



Release Notes for Cisco NCS 520 Series Ethernet Access Device, Cisco IOS XE Fuji 16.9.x

First Published: 2020-10-05

Last Modified: 2020-02-05

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 1

Cisco NCS 520 Series Ethernet Access Device Overview	1
Feature Navigator	2
Determining the Software Version	2
Supported FPGA Version	2
Software Licensing Overview	2
Limitations and Restrictions on the Cisco NCS 520 Series Ethernet Access Device	3
Field Notices and Bulletins	4
MIBs Support	4
Accessibility Features in the Cisco NCS 520 Series Ethernet Access Device	5

CHAPTER 2

New Features 7

New Software Features in Cisco IOS XE Fuji 16.9.7	7
New Hardware Features in Cisco IOS XE Fuji 16.9.7	7
New Software Features in Cisco IOS XE Fuji 16.9.6	7
New Hardware Features in Cisco IOS XE Fuji 16.9.6	8
New Software Features in Cisco IOS XE Fuji 16.9.5	8
New Hardware Features in Cisco IOS XE Fuji 16.9.5	8
New Software Features in Cisco IOS XE Fuji 16.9.4	8
New Hardware Features in Cisco IOS XE Fuji 16.9.4	8
New Software Features in Cisco IOS XE Fuji 16.9.3	8
New Hardware Features in Cisco IOS XE Fuji 16.9.3	8
New Software Features in Cisco IOS XE Fuji 16.9.2	8
New Hardware Features in Cisco IOS XE Fuji 16.9.2	8
Supported Software Features in Cisco IOS XE Fuji 16.9.1a	9

Supported Hardware Features in Cisco IOS XE Fuji 16.9.1a 9

CHAPTER 3

Caveats 11

Cisco Bug Search Tool 12

Open Caveats – Cisco IOS XE Fuji 16.9.7 12

Platform Independent Open Caveats – Cisco IOS XE Fuji 16.9.7 12

Resolved Caveats – Cisco IOS XE Fuji 16.9.7 12

Platform Independent Resolved Caveats – Cisco IOS XE Fuji 16.9.7 12

Open Caveats – Cisco IOS XE Fuji 16.9.6 13

Resolved Caveats – Cisco IOS XE Fuji 16.9.6 13

Open Caveats – Cisco IOS XE Fuji 16.9.5 13

Resolved Caveats – Cisco IOS XE Fuji 16.9.5 13

Open Caveats – Cisco IOS XE Fuji 16.9.4 14

Resolved Caveats – Cisco IOS XE Fuji 16.9.4 14

Open Caveats – Cisco IOS XE Fuji 16.9.4 14

Resolved Caveats - Platform Independent 14

Open Caveats – Cisco IOS XE Fuji 16.9.3 15

Resolved Caveats – Cisco IOS XE Fuji 16.9.3 15

Platform Independent Open Caveats - Cisco IOS XE Fuji 16.9.3 15

Open Caveats – Cisco IOS XE Fuji 16.9.2 15

Platform Independent Open Caveats - Cisco IOS XE Fuji 16.9.2 15

Resolved Caveats – Cisco IOS XE Fuji 16.9.2 16

Platform Independent Open Caveats - Cisco IOS XE Fuji 16.9.2 16

Open Caveats – Cisco IOS XE Fuji 16.9.1a 18

Closed Caveats – Cisco IOS XE Fuji 16.9.1a 18



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.

- [Cisco NCS 520 Series Ethernet Access Device Overview, on page 1](#)
- [Feature Navigator, on page 2](#)
- [Determining the Software Version, on page 2](#)
- [Supported FPGA Version, on page 2](#)
- [Software Licensing Overview, on page 2](#)
- [Limitations and Restrictions on the Cisco NCS 520 Series Ethernet Access Device, on page 3](#)
- [Field Notices and Bulletins, on page 4](#)
- [MIBs Support, on page 4](#)
- [Accessibility Features in the Cisco NCS 520 Series Ethernet Access Device, on page 5](#)

Cisco NCS 520 Series Ethernet Access Device Overview

The Cisco NCS 520 Series Ethernet Access Device is a family of low cost, fixed Carrier Ethernet Network Interface Devices (NID) and a switch that is targeted to be the next generation replacement of the Cisco ME 3400 series Access Switches. The Cisco NCS 520 Series Ethernet Access Device adds 10G NID and low-cost MBH switch to the existing Service Provider Access portfolio, with the following features:

- MEF CE 3.0 compliant
- Premium SKUs with support for extended temperature (from -40C to 65C)
- Conformal coating on the PCBAs (to be able to support installation in ventilated enclosures)

This release note contains information about the Cisco NCS 520 Series Ethernet Access Device, provides features information for these devices, hardware support, limitations and restrictions, and caveats.

This release note provides information for these variants of the Cisco NCS 520 Series Ethernet Access Device:

- N520-4G4Z-A (Base)
- N520-X-4G4Z-A (Premium)
- N520-X-4G4Z-D (Premium)
- N520-20G4Z-A (Base)
- N520-20G4Z-D (Base)
- N520-X-20G4Z-A (Premium)
- N520-X-20G4Z-D (Premium)

Feature Navigator

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

Determining the Software Version

Use the following commands to verify your software version:

- Consolidated Package— **show version**

Supported FPGA Version

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

Table 1: FPGA Versions for NCS520-20G4Z-A, NCS520-20G4Z-D, NCS520-X-20G4Z-A, NCS520-X-20G4Z-D, N520-4G4Z-A, N520-X-4G4Z-A and N520-X-4G4Z-D

Release	FPGA Version
Cisco IOS XE Fuji 16.9.7	0x0003001E

Software Licensing Overview

The Cisco NCS 520 Series Ethernet Access Device supports the following types of licenses:

- Port Licensing—Port Upgrade license is available as a "Pay as you Grow" model.

- 10G upgrade license
- 1G upgrade license
- Metro Access (default)

The following method is used to activate the above licenses:

- Cisco Software Licensing—The Cisco Software License Activation feature is a set of processes and components to activate Cisco software feature sets by obtaining and validating fee-based Cisco software licenses.



Note Licenses generated by the Cisco Software Licensing are tied to the UDI of the chassis and a corresponding watchtower device certificate (WDC) is stored in the system.

The following features are supported for the software licenses:

- QoS, with deep buffers and hierarchical QoS (HQOS)
- Layer 2: 802.1d, 802.1q
- Ethernet Virtual Circuit (EVC)
- Ethernet OAM (802.1ag, 802.3ah)
- IPv4 and IPv6 host connectivity

Limitations and Restrictions on the Cisco NCS 520 Series Ethernet Access Device



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 interface** 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
```
- Adding or deleting the Trunk Ethernet flow points (TEFPs) with scaled bridge-domain, without delay causes the Cisco NCS 520 Series Ethernet Access Device to crash.
- Virtual services should be deactivated and uninstalled before performing replace operations.
- The **controller** and **nid-controller** commands are not supported.
- Cisco NCS 520 Series Ethernet Access Device displays an error in Hierarchical QoS policy while trying to remove the **bandwidth** and **bandwidth percent** commands from the default parent class dynamically. To remove the commands, you must first remove the bandwidth from child class and then from the parent class.
- When port is in OPER-DOWN state, applying Hierarchical QoS followed by speed change sets wrong bandwidth values on standard queues. To work around the mismatch, you must reattach the policy to the port level again.

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.

MIBs Support

The below tables summarize the supported MIBs on the Cisco NCS 520 Series Ethernet Access Device.

Supported Systems SNMP MIBs		
IF-MIB	CISCO-flash-mib	cisco-ENTITY-ALARM
CISCO-ENTITY-EXT-MIB	CISCO-BULK-FILE-MIB	NOTIFICATION-LOG-MIB
SNMP-COMMUNITY-MIB	CISCO-ENHANCED-MEMPOOL-MIB	CISCO-SYSLOG-MIB
SNMP-FRAMEWORK-MIB	ENTITY-SENSOR-MIB	CISCO-CONFIG-MAN-MIB
SNMPv2-MIB	SNMP-MPD-MIB	entity-state-mib-cisco
CISCO-ENTITY-MIB	CISCO-ENTITY-SENSOR-MIB	
Supported Layer 2 and OAM SNMP MIBs		
DS1-MIB	CISCO-CDP-MIB	CISCO-CEF-MIB

Supported Layer 2 and OAM SNMP MIBs		
CISCO-IPSLA-ETHERNET-MIB	CISCO-ETHER-CFM-MIB	IEEE8021-CFM-MIB
Supported QoS SNMP MIBs		
CLASS-BASED-QOS-POLICING-MIB	CLASS-BASED-QOS-MARKING-MIB	CLASS-BASED-QOS-SHAPE-MIB
CISCO-CLASS-BASED-QOS-MIB		

Accessibility Features in the Cisco NCS 520 Series Ethernet Access Device

For a list of accessibility features in Cisco NCS 520 Series Ethernet Access Device, 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

New Features

This chapter describes the new hardware and software features supported on the Cisco ASR 920 Series Routers for this release.

- [New Software Features in Cisco IOS XE Fuji 16.9.7, on page 7](#)
- [New Hardware Features in Cisco IOS XE Fuji 16.9.7, on page 7](#)
- [New Software Features in Cisco IOS XE Fuji 16.9.6, on page 7](#)
- [New Hardware Features in Cisco IOS XE Fuji 16.9.6, on page 8](#)
- [New Software Features in Cisco IOS XE Fuji 16.9.5, on page 8](#)
- [New Hardware Features in Cisco IOS XE Fuji 16.9.5, on page 8](#)
- [New Software Features in Cisco IOS XE Fuji 16.9.4, on page 8](#)
- [New Hardware Features in Cisco IOS XE Fuji 16.9.4, on page 8](#)
- [New Software Features in Cisco IOS XE Fuji 16.9.3, on page 8](#)
- [New Hardware Features in Cisco IOS XE Fuji 16.9.3, on page 8](#)
- [New Software Features in Cisco IOS XE Fuji 16.9.2, on page 8](#)
- [New Hardware Features in Cisco IOS XE Fuji 16.9.2, on page 8](#)
- [Supported Software Features in Cisco IOS XE Fuji 16.9.1a, on page 9](#)
- [Supported Hardware Features in Cisco IOS XE Fuji 16.9.1a, on page 9](#)

New Software Features in Cisco IOS XE Fuji 16.9.7

There are no new features introduced for this release.

New Hardware Features in Cisco IOS XE Fuji 16.9.7

There are no new features introduced for this release.

New Software Features in Cisco IOS XE Fuji 16.9.6

There are no new Software Features introduced for this release.

New Hardware Features in Cisco IOS XE Fuji 16.9.6

There are no new features introduced for this release.

New Software Features in Cisco IOS XE Fuji 16.9.5

There are no new Software Features introduced for this release.

New Hardware Features in Cisco IOS XE Fuji 16.9.5

There are no new features introduced for this release.

New Software Features in Cisco IOS XE Fuji 16.9.4

There are no new Software Features introduced for this release.

New Hardware Features in Cisco IOS XE Fuji 16.9.4

There are no new features introduced for this release.

New Software Features in Cisco IOS XE Fuji 16.9.3

There are no new features introduced for this release.

New Hardware Features in Cisco IOS XE Fuji 16.9.3

There are no new features introduced for this release.

New Software Features in Cisco IOS XE Fuji 16.9.2

There are no new features introduced for this release.

New Hardware Features in Cisco IOS XE Fuji 16.9.2

There are no new features introduced for this release.

Supported Software Features in Cisco IOS XE Fuji 16.9.1a

Support for Flex Links

Flex Link is a pair of Layer 2 interfaces, where one interface is configured to act as a backup to the other. The feature provides an alternative solution to the Spanning Tree Protocol (STP), allowing you to turn off STP and still provide basic link redundancy. Flex Links are typically configured in service provider or enterprise networks, where, you do not want to run STP on the router.

For more information, see LAN Switching Configuration Guide (Cisco NCS 520 Series).

Supported Hardware Features in Cisco IOS XE Fuji 16.9.1a

The Cisco NCS 520 Series Ethernet Access Device supports the following four new variants in Cisco IOS XE Fuji 16.9.1:

- N520-20G4Z-A (Base)
- N520-20G4Z-D (Base)
- N520-X-20G4Z-A (Premium)
- N520-X-20G4Z-D (Premium)

This subfamily of variants have fixed ENET interfaces (20 x 1GE + 4 x 10GE ports available), with a single or dual power supply for AC and dual power supplies for DC.



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.

- [Cisco Bug Search Tool, on page 12](#)
- [Open Caveats – Cisco IOS XE Fuji 16.9.7, on page 12](#)
- [Platform Independent Open Caveats – Cisco IOS XE Fuji 16.9.7, on page 12](#)
- [Resolved Caveats – Cisco IOS XE Fuji 16.9.7, on page 12](#)
- [Platform Independent Resolved Caveats – Cisco IOS XE Fuji 16.9.7, on page 12](#)
- [Open Caveats – Cisco IOS XE Fuji 16.9.6, on page 13](#)
- [Resolved Caveats – Cisco IOS XE Fuji 16.9.6, on page 13](#)
- [Open Caveats – Cisco IOS XE Fuji 16.9.5, on page 13](#)
- [Resolved Caveats – Cisco IOS XE Fuji 16.9.5, on page 13](#)
- [Open Caveats – Cisco IOS XE Fuji 16.9.4, on page 14](#)
- [Resolved Caveats – Cisco IOS XE Fuji 16.9.4, on page 14](#)
- [Open Caveats – Cisco IOS XE Fuji 16.9.4, on page 14](#)
- [Resolved Caveats - Platform Independent, on page 14](#)
- [Open Caveats – Cisco IOS XE Fuji 16.9.3, on page 15](#)
- [Resolved Caveats – Cisco IOS XE Fuji 16.9.3, on page 15](#)
- [Platform Independent Open Caveats - Cisco IOS XE Fuji 16.9.3, on page 15](#)
- [Open Caveats – Cisco IOS XE Fuji 16.9.2, on page 15](#)
- [Platform Independent Open Caveats - Cisco IOS XE Fuji 16.9.2, on page 15](#)
- [Resolved Caveats – Cisco IOS XE Fuji 16.9.2, on page 16](#)
- [Platform Independent Open Caveats - Cisco IOS XE Fuji 16.9.2, on page 16](#)
- [Open Caveats – Cisco IOS XE Fuji 16.9.1a, on page 18](#)

- [Closed Caveats – Cisco IOS XE Fuji 16.9.1a, on page 18](#)

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 Fuji 16.9.7

Caveat ID Number	Description
CSCvn64703	Frames with packet size lesser than Port MTU and greater than 1500B counted as Giant Frames

Platform Independent Open Caveats – Cisco IOS XE Fuji 16.9.7

Caveat ID Number	Description
CSCvv79677	ASR902-RSP2 crashed after BGP flaps
CSCvv80471	IPv6 BGP update is not applied after changes to inbound route-map
CSCvw19062	Changing external route tag does not update origin code in BGP
CSCvw44599	IPSLA UDP-jitter: Packets are sent at appx 2ms less or more than the config packet interval

Resolved Caveats – Cisco IOS XE Fuji 16.9.7

Caveat ID Number	Description
CSCvw19031	ISIS frames not forwarded transparently

Platform Independent Resolved Caveats – Cisco IOS XE Fuji 16.9.7

Caveat ID Number	Description
CSCvu85572	Dynamic neighbor does not form when peer-group is shutdown in different vrf

Caveat ID Number	Description
CSCvv17560	BMP BGP server can lead to CPUHOG and crashes
CSCvv40006	Traceback: IP SLA triggers INJECT_HDR_LENGTH_ER and INJECT_FEATURE_ESCAPE log message
CSCvv64633	BGP: advertised community list is malformed due to GSHUT community
CSCvw05035	BGP fall-over not working when Null0 static route is configured
CSCvw37109	Pseudowire interface may be unexpectedly removed from VFI on unrelated configuration change
CSCvx02515	BGP IPv6 link-local session does not come up

Open Caveats – Cisco IOS XE Fuji 16.9.6

There are no Open Caveats for this release.

Resolved Caveats – Cisco IOS XE Fuji 16.9.6

Caveat ID Number	Description
CSCvo35846	Egress drops are always observed in the interface counters
CSCvs18938	Y1731-DMM reports a very high delay and jitter values periodically
CSCvs76696	After restart smart license registration will fail

Open Caveats – Cisco IOS XE Fuji 16.9.5

Caveat ID Number	Description
CSCvs18938	Y1731-DMM reports a very high delay and jitter values periodically

Resolved Caveats – Cisco IOS XE Fuji 16.9.5

Caveat ID Number	Description
CSCvg82472	hw-util logs need to suppress while rommon upgrade
CSCvj74297	External alarms not working for alarm pins one to three
CSCvr07281	NCS520: link type set to "no negotiation auto" for 10G ports.

Caveat ID Number	Description
CSCvr25191	NCS520: TFTP download time enhancement with BDI interface.

Open Caveats – Cisco IOS XE Fuji 16.9.4

Caveat ID Number	Description
CSCvj62049	Dom3::shut/no-shut on member link causes cpu to drop all control protocol pkts.
CSCvj74297	External Alarms not working for alarm pins one to three
CSCvh15960	During powercycle Dying GASP is not getting generated to remote peer on all the ports.

Resolved Caveats – Cisco IOS XE Fuji 16.9.4

Caveat ID Number	Description
CSCvn59099	STP peering not working on BD where there is a logical BDI interface created for the same.
CSCvp61364	Shaper calculation should be done in L1 rate.

Open Caveats – Cisco IOS XE Fuji 16.9.4

Caveat ID Number	Description
CSCvj62049	Dom3::shut/no-shut on member link causes cpu to drop all control protocol pkts.
CSCvj74297	External Alarms not working for alarm pins one to three
CSCvh15960	During powercycle Dying GASP is not getting generated to remote peer on all the ports.

Resolved Caveats - Platform Independent

Caveat ID Number	Description
CSCvk34062	LLDP TX not working on few ports after the router is reloaded

Open Caveats – Cisco IOS XE Fuji 16.9.3

Caveat ID Number	Description
CSCvj62049	Dom3::shut/no-shut on member link causes cpu to drop all control protocol pkts.
CSCvj74297	External Alarms not working for alarm pins one to three
CSCvh15960	During powercycle Dying GASP is not getting generated to remote peer on all the ports.

Resolved Caveats – Cisco IOS XE Fuji 16.9.3

There are no new Resolved Caveats for this release.

Platform Independent Open Caveats - Cisco IOS XE Fuji 16.9.3

Caveat ID Number	Description
CSCvk34062	LLDP TX not working on few ports after the router is reloaded

Open Caveats – Cisco IOS XE Fuji 16.9.2

Caveat ID Number	Description
CSCvj62049	Dom3::shut/no-shut on member link causes cpu to drop all control protocol pkts.
CSCvj74297	External Alarms not working for alarm pins one to three
CSCvh15960	During powercycle Dying GASP is not getting generated to remote peer on all the ports.

Platform Independent Open Caveats - Cisco IOS XE Fuji 16.9.2

Caveat ID Number	Description
CSCvj17588	Router may reload in BGP Router process when interface flap occurs with IPv6 MPLS per vrf routes
CSCvk59169	Strict SID has NOT been enabled in ISIS segment-routing
CSCvm52543	Subscriber session hangs after the upgrade and reload

Caveat ID Number	Description
CSCvm59483	Host crashes the DSP if ipv6 commands are configured under Service-Engine [Purge ipv6 config option]
CSCvm61279	Crash under AFW_application_process with shared-line configuration
CSCvm76590	CUBE does not forward 200 OK in SRTP-RTP scenario with TCL script on Dial-peer
CSCvm76699	TCP closed when using Virtual IP HA(high availability)setup with WSAPI registration
CSCvn01507	ISR not recalculating the hash value correctly after payload change
CSCvn02047	Configuring more than 5k NAT entries cause high CPU utilization with no traffic.

Resolved Caveats – Cisco IOS XE Fuji 16.9.2

Caveat ID Number	Description
CSCvj66322	Port-channel load balancing is not evenly distributed for known unicast traffic across multiple VLANS
CSCvm80578	NCS520 does not generate CFM Continuity Check message, when MEP interface is being shutdown
CSCvm92920	Support for NTP broadcast functionality in NCS520
CSCvj37650	Port-channel MTU configs do not get synced to all member links.

Platform Independent Open Caveats - Cisco IOS XE Fuji 16.9.2

Caveat ID Number	Description
CSCuz14861	IOS-XE Fails to correctly populate RTCP SSRC Field
CSCvf65079	ASR CUBE 1K reloaded with reason: RG-application reload on voice-b2bha RG
CSCvj16209	CME with external SIP trunk registration results into crash
CSCvj24940	Voice VRF with No Bind OPTIONS Ping response not sent
CSCvj25678	Crash after failing to modify xcode
CSCvj27172	Crash during Generic Call Filter Module cleanup
CSCvj43156	Crash in XDR process: "fib_rp_table_broker_encode_buf.size <= FIB_RP_TABLE_BROKER_ENC_BUF_SZ"
CSCvj50005	ISR4K PPE ucode crash when processing ipsec traffic on CWS tunnel

Caveat ID Number	Description
CSCvj69654	OSPF originates default route without "default-information originate"
CSCvj73544	OSPF routing loop for external route with multiple VLINKs/ABRs
CSCvj88138	VASI NAT: FTP ALG translation is sometimes failed
CSCvj91448	PKI:-IP address parsing issue while printing the subject name if classless IP is used in Trustpoint
CSCvj92548	CSR1k-FlexVPN: Spoke to Spoke: Implicit NHRP entry due to expired resolution request handling.
CSCvj92862	Router returns 255 length byte-stream chars instead of actual length for OSPFV2 Key-string
CSCvj95351	OSPF SR uloop : After issuing clear ip ospf process OSPF process crashed.
CSCvk00446	BGP high CPU when config 256k vxlan static route
CSCvk02072	Hoot-n-holler multicast traffic marked with DSCP 0
CSCvk07838	CUBE is using wrong source IP address to send SIP error
CSCvk10633	BGP crash while running show command and same time BGP peer reset
CSCvk12152	Unable to remove command ip nat inside destination
CSCvk15062	Modification to ZBFW access-lists do not reflect in TCAM
CSCvk17777	When using VRF NAT port used for ftp data is not freed
CSCvk24323	Router crash in ISIS with SR Ti-LFA
CSCvk27007	MGCP status remains Down after IOS upgrade caused by CSCvh70570
CSCvk37875	High Availability system with two Voice Gateways - Crash
CSCvk49905	Crash when shifting the layer 2 LACP member peer from one link to another
CSCvk53405	Router crash - AFW_application_process
CSCvk56331	Initial contact in IKEv1 phase 2 rekey (QM1) causes all crypto sessions to drop
CSCvk60184	Random crash of data plane with SRTP-SRTP / SRTP-RTP load tests
CSCvk65072	Crash due ZBF + NAT
CSCvk65354	Extension Mobility Not working when used with Greek locale on SIP CME
CSCvk66880	CUBE incorrectly fomats SIP SDP
CSCvk69075	No calls shown in output show call active voice brief on CUBE & stale entries are present

Caveat ID Number	Description
CSCvk69093	CUBE is not responding to SIP INFO
CSCvm01351	Observed IPv6 Adj memory leaks
CSCvm02627	Incorrect Contact port 5060 used instead of 5061 by CUBE in 302 Moved Temporarily message
CSCvm03744	%FMFP-3-OBJ_DWNLD_TO_DP_FAILED:fman_fp_image:xxx" appears when configured ip port-map on Router
CSCvm06270	ICMP unreachables are not sent to the client on C1117 platform
CSCvm08571	Rework need on CSCvj59170 to support SDP parsing
CSCvm16619	CPP-mcplo-ucode crash while encrypting SIP packets with ALG NAT for SIP
CSCvm53491	SIP CME Crashes when Calling Shared Line
CSCvm56592	CME/BE4K: Corrupted config file for Auto Registered IP Phones after reload
CSCvm56670	ACL dropping packets after updating it - %CPPEXMEM-3-NOMEM
CSCvm66103	Crash due to communication failure - IPC (Inter-Procedure Call) messages between DSP and RP.

Open Caveats – Cisco IOS XE Fuji 16.9.1a

Caveat ID Number	Description
CSCvj88373	NCS520: Ten Gigabit Ethernet interface failed to come up after the iomd crash.
CSCvh15960	During powercycle Dying GASP is not getting generated to remote peer on all the ports.
CSCvj37650	Port-channel MTU configs do not get synced to all member links.
CSCvj62049	Shut or no-shut on member link causes CPU to drop all control protocol packets.
CSCvj66322	Port-channel load balancing is not evenly distributed for known unicast traffic across multiple VLANs.
CSCvj74297	External alarms are not working for alarm pins of range one to three.

Closed Caveats – Cisco IOS XE Fuji 16.9.1a

Caveat ID Number	Description
CSCvg89141	The status of control-processor health is reported as unknown.

Caveat ID Number	Description
CSCvg97602	Queue-depth stats are not shown in show policy-map output even with full queue buffer consumption.
CSCvh71767	Set cos is not rejected on a egress policy-map.
CSCvh77557	EFP policy in H-QoS fails after interface speed is changed manually.
CSCvh80098	Randomly node reloads after ptpd_uea crash.
CSCvi25332	NCS520 node stuck after kernel panic.
CSCvi30503	The btrace logs rotation failed and bootflash size reduced after format bootflash.
CSCvi31277	The tamd process crash seen with multiple reloads.
CSCvi85835	With back-to-back connection on the copper ports, the ports are not coming up in 100M speed.

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2018 Cisco Systems, Inc. All rights reserved.

