



Release Notes for Cisco ASR 920 Series Aggregation Services Router, Cisco IOS XE 17.15.x

First Published: 2024-08-14

Last Modified: 2025-08-06

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 ASR 920 Series Routers Overview 2
- Feature Navigator 2
- Feature Matrix 2
- Software Licensing Overview 2
- Determining the Software Version 3
- Upgrading to a New Software Release 4
- Supported HoFPGA and ROMMON Versions 4
- Restrictions and Limitations 10
- Additional References 12

CHAPTER 2

What's New in Cisco IOS XE 17.15.x 13

- What's New in Hardware for Cisco IOS XE 17.15.4 13
- What's New in Software for Cisco IOS XE 17.15.4 13
- What's New in Hardware for Cisco IOS XE 17.15.3b 13
- What's New in Software for Cisco IOS XE 17.15.3b 13
- What's New in Hardware for Cisco IOS XE 17.15.2 14
- What's New in Software for Cisco IOS XE 17.15.2 14
- What's New in Hardware for Cisco IOS XE 17.15.1 15
- What's New in Software for Cisco IOS XE 17.15.1 15

CHAPTER 3

Caveats 17

- Open Caveats—Cisco IOS XE 17.15.4 17
- Resolved Caveats—Cisco IOS XE 17.15.4 18
- Open Caveats—Cisco IOS XE 17.15.3b 18
- Resolved Caveats—Cisco IOS XE 17.15.3b 18

Resolved Caveats – Cisco IOS XE 17.15.2	18
Open Caveats–Cisco IOS XE 17.15.2	19
Resolved Caveats – Cisco IOS XE 17.15.1	19
Open Caveats–Cisco IOS XE 17.15.1	19
Cisco Bug Search Tool	20



CHAPTER 1

Introduction

This release notes contain information about the Cisco ASR 920 Series Aggregation Services Routers, provides new and changed information for these routers, hardware support, limitations and restrictions, and caveats.

This release notes provides information for these variants of the Cisco ASR 920 Series Routers:

- ASR-920-12CZ-A
- ASR-920-12CZ-D
- ASR-920-4SZ-A
- ASR-920-4SZ-D
- ASR-920-10SZ-PD
- ASR-920-24SZ-IM
- ASR-920-24SZ-M
- ASR-920-24TZ-M
- ASR-920-12SZ-IM
- ASR-920-12SZ-A
- ASR-920-12SZ-D
- ASR 920-8S4Z-PD
- [Cisco ASR 920 Series Routers Overview, on page 2](#)
- [Feature Navigator, on page 2](#)
- [Feature Matrix, on page 2](#)
- [Software Licensing Overview, on page 2](#)
- [Determining the Software Version, on page 3](#)
- [Upgrading to a New Software Release, on page 4](#)
- [Supported HoFPGA and ROMMON Versions, on page 4](#)
- [Restrictions and Limitations, on page 10](#)
- [Additional References, on page 12](#)

Cisco ASR 920 Series Routers Overview

The Cisco ASR 920 Series Aggregation Services Routers provide a comprehensive and scalable set of Layer 2 and Layer 3 VPN services in a compact package. They are temperature-hardened, small form factor, with high throughput and low power consumption ideal for mobile backhaul, business services and residential voice, video, and data ("triple-play") applications.

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.

Feature Matrix

The feature matrix lists the features supported for each platform. For more information, see the [Cisco ASR 920 Series Aggregation Services Routers Feature Compatibility Matrix](#).

Software Licensing Overview

Starting with Cisco IOS XE Cupertino 17.7.1, PAK licenses are no longer available. When you purchase the Cisco IOS XE Cupertino 17.7.1 release or later, Smart Licensing is enabled by default. We recommend that you move to Smart Licensing before upgrading to Cisco IOS XE Cupertino 17.7.1 or a higher release, for a seamless experience.

If you are using Cisco IOS XE Bengaluru 17.6.1 or an earlier release version, Smart Licensing is not enabled by default. To enable Smart Licensing, see [Software Activation Configuration Guide \(Cisco IOS XE ASR 920 Routers\)](#).

The router offers the following base licenses:

- Metro Services
- Metro IP Services
- Advanced Metro IP access
- SDM Video Template

Table 1: Cisco ASR 920 Software Licenses Feature Set

Metro Services	Metro IP Services	Metro Aggregation Services
—	Includes all features in Metro Services	Includes all features in Metro IP Services
QoS, with deep buffers and hierarchical QoS (HQOS)	IP routing (RIP, OSPF, EIGRP, BGP, IS-IS)	MPLS (LDP and VPN)

Metro Services	Metro IP Services	Metro Aggregation Services
Layer 2: 802.1d, 802.1q	PIM (SM, DM, SSM), SSM mapping	MPLS TE and FRR
Ethernet Virtual Circuit (EVC)	BFD	MPLS OAM
Ethernet OAM (802.1ag, 802.3ah)	Multi-VRF CE (VRF lite) with service awareness (ARP, ping, SNMP, syslog, trace-route, FTP, TFTP)	MPLS-TP
Multiple Spanning Tree (MST) and Resilient Ethernet Protocol (REP)	IEEE 1588-2008 Ordinary Slave Clock and Transparent Clock	Pseudowire emulation (EoMPLS, CESoPSN, and SAToP)
Synchronous Ethernet	—	VPLS and HVPLS
IPv4 and IPv6 host connectivity	—	Pseudowire redundancy
—	—	MR-APS and mLACP

The router offers the following additional feature licenses:

- ATM
- IEEE 1588-2008 Boundary Clock/Master Clock
- OC-x Port License

Determining the Software Version

Use the following commands to verify your software version:

- Consolidated Package— **show version**

Table 2: ROMMON Version

PIDs	ROMMON
ASR-920-12SZ-A , ASR-920-12SZ-D	15.6(54r)S
ASR-920-12SZ-IM	15.6(54r)S
ASR-920-12CZ-A, ASR-920-12CZ-D, ASR-920-4SZ-A, ASR-920-4SZ-D, ASR-920-10SZ-PD,ASR-920-24SZ-IM, ASR-920-24SZ-M, ASR-920-24TZ-M, and ASR920-8S4Z-PD	15.6(56r)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 ASR 920 Series Routers](#).

Upgrading the FPD Firmware

FPD Firmware packages are bundled with the software package. FPD upgrade is automatically performed on 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 firmware upgrade.

Supported HoFPGA and ROMMON Versions

The tables below list the HoFPGA and ROMMON version of the software releases.

Table 3: HoFPGA and ROMMON Versions for the Cisco ASR-920-12CZ-A, ASR-920-12CZ-D, ASR-920-4SZ-A, ASR-920-4SZ-D, ASR-920-10SZ-PD, and ASR 920-8S4Z-PD

Release	HoFPGA Version	ROMMON Version
Cisco IOS XE Amsterdam 17.1.x	0X00040043 (BFD/default template) 0x00020009 (Netflow template)	15.6(32r)S
Cisco IOS XE Amsterdam 17.3.1	0X00020009	15.6(43r)S
Cisco IOS XE Amsterdam 17.3.2	0X00020009	15.6(43r)S
Cisco IOS XE Bengaluru 17.4.1	0X00040044 (BFD/default template)	15.6(44r)S
Cisco IOS XE Bengaluru 17.5.1	0X00040044 (BFD/default template)	15.6(44r)S
Cisco IOS XE Bengaluru 17.6.1	0X00040044	15.6(48r)S
Cisco IOS XE Bengaluru 17.6.2	0X00040044	15.6(48r)S
Cisco IOS XE Cupertino 17.7.1	0X00040044	15.6(48r)S
Cisco IOS XE Cupertino 17.8.1	0X00040044	15.6(48r)S
Cisco IOS XE Dublin 17.10.1	0X00040044	15.6(56r)S
Cisco IOS XE Dublin 17.11.1a	0X00040044	15.6(56r)S

Release	HoFPGA Version	ROMMON Version
Cisco IOS XE Dublin 17.12.1	0X00040044	15.6(56r)S
Cisco IOS XE Dublin 17.12.2a	0X00040044	15.6(56r)S
Cisco IOS XE 17.13.1	0X00040044	15.6(56r)S
Cisco IOS XE 17.15.1	0X00040044	15.6(56r)S
Cisco IOS XE 17.15.2	0X00040044	15.6(56r)S
Cisco IOS XE 17.15.3b	0X00040044	15.6(56r)S
Cisco IOS XE 17.15.4	0X00040044	15.6(56r)S

Table 4: HoFPGA and ROMMON Versions for the Cisco ASR-920-24SZ-IM, ASR-920-24SZ-M, and ASR-920-24TZ-M

Release	HoFPGA Version	ROMMON Version
Cisco IOS XE Amsterdam 17.1.x	0x00030014 (BFD/default template) 0x00030014 (Netflow template)	15.6(32r)S
Cisco IOS XE Amsterdam 17.3.1	0X00030014	15.6(43r)S
Cisco IOS XE Amsterdam 17.3.2	0X00030014	15.6(43r)S
Cisco IOS XE Bengaluru 17.4.1	0X00030016	15.6(44r)S
Cisco IOS XE Bengaluru 17.5.1	0X00040019	15.6(44r)S
Cisco IOS XE Bengaluru 17.6.1	0X0004001b	15.6(48r)S
Cisco IOS XE Bengaluru 17.6.2	0X0004001b	15.6(48r)S
Cisco IOS XE Cupertino 17.7.1	0X0004001b	15.6(48r)S
Cisco IOS XE Cupertino 17.8.1	0X0004001b	15.6(48r)S
Cisco IOS XE Dublin 17.10.1	0X0004001b	15.6(56r)S
Cisco IOS XE Dublin 17.11.1a	0X0004001b	15.6(56r)S
Cisco IOS XE Dublin 17.12.1	0X0004001b	15.6(56r)S
Cisco IOS XE Dublin 17.12.2a	0X0004001b	15.6(56r)S
Cisco IOS XE 17.13.1	0X0004001b	15.6(56r)S
Cisco IOS XE 17.15.1	0X0004001b	15.6(56r)S
Cisco IOS XE 17.15.2	0X0004001b	15.6(56r)S
Cisco IOS XE 17.15.3b	0X0004001b	15.6(56r)S

Release	HoFPGA Version	ROMMON Version
Cisco IOS XE 17.15.4	0X0004001b	15.6(56r)S

Table 5: HoFPGA and ROMMON Versions for the Cisco ASR-920-12SZ-IM

Release	HoFPGA Version	ROMMON Version
Cisco IOS XE Amsterdam 17.1.x	0x0003001B (BFD/default template) 0x00020008 (Netflow template)	15.6(24r)S
Cisco IOS XE Amsterdam 17.3.1	0X0003001b	15.6(43r)S
Cisco IOS XE Amsterdam 17.3.2	0X0003001b	15.6(43r)S
Cisco IOS XE Bengaluru 17.4.1	0X0003001e	15.6(43r)S
Cisco IOS XE Bengaluru 17.5.1	0X0003001e	15.6(43r)S
Cisco IOS XE Bengaluru 17.6.1	0X0003001e	15.6(46r)S
Cisco IOS XE Bengaluru 17.6.2	0X0003001e	15.6(46r)S
Cisco IOS XE Cupertino 17.7.1	0x0003001e	15.6(46r)S
Cisco IOS XE Cupertino 17.8.1	0x0003001e	15.6(46r)S
Cisco IOS XE Dublin 17.10.1	0X0003001e	15.6(54r)S
Cisco IOS XE Dublin 17.11.1a	0X0003001e	15.6(54r)S
Cisco IOS XE Dublin 17.12.1	0X0003001e	15.6(54r)S
Cisco IOS XE Dublin 17.12.2a	0X0003001e	15.6(54r)S
Cisco IOS XE 17.13.1	0X0003001e	15.6(54r)S
Cisco IOS XE 17.15.1	0X0003001e	15.6(54r)S
Cisco IOS XE 17.15.2	0X0003001e	15.6(54r)S
Cisco IOS XE 17.15.3b	0X0003001e	15.6(54r)S
Cisco IOS XE 17.15.4	0X0003001e	15.6(54r)S

Table 6: HoFPGA and ROMMON Versions for the Cisco ASR-920-12SZ-A and ASR-920-12SZ-D

Release	HoFPGA Version	ROMMON Version
Cisco IOS XE Amsterdam 17.1.x	0x00010039 (BFD/default template) 0x10000007 (Netflow template)	15.6(29r)S

Release	HoFPGA Version	ROMMON Version
Cisco IOS XE Amsterdam 17.3.1	0X10000008	15.6(43r)S
Cisco IOS XE Amsterdam 17.3.2	0X10000008	15.6(43r)S
Cisco IOS XE Bengaluru 17.4.1	0X00010040 (BFD/default template)	15.6(43r)S
Cisco IOS XE Bengaluru 17.5.1	0X10000008	15.6(43r)S
Cisco IOS XE Bengaluru 17.6.1	0X10000008	15.6(46r)S
Cisco IOS XE Bengaluru 17.6.2	0X00020043	15.6(46r)S
Cisco IOS XE Cupertino 17.7.1	0X00020043	15.6(46r)S
Cisco IOS XE Cupertino 17.8.1	0X00020043	15.6(46r)S
Cisco IOS XE Dublin 17.10.1	0X00020043	15.6(54r)S
Cisco IOS XE Dublin 17.11.1a	0X00020043	15.6(54r)S
Cisco IOS XE Dublin 17.12.1	0X00020043	15.6(54r)S
Cisco IOS XE Dublin 17.12.2a	0X00020043	15.6(54r)S
Cisco IOS XE 17.13.1	0X00020043	15.6(54r)S
Cisco IOS XE 17.15.1	0X00020043	15.6(54r)S
Cisco IOS XE 17.15.2	0X00020043	15.6(54r)S
Cisco IOS XE 17.15.3b	0X00020043	15.6(54r)S
Cisco IOS XE 17.15.4	0X00020043	15.6(54r)S

Table 7: IM FPGA Versions for the Cisco ASR-920-24SZ-IM

Release	Gigabit Ethernet Interface Module (Phase 1) FPGA	Gigabit Ethernet Interface Module (Phase2) FPGA	8 T1/E1	16 T1/E1	32 T1/E1
Cisco IOS XE Amsterdam 17.1.x	0.49	69.24	0.54	0.54	0.46
Cisco IOS XE Amsterdam 17.3.1	0.49	69.24	0.54	0.54	0.46
Cisco IOS XE Amsterdam 17.3.2	0.75	N/A	N/A	0.54	0.46

Release	Gigabit Ethernet Interface Module (Phase 1) FPGA	Gigabit Ethernet Interface Module (Phase2) FPGA	8 T1/E1	16 T1/E1	32 T1/E1
Cisco IOS XE Bengaluru 17.4.1	0.75	N/A	N/A	0.54	0.46
Cisco IOS XE Bengaluru 17.5.1	0.75	N/A	N/A	0.54	0.46
Cisco IOS XE Bengaluru 17.6.1	0.75	69.24	0.54	0.54	0.46
Cisco IOS XE Bengaluru 17.6.2	0.75	69.24	0.54	0.54	0.46
Cisco IOS XE Cupertino 17.7.1	0.75	69.24	0.54	0.54	0.46
Cisco IOS XE Cupertino 17.8.1	0.75	69.24	0.54	0.54	0.46
Cisco IOS XE Dublin 17.10.1	0.75	69.24	0.54	0.54	0.46
Cisco IOS XE Dublin 17.11.1a	0.75	69.24	0.54	0.54	0.46
Cisco IOS XE Dublin 17.12.1	0.75	69.24	0.54	0.54	0.46
Cisco IOS XE Dublin 17.12.2a	0.75	69.24	0.54	0.54	0.46
Cisco IOS XE 17.13.1	0.75	69.24	0.54	0.54	0.46
Cisco IOS XE 17.15.1	0.75	69.24	0.54	0.54	0.46
Cisco IOS XE 17.15.2	0.75	69.24	0.54	0.54	0.46
Cisco IOS XE 17.15.3b	0.75	69.24	0.54	0.54	0.46
Cisco IOS XE 17.15.4	0.75	69.24	0.54	0.54	0.46

Table 8: IM FPGA Versions for the Cisco ASR-920-12SZ-IM

Release	Gigabit Ethernet Interface Module (Phase 1) FPGA	Gigabit Ethernet Interface Module (Phase2) FPGA	8 T1/E1	16 T1/E1	32 T1/E1
Cisco IOS XE Amsterdam 17.1.x	0.49	69.24	0.54	0.54	0.46
Cisco IOS XE Amsterdam 17.3.1	0.49	69.24	0.54	0.54	0.46
Cisco IOS XE Amsterdam 17.3.2	0.75	N/A	N/A	0.54	0.46
Cisco IOS XE Bengaluru 17.4.1	0.75	N/A	N/A	0.54	0.46
Cisco IOS XE Bengaluru 17.5.1	0.75	N/A	N/A	0.54	0.46
Cisco IOS XE Bengaluru 17.6.1	0.75	69.24	0.54	0.54	0.46
Cisco IOS XE Bengaluru 17.6.2	0.75	69.24	0.54	0.54	0.46
Cisco IOS XE Cupertino 17.7.1	0.75	69.24	0.54	0.54	0.46
Cisco IOS XE Cupertino 17.8.1	0.75	69.24	0.54	0.54	0.46
Cisco IOS XE Dublin 17.10.1	0.75	69.24	0.54	0.54	0.46
Cisco IOS XE Dublin 17.11.1a	0.75	69.24	0.54	0.54	0.46
Cisco IOS XE Dublin 17.12.1	0.75	69.24	0.54	0.54	0.46
Cisco IOS XE Dublin 17.12.2a	0.75	69.24	0.54	0.54	0.46

Release	Gigabit Ethernet Interface Module (Phase 1) FPGA	Gigabit Ethernet Interface Module (Phase2) FPGA	8 T1/E1	16 T1/E1	32 T1/E1
Cisco IOS XE 17.13.1	0.75	69.24	0.54	0.54	0.46
Cisco IOS XE 17.15.1	0.75	69.24	0.54	0.54	0.46
Cisco IOS XE 17.15.2	0.75	69.24	0.54	0.54	0.46
Cisco IOS XE 17.15.3b	0.75	69.24	0.54	0.54	0.46
Cisco IOS XE 17.15.4	0.75	69.24	0.54	0.54	0.46

Restrictions and Limitations



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.

- Embedded Packet Capture (EPC) is not supported on ASR 920 routers.
- 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.
- Adding or deleting the Trunk Ethernet flow points (TEFPs) with scaled bridge-domain, without delay causes the Cisco ASR 920 Series router to crash.
- Virtual services should be deactivated and uninstalled before performing replace operations.

- The Cisco ASR920 Series Routers no longer support the controller and nid-controller commands for the Cisco ME1200 switch.
- The following interface modules (IMs) do not require the activation command for IM boot up, provided no other IM is activated in subslot 0/1 before.

However, if an IM was activated in the system earlier, deactivate the previously-activated IM before inserting a new IM in system.

- 16-Port T1/E1 Interface Module
 - 32-Port T1/E1 Interface Module
 - 8-Port T1/E1 Interface Module
 - 4-port OC3/STM-1 (OC-3) or 1-port OC12/STM-4 (OC-12) Interface Module
 - 14-Port Serial Interface Module
 - 6-Port E and M Interface Module
 - 4-Port C37.94 Interface Module
- RS422 works on ports from 0 to 7 only.
 - The frame drops may occur for packets with packet size of less than 100 bytes, when there is a line rate of traffic over all 1G or 10G interfaces available in the system. This restriction is applicable only on RSP2 module and ASR 920 platform, and is not applicable for RSP3 module.
 - MPLS VC label packet with time-to-live (TTL) value of 2 is dropped at egress MPLS PE device due to ASIC limitations. During PHP process, MPLS TTL value for the VC label is decremented by one with implicit-null. The VC label-related TTL value is set to 255 while imposing the VC label due to multiple VC switching scenarios.
- Use the **no mpls ip propagate-ttl** command as the Short Pipe mode for the required label.
- Interface naming is from right to left. For more information, see the Cisco ASR 920 SoftwareConfiguration Guide .
 - 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 IPsectunnels for the first time.
 - One Ternary Content-Addressable Memory (TCAM) entry is utilized for Segment Routing Performance Measurement. This is required for the hardware timestamping to function.
 - 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.
 - 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.

- 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.

Additional References

Product Information

- [Cisco ASR 920 Series Aggregation Services Router Data Sheets](#)

Hardware Installation Guides

- [Cisco ASR 920 Series Aggregation Services Router Hardware Guides](#)

Software Configuration Guides

- [Cisco ASR 920 Series Aggregation Services Router Configuration Guides](#)

Regulatory Compliance and Safety Information

- [Regulatory Compliance and Safety Information for the Cisco ASR 920 Series Aggregation Services Routers](#)

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 ASR 920 Series Routers

For a list of accessibility features in Cisco ASR 920 Series Routers, 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.

End-of-Life and End-of-Sale Notices

For End-of-Life and End-of-Sale Notices for the Cisco ASR 920 Series Routers, see <http://www.cisco.com/c/en/us/products/routers/asr-920-series-aggregation-services-router/eos-eol-notice-listing.html>.



CHAPTER 2

What's New in Cisco IOS XE 17.15.x

- [What's New in Hardware for Cisco IOS XE 17.15.4, on page 13](#)
- [What's New in Software for Cisco IOS XE 17.15.4, on page 13](#)
- [What's New in Hardware for Cisco IOS XE 17.15.3b, on page 13](#)
- [What's New in Software for Cisco IOS XE 17.15.3b, on page 13](#)
- [What's New in Hardware for Cisco IOS XE 17.15.2, on page 14](#)
- [What's New in Software for Cisco IOS XE 17.15.2, on page 14](#)
- [What's New in Hardware for Cisco IOS XE 17.15.1, on page 15](#)
- [What's New in Software for Cisco IOS XE 17.15.1, on page 15](#)

What's New in Hardware for Cisco IOS XE 17.15.4

There are no new hardware features in this release.

What's New in Software for Cisco IOS XE 17.15.4

There are no new software features introduced for this release.

What's New in Hardware for Cisco IOS XE 17.15.3b

There are no new hardware features in this release.

What's New in Software for Cisco IOS XE 17.15.3b

Feature	Description
IP Addressing	

Feature	Description
Optimizing security and CPU utilization using software ACL in VRF traffic management	The Software ACL (SW ACL) is a platform-specific feature designed to control Layer 3 VRF traffic, such as ICMP, SSH, and Telnet, by managing traffic punted to the CPU. This feature enhances security and optimizes CPU utilization by allowing only explicitly permitted traffic to reach the CPU. The software ACLs enhance reliable and secure VRF-based services in enterprise networks and service provider networks. Command introduced: platform sw_acl enable interface {icmp ssh telnet}
MPLS	
Support for Co-routed Inter-area Flex-LSP Tunnels in Point-to-Point OSPF network	Co-routed Flex LSP tunnels now support an inter-area and multiple areas in a Point-to-Point OSPF network. For example, in an inter-area OSPF network, both the head-end or tail-end for a bidirectional LSPs that are in different areas learn the network topology and perform the automatic path redundancy when there is a network link failure.

What's New in Hardware for Cisco IOS XE 17.15.2

There are no new hardware features in this release.

What's New in Software for Cisco IOS XE 17.15.2

Feature	Description
Chassis	
NCCS 3GPP IP Specification Compliance for Interfaces	The router adheres to and complies with the IP specification guidelines as outlined by the National Centre for Communication Security (NCCS) certification, which is based on the 3rd Generation Partnership Project (3GPP) standards. This compliance ensures that the router meets rigorous security and performance benchmarks, providing users with a reliable and secure networking solution that aligns with industry best practices and regulatory requirements.
SNMP Dying Gasp support over IPv6 BGP Labeled Unicast Network	In addition to IPv4, SNMP dying gasp over FPGA is now extended to IPv6 BGP-Labeled Unicast (BGP-LU) network scenarios. This enhancement allows administrators to maintain and monitor their networks more effectively and robustly, ensuring reliable notification and management of critical network events across both IPv4 and IPv6 environments.

What's New in Hardware for Cisco IOS XE 17.15.1

Optics	Description
Management Port LED Status Indicators	The right LED indicator for the management port on the router now displays the link status and activity of the management port. You can monitor and troubleshoot the status and activity of the management port more effectively when the LED indicator turns green or in the Off state. For more details on the link status and activity, see the CPU Management Port LED Indication table: • Cisco ASR-920-12SZ-IM and ASR-920U-12SZ-IM • Cisco ASR-920-24SZ-IM, Cisco ASR-920-24SZ-M, Cisco ASR-920-24TZ-M

What's New in Software for Cisco IOS XE 17.15.1

Feature	Description
Alarm Configuring and Monitoring	
SONET Alarms for APS	• With Automatic Protection Switching (APS), SONET alarms soaking as per the recommendation from GR-253. • Alarm is raised or cleared during APS manual, force, and lock out switch actions. • When traffic is switched to an alternate link in the APS group, the severity of the alarms is affected based on service impact.
SD-BER and SF-BER Alarms for T1/E1 and T3/E3 services	Signal Failure-Bit Error Rate (SF-BER) and Signal Degrade-BER (SD-BER) alarms are declared when there is a signal failure or signal degradation that happens in the traffic. These alarms may be raised when the error rate of a given entity exceeds the user-configured BER threshold value. This helps the administrator to take corrective actions.
CEM OCx	
DDS DS0 Remote Latching Loopback	DS0 loopback is used for testing and troubleshooting the T1 or E1, T3 or E3, and OCx channel over PSN. You can configure DS0 loopback on these controllers for remote devices.
Protection Switching Count for Protected SONET Interface	In SONET with redundancy, an Automatic protection switching (APS) occurs between working and standby protection networks due to reasons like a circuit failure. Whenever the switching happens, the switching count is tracked using a Protection Switching Count (PSC) parameter. Depending on the PSC count, you can debug the network to identify the reason for extensive switching and work on the corrective actions.

Feature	Description
Performance Routing	
TCAM and NFT Commands	New commands have been introduced for the Ternary Content-Addressable Memory (TCAM) and NFT. TCAM You can now view the Ternary Content-Addressable Memory (TCAM) utilization for each control plane TCAM entry. Command: show platform hardware pp active tcam utilization control-plane-sessions NFT - You can now enable the collection of the packets punted to the CPU from the NFT hash table. Command: platform nft-summarization enable - Once the above command is enabled, you can use a timer to clean up the NFT hash table. Command: platform nft-summarization timer-value - You can view a summary of the packets punted to the CPU from the NFT hash table. Command: show platform hardware pp active infrastructure pi nft summary



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 17.15.4, on page 17](#)
- [Resolved Caveats—Cisco IOS XE 17.15.4, on page 18](#)
- [Open Caveats—Cisco IOS XE 17.15.3b, on page 18](#)
- [Resolved Caveats—Cisco IOS XE 17.15.3b, on page 18](#)
- [Resolved Caveats – Cisco IOS XE 17.15.2, on page 18](#)
- [Open Caveats—Cisco IOS XE 17.15.2, on page 19](#)
- [Resolved Caveats – Cisco IOS XE 17.15.1, on page 19](#)
- [Open Caveats—Cisco IOS XE 17.15.1, on page 19](#)
- [Cisco Bug Search Tool, on page 20](#)

Open Caveats—Cisco IOS XE 17.15.4

Identifier	Headline
CSCwp67315	Disable unsupported BER rate at path layer - CISCOCE-345
CSCwp64279	ASR-920 - CFM MIP auto-creation issue: MIP is not displayed in link-traces.

Resolved Caveats—Cisco IOS XE 17.15.4

Identifier	Headline
CSCwo58612	REP loop formed with multicast MAC when advertised through VRRP protocol.
CSCwm67252	ASR9xx shelf LED glowing without any alarm in the system - CISCOCE-316.
CSCwp12666	ASR 902 router goes down with nested peer-policy templates.
CSCwk48598	ASR-920-12SZ-IM: PSU/FAN showing as N/A after silent reload (last reboot reason is cpu hard reset).
CSCwo42037	QoS buffer carving for control plane requires improvement.
CSCwo50314	B3 SD and SF alarms raised concurrently.
CSCwo19003	Reboot after running the show mac-address table , show bridge-domain , and other show commands.
CSCwp09722	Smart licensing is not remaining registered status while the upgrading OS.
CSCwo28439	Incorrect clock selection interface is displaying for the show network-clock sync CLI command.

Open Caveats—Cisco IOS XE 17.15.3b

There are no open caveats in this release.

Resolved Caveats—Cisco IOS XE 17.15.3b

Identifier	Headline
CSCwm82342	Post reload HSRP is stuck in Init state and shows interface down
CSCwn94246	XCVR incompatible alarm missing without Sonet controller configurations.
CSCwn41240	Observed nnframed T1 as none and not shown in running-config under T3 controller.
CSCwo10841	XCVR incompatible alarm not asserted in Bay0 sonet controller cards

Resolved Caveats – Cisco IOS XE 17.15.2

Identifier	Headline
CSCwm91197	Silent reload of 3GMS IM due to PCI transaction failure.

Identifier	Headline
CSCwm86214	LDP session flap causes memory leak for EMPLS3LD which leads to RSP crash.

Open Caveats–Cisco IOS XE 17.15.2

Identifier	Headline
CSCwm63093	Protocol or interface configuration from start or run file is missing after reload issue.
CSCwm04031	17.9.2a-Both active and standby RSP's OAM or CFM configurations automatically changed after a reload.

Resolved Caveats – Cisco IOS XE 17.15.1

Identifier	Headline
CSCwi76112	Message to be displayed for M13 framing when configured with clear-channel
CSCwi60730	Speed LED status is not correct when sonet/sdh mode is configured
CSCwi33111	T1: Sev changes back from major to minor after IM OIR.
CSCwj06370	Serial cease traffic when configuring module other port
CSCwj05647	3GMS Serial interface protocol down with specific Modem
CSCwj12451	Update 2^20-O151 QRSS bert help string with QRSS Keyword
CSCwj44502	DCR clocking fails to get acquired on the with sts1-E mode
CSCwj99522	Need to support dtr not-used CLI in RS232 transparent mode
CSCwi92203	Channelized DS3: RAI is propagating to all DS1's when DS3 RAI is asserted

Open Caveats–Cisco IOS XE 17.15.1

Identifier	Headline
CSCwk46171	Enabling T1/E1 TPoP causes latency for control plane packets
CSCwk58917	L-bit propagation not enabled for LOF alarm after framing change with framed SAToP
CSCwk02087	BFD stuck in INIT state for interface Te0/0/0 & Te0/4/3
CSCwh75614	Increased CPU after upgrading router to 17.6.3 from 16.9.4 when 1000 SLM/DMM sessions are configured

Identifier	Headline
CSCwj60760	Confd process not in Started State in 5 mins after netconf-yang config is done
CSCwk27810	After reconfiguring second synce source the QL-failed for that source interface and ranking also 254

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>