Caveat ID Number	Description
CSCvy92074	MTU programming for MPLS Layer 2 VC may fail after interface flaps
CSCvz02352	Error objects are seen in mlist area
CSCvy74356	In T3 controller-CT3 E1 and CT3 mode the loopback local is not getting applied and the controller stays down

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