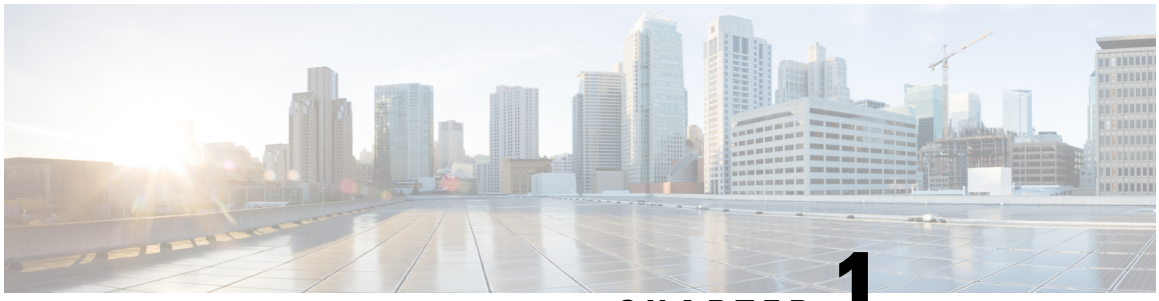
Release Notes for Cisco NCS 4201 and Cisco NCS 4202 Series, Cisco IOS XE Amsterdam 17.3.x

First Published: 2023-03-16

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

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).

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(43r)S
- NCS4202—15.6(43r)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 17.3.1 release:

- NCS4201—0X00030014
- NCS4202—0X0003001b

The following is the CEM FPGA version:

- NCS4202—0x10210074

The following are HoFPGA versions bundled in the IOS for 17.3.2 release:

- NCS4201—0X00030014
- NCS4202—0X0003001b

The following is the CEM FPGA version:

- NCS4202—NA

The following are HoFPGA versions bundled in the IOS for 17.3.3 release:

- NCS4201—0X00030015
- NCS4202—0X0003001e

The following is the CEM FPGA version:

- NCS4202—NA

The following are HoFPGA versions bundled in the IOS for 17.3.4 release:

- NCS4201—0X00030016

  ROMMON version—15.6(43r)S
- NCS4202— 0X0003001e

  ROMMON version—15.6(43r)S

The following is the CEM FPGA version:

- NCS4202— 0X00020008

The following are HoFPGA versions bundled in the IOS for 17.3.5 release:

- NCS4201—0X0004001b
- ROMMON version—15.6(43r)S
- NCS4202— 0X0003001e
- ROMMON version—15.6(43r)S

The following is the CEM FPGA version:

- NCS4202— 0X00020008

The following are HoFPGA versions bundled in the IOS for 17.3.7 release:

- NCS4201—0X0004001b
- ROMMON version—15.6(43r)S
- NCS4202— 0X0003001e
- ROMMON version—15.6(43r)S

The following is the CEM FPGA version:

- NCS4202— 0X00020008

The following are HoFPGA versions bundled in the IOS for 17.3.8 release:

- NCS4201—0X0004001b
- ROMMON version—15.6(43r)S
- NCS4202— 0X0003001e
- ROMMON version—15.6(43r)S

The following is the CEM FPGA version:

- NCS4202— 0X00020008

The following are HoFPGA versions bundled in the IOS for 17.3.8a release:

- NCS4201—0X0004001b
- ROMMON version—15.6(43r)S
- NCS4202— 0X0003001e
- ROMMON version—15.6(43r)S

The following is the CEM FPGA version:

- NCS4202— 0X00020008

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
```

- VCoP/TSoP smart SFPs are not 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, secondary ROMMON partition is also auto upgraded after a successful primary ROMMON partition upgrade is complete. You can reload the router at the next planned reload to complete the secondary ROMMON upgrade.
- For Cisco IOS XE Amsterdam Release 17.3.x, Cisco IOS XE Bengaluru Release 17.4.x, and earlier, the secondary ROMMON partition is not auto upgraded. You must manually upgrade it using the **upgrade rom-mon filename** command.
- Starting with ROMMON release version 15.6(43r)S, ROMMON version is secure. Once the ROMMON version is upgraded, it cannot be downgraded to a non-secure ROMMON version.
- Secure ROMMON is supported from Cisco IOS XE Amsterdam Release 17.3.1 onwards. However, it is compatible with all the releases.

  Any future secure ROMMON upgrade or downgrade is only possible from Cisco IOS XE Amsterdam Release 17.3.1 onwards.
- Any non-secure FPGA bundled releases moving to Cisco IOS XE Bengaluru Release 17.3.x or future releases can result in an FPGA upgrade and a ROMMON upgrade. If FPGA upgrade happens parallely with the ROMMON upgrade, you can only expect a single reload. If FPGA upgrade gets delayed and happens post ROMMON upgrade, two reloads are expected to complete both the upgrade processes. This is followed by a successful bootup of the target release image.

Additional References

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.

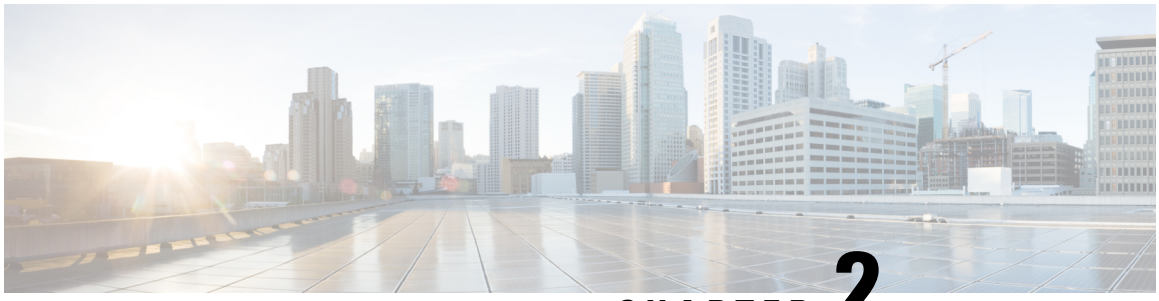
MIB Support

To view supported MIB, go to http://tools.cisco.com/ITDIT/MIBS/MainServlet.

Accessibility Features in the Cisco NCS 4201 and Cisco NCS 4202 Series

For a list of accessibility features in Cisco NCS 4201 and Cisco NCS 4202 Series, see the Voluntary Product Accessibility Template (VPAT) on the Cisco website, or contact accessibility@cisco.com.

All product documents are accessible except for images, graphics, and some charts. If you would like to receive the product documentation in audio format, braille, or large print, contact accessibility@cisco.com.



CHAPTER 2

What's New in Cisco IOS XE Amsterdam 17.3.x

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

What's New in Hardware for Cisco IOS XE Amsterdam 17.3.8a

There are no new hardware features in this release.

What's New in Software for Cisco IOS XE Amsterdam 17.3.8a

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 Amsterdam 17.3.8

There are no new hardware features in this release.

What's New in Software for Cisco IOS XE Amsterdam 17.3.8

There are no new software features in this release.

What New in Hardware - Cisco IOS XE Amsterdam 17.3.7

There are no new hardware features in this release.

What New in Software - Cisco IOS XE Amsterdam 17.3.7

There are no new software features in this release.

What New in Hardware - Cisco IOS XE Amsterdam 17.3.6

There are no new hardware features in this release.

What New in Software - Cisco IOS XE Amsterdam 17.3.6

There are no new software features in this release.

What New in Hardware - Cisco IOS XE Amsterdam 17.3.5

There are no new hardware features in this release.

What New in Software - Cisco IOS XE Amsterdam 17.3.5

There are no new software features in this release.

What New in Hardware - Cisco IOS XE Amsterdam 17.3.4

There are no new hardware features in this release.

What New in Software - Cisco IOS XE Amsterdam 17.3.4

There are no new software features in this release.

What New in Hardware - Cisco IOS XE Amsterdam 17.3.3

There are no new hardware features in this release.

What New in Software - Cisco IOS XE Amsterdam 17.3.3

There are no new software features in this release.

What New in Hardware - Cisco IOS XE Amsterdam 17.3.2a

There are no new hardware features in this release.

What New in Software - Cisco IOS XE Amsterdam 17.3.2a

There are no new software features in this release.

What New in Hardware - Cisco IOS XE Amsterdam 17.3.1

There are no new hardware features in this release.

What New in Software - Cisco IOS XE Amsterdam 17.3.1

Feature	Description
Segment Routing	
EVPN Single-Homing Over Segment Routing	The EVPN Single-Homing feature utilizes the BGP MPLS-based Ethernet VPN functionality as defined in RFC 7432. That is, to achieve single-homing between a Provider Edge (PE) and a Customer Edge (CE) device. There are three fundamental building blocks for EVPN technology, EVPN Instance (EVI), Ethernet Segment (ES), EVPN BGP routes and extended communities. For EVPN Single-Homing feature, a CE device is attached to a single PE device and has an Ethernet Segment.

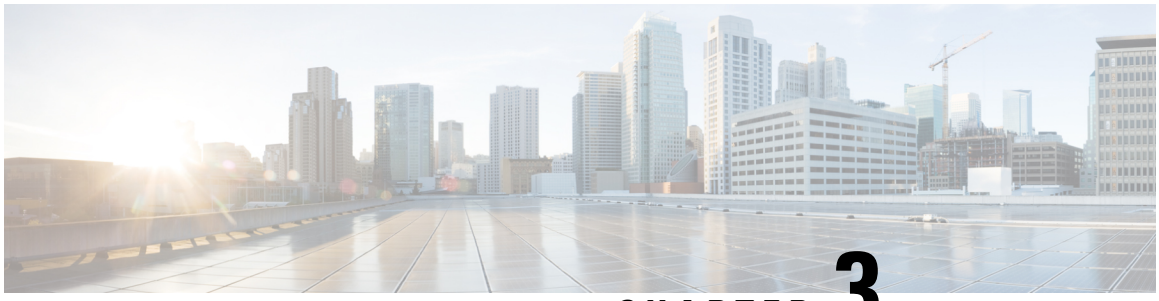
Feature	Description
SR-TE Per-Flow (Class) ODN and Automated Steering (PCE Delegated)	This feature lets you steer traffic with SR-TE PFP based on the QoS markings on the packets. The traffic is then switched onto the appropriate path based on the forward classes of the packet.
Segment Routing Performance Measurement Delay Measurement Using RFC 5357 (TWAMP Light)	This feature enables hardware timestamping. The Performance Measurement (PM) for link delay uses the light version of Two-Way Active Measurement Protocol (TWAMP) over IP and UDP defined in Appendix I of RFC 5357. TWAMP provides an alternative for interoperability when RFC 6374 is not used.
Segment Routing Performance Measurement End-to-End Delay Measurement	This feature allows to monitor the end-to-end delay experienced by the traffic sent over a Segment Routing policy. This feature ensures the delay does not exceed the specified threshold value and violate the SLAs. Use this feature to apply extended TE link delay metric (minimum delay value) to compute paths for Segment Routing policies as an optimization metric or as an accumulated delay bound.
Static Route Traffic Steering Using SR-TE Policy	This feature allows the non colored (BGP Extended Community) prefix to steer traffic over static policy. Prior to this release, only colored (BGP Extended Community) prefix could automatically steer traffic based on the defined policy using a tunnel interface. Unlike non colored prefix, this was possible only for the colored prefix as it could match the SR policy. IPv4 static routes are now enhanced to leverage the SR policies to aid Segment Routing Traffic Engineering (SR-TE). This facilitates traffic steering for non colored prefix as you can now configure IP Static Route with SR static policy. The following new keyword for the **ip route** command is introduced: **segment-routing policy** [*policy name*]
MPLS Traffic Engineering Path Link and Node Protection	
Static PW over P2MP	The Static Pseudowires over Point-to-Multipoint Traffic Engineering (P2MP TE) feature emulates the essential attributes of a unidirectional P2MP service. It can be used to transport layer 2 multicast services from a single source to one or more destinations. This feature is supported on the Cisco RSP2 module.
Timing and Synchronization	

Feature	Description
Telemetry for GNSS Module	This feature provides externalization of operational data using Network Configuration Protocol (NETCONF) or Yet Another Next Generation (YANG) data modeling language. Prior to this release, the traditional show commands were available to only view the GNSS statistic data. But, you could not use these show command outputs to manage network devices as demanded by centralized orchestration application such as Cisco Digital Network Architecture Center (DNAC). The introduction of this feature provides externalization of operational data using Network Configuration Protocol (NETCONF) or Yet Another Next Generation (YANG) data modeling language to bring more visibility in the timing services operations.
Alarm Configuring and Monitoring Guide, Cisco IOS XE 17 (Cisco NCS 4200 Series)	
Support for New Alarm Profile based on the Telcordia Profile for Chassis	The alarm profile based on Telcordia includes "Service Affecting" information for chassis entities. This information enables you to check the service affecting state for each alarm under a chassis.
IP Routing: BFD	
BFD Dampening	Bidirectional Forwarding Detection (BFD) is a detection protocol that is designed to provide fast forwarding path failure detection for encapsulations, topologies, and routing protocols. BFD provides a consistent failure detection method. BFD detects forwarding path failures at a uniform rate, rather than the variable rates for different routing protocol.
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	
IMA3G 1+1 OC3/12 Single Card APS Support	Automatic protection switching (APS) is a protection mechanism for SONET networks that enables SONET connections to switch to another SONET circuit when a circuit failure occurs. This protection schemes allows a pair of SONET 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. In the 1+1 architecture, there is one working interface (circuit) and one protection interface, and the same payload from the transmitting end is sent to both the receiving ends. The receiving end decides which interface to use.
Interworking Support for nxDS0	Interworking function (IWF) for PPP/HDLC is supported on Ethernet for E1/STM1 ports. This support is extended at nxDS0 level to speed up the GSR TDM migration.
IP Multicast: Multicast	
Aggregated Interface Statistics on Bundle	Aggregate multicast packet count is implemented for all the (S,G) entries for which the given BDI serves as the OIF.
Native Multicast SLA Measurement with MLDP	Outgoing interface (OIF) statistics in a native multicast setup implements an extra output to include the packet count sent over the (S,G) entry and the traffic rate.

Feature	Description
MPLS Layer 2 VPNs	
EVPN Single-Homing Over MPLS for NCS 4201 and NCS 4202	The EVPN Single-Homing feature utilizes the BGP MPLS-based Ethernet VPN functionality as defined in RFC 7432. That is, to achieve single-homing between a Provider Edge (PE) and a Customer Edge (CE) device. There are three fundamental building blocks for EVPN technology, EVPN Instance (EVI), Ethernet Segment (ES), EVPN BGP routes and extended communities. For EVPN Single-Homing feature, a CE device is attached to a single PE device and has an Ethernet Segment.

Other Supported Features in this Release

- **Configurable Y.1564 Service Activation Frame Sizes and EMIX Support**—Enterprise traffic (EMIX) packet size (default abceg pattern) is supported. For EMIX traffic, ITU-T Rec. Y.1564 packet sizes of 64, 128, 256, 1024, and 1518 bytes are supported. For more information, see the IP SLAs Configuration Guide, Cisco IOS XE 17 (Cisco ASR 4200 Series) .
- **Final ROMMON package**—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. For more information, see the High Availability Configuration Guide, Cisco IOS XE Amsterdam 17(Cisco NCS 4200 Series).
- Prior to release Cisco IOS XE Amsterdam 17.3.1, in case of Protocol Independent Multicast (PIM) Source Specific Multicast (SSM) with Bridge Domain Interface (BDI) as Incoming Interface (IIF), IGMP snooping was not supported on the corresponding Bridge Domain (BD). And, in case of PIM Sparse Mode (PIM-SM) with Bridge Domain Interface (BDI) as Incoming Interface (IIF), IGMP snooping was not supported on the corresponding BD in non-Designated Router (DR) node. To overcome these restrictions, enable the command **platform multicast bridge-tcam-handling disable** and reload the router.



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 Amsterdam 17.3.8a

There are no open caveats in this release.

Resolved Caveats – Cisco IOS XE Amsterdam 17.3.8a

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

Open Caveats – Cisco IOS XE Amsterdam 17.3.8

There are no open caveats in this release.

Resolved Caveats – Cisco IOS XE Amsterdam 17.3.8

There are no resolved caveats in this release.

Open Caveats – Cisco IOS XE Amsterdam 17.3.7

Identifier	Headline
CSCwb60002	Router may experience an unexpected reset when configuring or using interface BDI >= 4097
CSCwb77396	G.8032: Ring brief output doesnt display the Block port flag in Idle state
CSCwb60655	RSP2 : Interface remains down after SSO or ISSU upgrade
CSCwa30653	MVPN Profile 14 : Data MDT traffic not flowing with 2 paths when OSPF cost configured on 1 path
CSCwb75983	BFD Session with authentication with 16 or more characters remains down
CSCwc58616	Mac learning not happening for TRUNK EFP BDs associated with VPLS and the traffic are dropped

Resolved Caveats – Cisco IOS XE Amsterdam 17.3.7

Identifier	Headline
CSCvz73321	PEGM/RSP2: Rommon and fpga upgrade synchronization during autoupgrade
CSCwa29664	BGP neighbor cannot up with bfd strict-mode configured
CSCwd15539	RSP2/RSP3 : IM's shouldn't reload during sipspa install stage 3 in single step install ISSU
CSCwe13024	ASR900-RSP2: All readings for Power supply unit reflect as zero though the unit is functional

Open Caveats – Cisco IOS XE Amsterdam 17.3.6

Identifier	Headline
CSCwc84627	IM goes continous reboot for a PCIE bus error
CSCwc79322	Memory leak on ptpd_uea process

Open Caveats – Cisco IOS XE Amsterdam 17.3.6 - Platform Independent

Identifier	Headline
CSCvu15652	CEM26K : confiig / unconfig of CEME26K circuits causes 1-2 ckts in down state in standby mode.
CSCvv74332	VPLSoBKPW:MAC not flushed/withdrawn in remote peer on VC swichover from active to standby mode.
CSCwa30653	MVPN Profile 14 : Data MDT traffic not flowing with 2 paths when OSPF cost configured on 1 path
CSCvu06350	16.12.3 ES: Active RP crashed due to UNIX-EXT-SIGNAL: Segmentation fault(11), Process = BFD events
CSCvw19225	[17.5 EIGRP] Deleting bgp config does not remove the redistribute vrf CLI under Eigrp process
CSCwc25454	SSH to IPv6 LinkLocal address don't work without explict "ip ssh source-interface" configuration

Resolved Caveats – Cisco IOS XE Amsterdam 17.3.6

Identifier	Headline
CSCwb77723	ASR920/Cylon Duplicated unicast ARP packets
CSCwb01940	ASR920 drops L2 multicast traffic upon REP topology change
CSCwb01224	Multihop BFD transit packets getting droppedn on ASR920 after upgrade to 17.3.3

Resolved Caveats – Cisco IOS XE Amsterdam 17.3.6 - Platform Independent

Identifier	Headline
CSCwb66047	RSP3/ASR920/RSP2:node crashed @ l2rib_obj_peer_tbl_cmd_print

Open Caveats – Cisco IOS XE Amsterdam 17.3.5

There are no open caveats in this release.

Open Caveats – Cisco IOS XE Amsterdam 17.3.5 - Platform Independent

Caveat ID Number	Description
CSCwa36608	ICCP is stuck on CONNECTING state after RSP SO on Active PoA

Resolved Caveats – Cisco IOS XE Amsterdam 17.3.5

Caveat ID Number	Description
CSCvx58983	Xconnect Interface Flapping is seen when shut/no shut is issued or hardware failure occurs in path of Xconnect
CSCwa41638	MAC Table and L2VPN EVPN Table are out of sync
CSCwa09302	iMSG serial interfaces bitrate/sec data is displayed incorrectly in show command output
CSCvy25392	Cannot delete recovered clock configuration from STS-3c

Caveat ID Number	Description
CSCvy64788	LLC frames are getting looped back due to autonomic networking
CSCvy78284	Router will crash when zeroised RSA key is regenerated
CSCvy92074	MTU programming for MPLS L2 VC may fail after interface flaps
CSCvz20857	STS1E controller bay/port is wrong in controller UPDOWN syslog during T3 alarm
CSCvz42622	TPOP T1 SATOP : Cable length range needs to be changed to be consistent with the IMA48D/IMA3G
CSCvz79672	HQoS on egress TenGig interface is not working properly

Resolved Caveats – Cisco IOS XE Amsterdam 17.3.5 - Platform Independent

Caveat ID Number	Description
CSCvy56660	mlacp backbone interface defined in netconf as Container instead of list entry
CSCvy91369	IOS-XE : IPSLA ICMP-Jitter over L3VPN results incorrect jitter value.
CSCvz25471	NSO configuration push failure is seen due to GETCONF on BD gives additional value “mac learning”

Open Caveats – Cisco IOS XE Amsterdam 17.3.4

Caveat ID Number	Description
CSCvy25392	Cannot delete recovered clock configuration from STS-3c
CSCvy92074	MTU programming for MPLS l2 VC may fail after interface flaps

Open Caveats – Cisco IOS XE Amsterdam 17.3.4 - Platform Independent

There are no platform independent open caveats for this release.

Resolved Caveats – Cisco IOS XE Amsterdam 17.3.4

Caveat ID Number	Description
CSCvv99456	ACL entries with FRAGMENT keywords are not working on the router
CSCvx47340	When you insert 10G XFP in 10G port from 1G SFP, multicast traffic stops
CSCvx55831	Ingress Policy with set qos-group action creates extra TCAM entry with match on egress policy
CSCvx99501	Wrong SNMP traps are generated for high voltage threshold violations
CSCvy07380	IPSG does not deny traffic for few VLANS / BDs when DHCP binding entry does not exist
CSCvy16480	USB flashcards are not mounted on new router
CSCvy19318	MH-BFD over IPv6 stops working after upgrade
CSCvy82320	DHCP packets get dropped in case snopping is enabled
CSCvr43362	NCS 4202: Fan speed control measures for overheating router

Resolved Caveats – Cisco IOS XE Amsterdam 17.3.4 - Platform Independent

Caveat ID Number	Description
CSCvy04023	NETCONF datastore PTP data may unsync from running configuration

Open Caveats – Cisco IOS XE Amsterdam 17.3.3

Caveat ID Number	Description
CSCvs50029	Interface flaps and input errors are seen with optics GLC-FE-100BX-D

Open Caveats – Cisco IOS XE Amsterdam 17.3.3 - Platform Independent

Caveat ID Number	Description
CSCvu15652	CEM26K : confiiguration or unconfiguration of CEME26K circuits causes 1-2 ckts in down state in standby Cisco RSP3 module
CSCvu77385	[SVSP-457]-Full throughput is not working priority shaper percent is greater than ~40" 4206/4216 over 100g NNI
CSCvv71209	MTU changes on access interface causing low memory and stby RSP crash
CSCvv86988	Standby RP IOSD crashes continuously when serial acr nxds0 configs are applied
CSCvw54661	HS2 node is chasing with core generation and core is pointing to EFP process
CSCvw77485	Router may not send PIM register message if RP is reachable over TE tunnel

Resolved Caveats – Cisco IOS XE Amsterdam 17.3.3

Caveat ID Number	Description
CSCvw06674	Router crashes while deleting a BFD session
CSCvw34109	PTP failure due to LSMPI buffer exhaustion
CSCvr43362	NCS 4202: Fan speed control measures for overheating router

Resolved Caveats – Cisco IOS XE Amsterdam 17.3.3 - Platform Independent

Caveat ID Number	Description
CSCvg75709	Unnecessary RIB updates are observed when metric-style transition is configured
CSCvv40006	Traceback: IP SLA triggers INJECT_HDR_LENGTH_ER and INJECT_FEATURE_ESCAPE log messages
CSCvv79677	Cisco RSP2 module crashes after BGP flaps
CSCvv91741	Resequencing ACL with remarks only resequences permit or deny entries, remarks are not changed
CSCvw05035	BGP fall-over is not working when Null0 static route is configured

Caveat ID Number	Description
CSCvw19062	Changing external route tag does not update origin code in BGP
CSCvw37109	Pseudowire interface may be unexpectedly removed from VFI on unrelated configuration change
CSCvw86336	Unsupported interfaces for 'logging event link-status' needs to be removed in mapping

Resolved Caveats – Cisco IOS XE Amsterdam 17.3.2a

Caveat ID Number	Description
CSCvv10229	EDPL enhancement: Attach or detach pre-exising service-policy on EDPL is started or stopped
CSCvv16784	Automatic reload should happen after disabling platform bridging TCAM handling
CSCvr43362	NCS 4202: Fan speed control measures for overheating router

Resolved Caveats – Cisco IOS XE Amsterdam 17.3.2a - Platform Independent

Caveat ID Number	Description
CSCvc33357	Incorrect BC value is seen under **show policy-map** command when user-defined percentage based CIR is defined

Open Caveats – Cisco IOS XE Amsterdam 17.3.2a

Caveat ID Number	Description
CSCvu99207	Incorrect STP forwarding state programming occurs in platform
CSCvv14654	OOM kernel crash is seen in 3node stitching while using workarounds to recover traffic
CSCvw34109	PTP RX failure due to LSMPI buffer exhaustion

Open Caveats – Cisco IOS XE Amsterdam 17.3.x

Caveat ID Number	Description
CSCvs50029	Interface flaps and input errors are seen with optics GLC-FE-100BX-D

Caveat ID Number	Description
CSCvw34109	PTP RX failure due to LSMPI buffer exhaustion

Resolved Caveats – Cisco IOS XE Amsterdam 17.3.x

Caveat ID Number	Description
CSCvk22965	Bulk License 'Out of Compliance' support
CSCvr97004	VTY lines higher than 5 cannot be configured on NVGEN
CSCvs34376	**show pl ha pp act interface** command output does not show priority queue (HPCT) packet counters
CSCvs34482	ISSU does not work on RSP2 nodes
CSCvs50346	Random number of physical interfaces goes AdminDown when a single interface is shut down
CSCvs58497	After IPv6 nd cache is expired, transit traffic fails when ECMP is enabled
CSCvs70140	The interface output of CEM traffic rate is incorrect on the router
CSCvt32521	Duplex half changes to full after reload
CSCvu34503	Bundle 43r ROMMON changes to 17.3.1
CSCvu49097	Ports on the router do not come up when 1G SFPs are used
CSCvu78801	PPPoE VSA tags get overwritten at each PPPoE IA
CSCvr43362	NCS 4202: Fan speed control measures for overheating router

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