Release Notes for Cisco ASR 920 Series Aggregation Services Router, 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** 1

Documentation Updates 2

Feature Matrix 3

Cisco ASR 920 Series Routers Overview 3

Feature Navigator 3

Determining the Software Version 3

Upgrading to a New Software Release 4

Supported HoFPGA and ROMMON Versions 4

Software Licensing Overview 8

Limitations and Restrictions on the Cisco ASR 920 Series Routers 10

Additional References 12

CHAPTER 2 **What's New in Cisco IOS XE Amsterdam 17.3.x** 15

What's New in Hardware for Cisco IOS XE Amsterdam 17.3.8a 15

What's New in Software for Cisco IOS XE Amsterdam 17.3.8a 15

What's New in Hardware for Cisco IOS XE Amsterdam 17.3.8 16

What's New in Software for Cisco IOS XE Amsterdam 17.3.8 16

What's New in Hardware for Cisco IOS XE Amsterdam 17.3.7 16

What's New in Software for Cisco IOS XE Amsterdam 17.3.7 16

What's New in Hardware for Cisco IOS XE Amsterdam 17.3.6 16

What's New in Software for Cisco IOS XE Amsterdam 17.3.6 16

What's New in Hardware for Cisco IOS XE Amsterdam 17.3.5 16

What's New in Software for Cisco IOS XE Amsterdam 17.3.5 16

What's New in Hardware for Cisco IOS XE Amsterdam 17.3.4 16

What's New in Software for Cisco IOS XE Amsterdam 17.3.4 17

What's New in Hardware for Cisco IOS XE Amsterdam 17.3.3 17

What's New in Software for Cisco IOS XE Amsterdam 17.3.3 **17**

What's New in Hardware for Cisco IOS XE Amsterdam 17.3.2a **17**

What's New in Software for Cisco IOS XE Amsterdam 17.3.2a **17**

What's New in Hardware for Cisco IOS XE Amsterdam 17.3.1 **17**

What's New in Software for Cisco IOS XE Amsterdam 17.3.1 **17**

CHAPTER 3 **Caveats** **21**

Resolved Caveats – Cisco IOS XE Amsterdam 17.3.8a **22**

Open Caveats – Cisco IOS XE Amsterdam 17.3.8a **22**

Resolved Caveats – Cisco IOS XE Amsterdam 17.3.8 **22**

Open Caveats – Cisco IOS XE Amsterdam 17.3.8 **22**

Resolved Caveats – Cisco IOS XE Amsterdam 17.3.7 **22**

Open Caveats – Cisco IOS XE Amsterdam 17.3.7 **22**

Resolved Caveats – Cisco IOS XE Amsterdam 17.3.6 **23**

Resolved Caveats – Cisco IOS XE Amsterdam 17.3.6 - Platform Independent **23**

Open Caveats – Cisco IOS XE Amsterdam 17.3.6 **23**

Open Caveats – Cisco IOS XE Amsterdam 17.3.6 - Platform Independent **24**

Resolved Caveats – Cisco IOS XE Amsterdam 17.3.5 **24**

Resolved Caveats – Cisco IOS XE Amsterdam 17.3.5 - Platform Independent **25**

Open Caveats – Cisco IOS XE Amsterdam 17.3.5 **25**

Open Caveats – Cisco IOS XE Amsterdam 17.3.5 - Platform Independent **25**

Resolved Caveats – Cisco IOS XE Amsterdam 17.3.4 **25**

Resolved Caveats – Cisco IOS XE Amsterdam 17.3.4 - Platform Independent **26**

Open Caveats – Cisco IOS XE Amsterdam 17.3.4 **26**

Open Caveats – Cisco IOS XE Amsterdam 17.3.4 - Platform Independent **26**

Resolved Caveats – Cisco IOS XE Amsterdam 17.3.3 **26**

Resolved Caveats – Cisco IOS XE Amsterdam 17.3.3 - Platform Independent **27**

Open Caveats – Cisco IOS XE Amsterdam 17.3.3 **27**

Open Caveats – Cisco IOS XE Amsterdam 17.3.3 - Platform Independent **27**

Resolved Caveats – Cisco IOS XE Amsterdam 17.3.2a **28**

Resolved Caveats – Cisco IOS XE Amsterdam 17.3.2a - Platform Independent **28**

Open Caveats – Cisco IOS XE Amsterdam 17.3.2a **28**

Open Caveats – Cisco IOS XE Amsterdam 17.3.x **28**

Resolved Caveats – Cisco IOS XE Amsterdam 17.3.x **29**

Cisco Bug Search Tool 29

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.

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 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-920-20SZ-M
- ASR-920-12SZ-IM
- ASR-920-12SZ-A
- ASR-920-12SZ-D
- ASR 920-8S4Z-PD

- Documentation Updates, on page 2
- Feature Matrix, on page 3
- Cisco ASR 920 Series Routers Overview, on page 3
- Feature Navigator, on page 3
- Determining the Software Version, on page 3
- Upgrading to a New Software Release, on page 4
- Supported HoFPGA and ROMMON Versions, on page 4
- Software Licensing Overview, on page 8
- Limitations and Restrictions on the Cisco ASR 920 Series Routers, on page 10
- Additional References, on page 12

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 ASR 920 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 Etherchannel Configuration Guide, Cisco IOS XE 17 (Cisco ASR 920 Series).

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.

The cumulative Feature Compatibility Release Matrix is available on Content Hub.

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.

Determining the Software Version

Use the following commands to verify your software version:

- Consolidated Package— **show version**

Table 1: ROMMON Version

PIDs	ROMMON
ASR-920-12SZ-A , ASR-920-12SZ-D	15.6(43r)S
ASR-920-12SZ-IM	15.6(43r)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, ASR920-8S4Z-PD, and ASR-920-20SZ-M	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 ASR 920 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.

Supported HoFPGA and ROMMON Versions

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

Table 2: 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 Gibraltar 16.12.1	0X00040043	15.6(32r)S
Cisco IOS XE Gibraltar 16.12.2a	0x00040043 (BFD/default template) 0x00020009 (Netflow template)	15.6(32r)S
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 Amsterdam 17.3.3	0X00020009	15.6(43r)S
Cisco IOS XE Amsterdam 17.3.4	0X00040044	15.6(43r)S
Cisco IOS XE Amsterdam 17.3.5	0X00040044	15.6(43r)S
Cisco IOS XE Amsterdam 17.3.6	0X00040044	15.6(43r)S
Cisco IOS XE Amsterdam 17.3.7	0X00040044	15.6(43r)S
Cisco IOS XE Amsterdam 17.3.8	0X00040044	15.6(43r)S

Release	HoFPGA Version	ROMMON Version
Cisco IOS XE Amsterdam 17.3.8a	0X00040044	15.6(43r)S

Table 3: 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 Gibraltar 16.12.1	0X00030014	15.6(32r)S
Csico IOS XE Gibraltar 16.12.2a	0x00030014 (BFD/default template) 0x00030014 (Netflow template)	15.6(32r)S
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 Amsterdam 17.3.3	0X00030015	15.6(43r)S
Cisco IOS XE Amsterdam 17.3.4	0X00030014	15.6(43r)S
Cisco IOS XE Amsterdam 17.3.5	0X0004001b	15.6(43r)S
Cisco IOS XE Amsterdam 17.3.6	0X0004001b	15.6(43r)S
Cisco IOS XE Amsterdam 17.3.7	0X0004001b	15.6(43r)S
Cisco IOS XE Amsterdam 17.3.8	0X0004001b	15.6(43r)S
Cisco IOS XE Amsterdam 17.3.8a	0X0004001b	15.6(43r)S

Table 4: HoFPGA and ROMMON Versions for the Cisco ASR-920-12SZ-IM

Release	HoFPGA Version	ROMMON Version
Cisco IOSXE Gibraltar 16.12.1	0X0003001B	15.6(24r)S
Csico IOS XE Gibraltar 16.12.2a	0x0003001B (BFD/default template) 0x00020008 (Netflow template)	15.6(24r)S
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

Release	HoFPGA Version	ROMMON Version
Cisco IOS XE Amsterdam 17.3.2	0X0003001b	15.6(43r)S
Cisco IOS XE Amsterdam 17.3.3	0X0003001e	15.6(43r)S
Cisco IOS XE Amsterdam 17.3.4	0X0003001e	15.6(43r)S
Cisco IOS XE Amsterdam 17.3.5	0X0003001e	15.6(43r)S
Cisco IOS XE Amsterdam 17.3.6	0X0003001e	15.6(43r)S
Cisco IOS XE Amsterdam 17.3.7	0X0003001e	15.6(43r)S
Cisco IOS XE Amsterdam 17.3.8	0X0003001e	15.6(43r)S
Cisco IOS XE Amsterdam 17.3.8a	0X0003001e	15.6(43r)S

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

Release	HoFPGA Version	ROMMON Version
Cisco IOS XE Gibraltar 16.12.1	0X00010039	15.6(29r)S
Csico IOS XE Gibraltar 16.12.2a	0x00010039 (BFD/default template) 0x10000007 (Netflow template)	15.6(29r)S
Cisco IOS XE Amsterdam 17.1.x	0x00010039 (BFD/default template) 0x10000007 (Netflow template)	15.6(29r)S
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 Amsterdam 17.3.3	0X10000008	15.6(43r)S
Cisco IOS XE Amsterdam 17.3.4	0X10000008	15.6(43r)S
Cisco IOS XE Amsterdam 17.3.5	0X00020043	15.6(43r)S
Cisco IOS XE Amsterdam 17.3.6	0X00020043	15.6(43r)S
Cisco IOS XE Amsterdam 17.3.7	0X00020043	15.6(43r)S
Cisco IOS XE Amsterdam 17.3.8	0X00020043	15.6(43r)S
Cisco IOS XE Amsterdam 17.3.8a	0X00020043	15.6(43r)S

Table 6: 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
Cisco IOS XE Amsterdam 17.3.3	0.75	N/A	N/A	0.54	0.46
Cisco IOS XE Amsterdam 17.3.4	0.75	69.24	0.54	0.54	0.46
Cisco IOS XE Amsterdam 17.3.5	0.75	69.24	0.54	0.54	0.46
Cisco IOS XE Amsterdam 17.3.6	0.75	69.24	0.54	0.54	0.46
Cisco IOS XE Amsterdam 17.3.7	0.75	69.24	0.54	0.54	0.46
Cisco IOS XE Amsterdam 17.3.8	0.75	69.24	0.54	0.54	0.46
Cisco IOS XE Amsterdam 17.3.8a	0.75	69.24	0.54	0.54	0.46

Table 7: 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 Amsterdam 17.3.3	0.75	N/A	N/A	0.54	0.46
Cisco IOS XE Amsterdam 17.3.4	0.75	69.24	0.54	0.54	0.46
Cisco IOS XE Amsterdam 17.3.5	0.75	69.24	0.54	0.54	0.46
Cisco IOS XE Amsterdam 17.3.6	0.75	69.24	0.54	0.54	0.46
Cisco IOS XE Amsterdam 17.3.7	0.75	69.24	0.54	0.54	0.46
Cisco IOS XE Amsterdam 17.3.8	0.75	69.24	0.54	0.54	0.46
Cisco IOS XE Amsterdam 17.3.8a	0.75	69.24	0.54	0.54	0.46

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 8: 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)
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

Limitations and Restrictions on the Cisco ASR 920 Series Routers

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
  ```

- 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 following restriction is applicable only to:

    - Cisco ASR-920-24SZ-IM, Cisco ASR-920-24SZ-M, and Cisco ASR-920-24TZ-M
    - Cisco ASR-920-20SZ-M
        - Traffic is dropped when packets of size 64 to 100 bytes are sent on 1G and 10G ports.
            - For 64-byte packets, traffic drop is seen at 70% and beyond of the line rate.
            - For 90-byte packets, traffic drop is seen at 90% and beyond of the line rate.
            - For 95-byte packets, traffic drop is seen at 95% and beyond of the line rate.
        - Traffic is dropped when:
            - Traffic is sent on a VRF interface.
            - Traffic is sent across layer 2 and layer 3.

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

- 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.
- 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 ASR-920-12SZ-IM, Cisco ASR-920U-12SZ-IM, and Cisco ASR-920U-12SZ-IM-CC. For Cisco ASR-920-12SZ-A and Cisco ASR-920-12SZ-D, Cisco IOS XE Amsterdam 17.3.1 has to be installed in sub packages mode. Booting in sub package mode takes care of auto upgrade to ROMMON version 15_6_43r_s on bootup. This workaround is not applicable to devices installed with ROMMON version 15.6(9r)S.
- 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.
- 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.
- Starting with Cisco IOS XE Bengaluru Release 17.4.1, Cisco ASR-920-24SZ-IM, Cisco ASR-920-24SZ-M, Cisco ASR-920-24TZ-M, Cisco ASR 920-10SZ-PD, Cisco ASR-920-12CZ-A/ASR-920-12CZ-D, Cisco ASR-920-4SZ-A/ASR-920-4SZ-D, and Cisco ASR-920-20SZ-M routers are auto upgraded to ROMMON version 15_6_44r_s.
- 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.

  However, starting with Cisco IOS XE Bengaluru Release 17.5.1, Cisco ASR-920-12SZ-IM, Cisco ASR-920U-12SZ-IM, Cisco ASR-920U-12SZ-IM-CC, Cisco ASR-920-12SZ-A and Cisco ASR-920-12SZ-D, ROMMON and FPGA upgrade are synchronized to happen in a single reload.

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 Amsterdam 17.3.x

This chapter describes the new hardware and software features supported on the Cisco ASR 920 Series routers in the following releases:

- What's New in Hardware for Cisco IOS XE Amsterdam 17.3.8a, on page 15
- What's New in Software for Cisco IOS XE Amsterdam 17.3.8a, on page 15
- What's New in Hardware for Cisco IOS XE Amsterdam 17.3.8, on page 16
- What's New in Software for Cisco IOS XE Amsterdam 17.3.8, on page 16
- What's New in Hardware for Cisco IOS XE Amsterdam 17.3.7, on page 16
- What's New in Software for Cisco IOS XE Amsterdam 17.3.7, on page 16
- What's New in Hardware for Cisco IOS XE Amsterdam 17.3.6, on page 16
- What's New in Software for Cisco IOS XE Amsterdam 17.3.6, on page 16
- What's New in Hardware for Cisco IOS XE Amsterdam 17.3.5, on page 16
- What's New in Software for Cisco IOS XE Amsterdam 17.3.5, on page 16
- What's New in Hardware for Cisco IOS XE Amsterdam 17.3.4, on page 16
- What's New in Software for Cisco IOS XE Amsterdam 17.3.4, on page 17
- What's New in Hardware for Cisco IOS XE Amsterdam 17.3.3, on page 17
- What's New in Software for Cisco IOS XE Amsterdam 17.3.3, on page 17
- What's New in Hardware for Cisco IOS XE Amsterdam 17.3.2a, on page 17
- What's New in Software for Cisco IOS XE Amsterdam 17.3.2a, on page 17
- What's New in Hardware for Cisco IOS XE Amsterdam 17.3.1, on page 17
- What's New in Software for Cisco IOS XE Amsterdam 17.3.1, on page 17

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's New in Hardware for Cisco IOS XE Amsterdam 17.3.7

There are no new hardware features in this release.

What's New in Software for Cisco IOS XE Amsterdam 17.3.7

There are no new software features in this release.

What's New in Hardware for Cisco IOS XE Amsterdam 17.3.6

There are no new hardware features in this release.

What's New in Software for Cisco IOS XE Amsterdam 17.3.6

There are no new software features in this release.

What's New in Hardware for Cisco IOS XE Amsterdam 17.3.5

There are no new hardware features in this release.

What's New in Software for Cisco IOS XE Amsterdam 17.3.5

There are no new software features in this release.

What's New in Hardware for Cisco IOS XE Amsterdam 17.3.4

There are no new hardware features in this release.

What's New in Software for Cisco IOS XE Amsterdam 17.3.4

There are no new software features in this release.

What's New in Hardware for Cisco IOS XE Amsterdam 17.3.3

There are no new hardware features in this release.

What's New in Software for Cisco IOS XE Amsterdam 17.3.3

There are no new software features in this release.

What's New in Hardware for Cisco IOS XE Amsterdam 17.3.2a

There are no new hardware features in this release.

What's New in Software for Cisco IOS XE Amsterdam 17.3.2a

There are no new software features in this release.

What's New in Hardware for Cisco IOS XE Amsterdam 17.3.1

There are no new hardware features in this release.

What's New in Software for 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. This feature is supported on Cisco ASR-920-12SZ-A and Cisco ASR-920-12SZ-D and Cisco ASR-920-12SZ-IM and ASR-920U-12SZ-IM.
Alarm Configuring and Monitoring Guide, Cisco IOS XE 17 (ASR 920 Series Routers)	
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.
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 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.
IP Multicast: PIM	
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.

Feature	Description
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.
MPLS Layer 2 VPNs	
EVPN Single-Homing Over MPLS	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. This feature is supported on the Cisco ASR 920 routers.

Other Supported Features in this Release

- **Bulk License**—From Cisco IOS XE Release 17.3.1 onwards, bulk port license will not be requested explicitly from the Smart Licensing server by IOS-XE software. Instead, an equivalent Port Upgrade License is consumed. For more information, see the Software Activation Configuration Guide (Cisco ASR 920 Routers).

- **Configurable Y.1564 Service Activation Frame Sizes and EMIX Support**—Starting with Cisco IOS XE Amsterdam 17.3.1 release, EMIX packet size is supported. For EMIX traffic, packet sizes of 64, 128, 256, 1024 and 1518 bytes are supported. These packet sizes are forwarded in ration of 1:1:1:1:1. For more information, see the IP SLAs Configuration Guide, Cisco IOS XE 17 (Cisco ASR 920 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 ASR-920-12SZ-IM and ASR-920U-12SZ-IM. For more information, see the Upgrading the Software on the Cisco ASR 920 Series Routers.

- **Ingress ACL to Filter Multicast Packets**—Starting with Cisco IOS XE Amsterdam 17.3.1, you can enable the **platform acl deny-acl-drop-set** command to drop all types of packets. For more information, see the Security Configuration Guide: Access Control Lists, Cisco IOS XE 17 (Cisco ASR 920 Routers).

- 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.

- 100 Mbps interface speed is supported on Cisco ASR-920-12SZ-A and Cisco ASR-920-12SZ-D.

CHAPTER 3

Caveats

This chapter describes open and resolved severity 1 and 2 caveats and select severity 3 caveats:

- The "Open Caveats" sections list open caveats that apply to the current release and may apply to previous releases. A caveat that is open for a prior release and is still unresolved applies to all future releases until it is resolved.
- The "Resolved Caveats" sections list caveats resolved in a specific release, but open in previous releases.

The bug IDs are sorted alphanumerically.

Note The Caveats section includes the bug ID and a short description of the bug. For details on the symptoms, conditions, and workaround for a specific caveat you must use the Bug Search Tool.

- Resolved Caveats – Cisco IOS XE Amsterdam 17.3.8a, on page 22
- Open Caveats – Cisco IOS XE Amsterdam 17.3.8a, on page 22
- Resolved Caveats – Cisco IOS XE Amsterdam 17.3.8, on page 22
- Open Caveats – Cisco IOS XE Amsterdam 17.3.8, on page 22
- Resolved Caveats – Cisco IOS XE Amsterdam 17.3.7, on page 22
- Open Caveats – Cisco IOS XE Amsterdam 17.3.7, on page 22
- Resolved Caveats – Cisco IOS XE Amsterdam 17.3.6, on page 23
- Resolved Caveats – Cisco IOS XE Amsterdam 17.3.6 - Platform Independent, on page 23
- Open Caveats – Cisco IOS XE Amsterdam 17.3.6, on page 23
- Open Caveats – Cisco IOS XE Amsterdam 17.3.6 - Platform Independent, on page 24
- Resolved Caveats – Cisco IOS XE Amsterdam 17.3.5, on page 24
- Resolved Caveats – Cisco IOS XE Amsterdam 17.3.5 - Platform Independent, on page 25
- Open Caveats – Cisco IOS XE Amsterdam 17.3.5, on page 25
- Open Caveats – Cisco IOS XE Amsterdam 17.3.5 - Platform Independent, on page 25
- Resolved Caveats – Cisco IOS XE Amsterdam 17.3.4, on page 25
- Resolved Caveats – Cisco IOS XE Amsterdam 17.3.4 - Platform Independent, on page 26
- Open Caveats – Cisco IOS XE Amsterdam 17.3.4, on page 26
- Open Caveats – Cisco IOS XE Amsterdam 17.3.4 - Platform Independent, on page 26
- Resolved Caveats – Cisco IOS XE Amsterdam 17.3.3, on page 26
- Resolved Caveats – Cisco IOS XE Amsterdam 17.3.3 - Platform Independent, on page 27
- Open Caveats – Cisco IOS XE Amsterdam 17.3.3, on page 27

- Open Caveats – Cisco IOS XE Amsterdam 17.3.3 - Platform Independent, on page 27
- Resolved Caveats – Cisco IOS XE Amsterdam 17.3.2a, on page 28
- Resolved Caveats – Cisco IOS XE Amsterdam 17.3.2a - Platform Independent, on page 28
- Open Caveats – Cisco IOS XE Amsterdam 17.3.2a, on page 28
- Open Caveats – Cisco IOS XE Amsterdam 17.3.x, on page 28
- Resolved Caveats – Cisco IOS XE Amsterdam 17.3.x, on page 29
- Cisco Bug Search Tool, on page 29

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 17.3.8a

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 17.3.8

There are no open caveats in this release.

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
CSCvy09725	Software solution to detect the BAD PSU

Open Caveats – Cisco IOS XE Amsterdam 17.3.7

Identifier	Headline
CSCvy81362	ASR920: Controllers are down due to LP-LOP alarm After CE reboots

Identifier	Headline
CSCwb60002	ASR900 may experience an unexpected reset when configuring or using interface BDI &gt;= 4097
CSCwb75983	BFD Session with authentication with 16 or more characters remains down
CSCwa30653	MVPN Profile 14 : Data MDT traffic not flowing with 2 paths when OSPF cost configured on 1 path
CSCwb77396	G.8032: Ring brief output doesnt display the Block port flag in Idle state
CSCwc58616	Mac learning not happening for TRUNK EFP BDs associated with VPLS and the traffic are dropped

Resolved Caveats – Cisco IOS XE Amsterdam 17.3.6

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 17.3.6

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 17.3.5

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
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 17.3.5

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 17.3.4

Caveat ID Number	Description
CSCvv99456	ACL entries with FRAGMENT keywords are not working on the ASR920 platform
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 ASR-920-12CZ-A
CSCvy19318	MH-BFD over IPv6 stops working after upgrade
CSCvy82320	DHCP packets get dropped in case snopping is enabled

Caveat ID Number	Description
CSCvr43362	ASR-920-12SZ-IM, ASR-920-12SZ-A/ASR-920-12SZ-D: 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 17.3.4

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 17.3.3

Caveat ID Number	Description
CSCvw06674	Router crashes while deleting a BFD session
CSCvw34109	PTP failure due to LSMPI buffer exhaustion
CSCvr43362	ASR-920-12SZ-IM, ASR-920-12SZ-A/ASR-920-12SZ-D: 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
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

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 in ASR920-12CZ

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

Caveat ID Number	Description
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 17.3.2a

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	ASR-920-12SZ-IM, ASR-920-12SZ-A/ASR-920-12SZ-D: 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 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 in Cisco ASR920-12CZ

Caveat ID Number	Description
CSCvw34109	PTP 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 change to full after reload
CSCvu34503	Bundle 43r ROMMON Changes to 17.3.1
CSCvu49097	Ports on Cisco ASR920-12SZ-D do not come up when 1G SFPs are used
CSCvu78801	PPPoE VSA tags gets overwritten at each PPPoE IA
CSCvr43362	ASR-920-12SZ-IM, ASR-920-12SZ-A/ASR-920-12SZ-D: 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