

# Release Notes for Cisco ASR 1000 Series, Cisco IOS XE Amsterdam 17.2.x

---

First Published: 2020-03-04

## New and Enhanced Software Features for Cisco IOS XE Amsterdam 17.2.1r

### New and Enhanced Features for Cisco IOS XE Amsterdam 17.2.1r



---

**Note** Cisco IOS XE Amsterdam 17.2.1r is the first release for Cisco ASR 1000 Series Aggregation Services Routers in the Cisco IOS XE Amsterdam 17.2.1 release series.

---



---

**Note** When you upgrade from one IOS XE release to another, you may see `%Invalid IPv6 address` error in the console log file. To rectify this error, enter global configuration mode, and re-enter the missing IPv6 alias commands and save the configuration. The commands will be persistent on subsequent reloads.

---

- **eZPM Performance Improvement**—The ezPM (easy performance monitor) introduces a performance improvement to the Application Performance profile for the following monitors:
  - application-client-server-stats
  - application-response-time
  - application-stats
  - media
  - url

The performance improvement is achieved by using the **mode optimised** command, which is enabled by default. If any other monitors are enabled, the performance improvement is automatically disabled.

- **6VPE over DMVPN with IPv6 Transport**—This feature supports multi-tenant IPv6 LAN prefixes. You can create these prefixes using an IPv6 DMVPN transport over the IPv4 overlay neighborhood.
- **MAG or customer-specific SLA Configuration**—This feature lets you configure MAG and customer-specific SLA to enable or disable IP SLA probes for PMIPv6 multipath management. To change the IP SLA probe parameters, use the **enable-sla** command.
- **Install and Deploy Cisco IOS XE and Cisco IOS XE SD-WAN Functionality on Edge Router**—This feature supports the use of a single `universalk9` image to deploy Cisco IOS XE SD-WAN and Cisco IOS XE functionality on all the supported devices. This `universalk9` image supports two modes - Autonomous mode (for IOS XE features) and controlled mode (for SD-WAN features).

- **Fail Close Revert Mode**—This feature lets group members remove the downloaded key server policy when there is no rekey or the group member is not able to re-register to the key server, and therefore return to the fail close mode.
- **Partial Configuration on CPE**—This feature supports use of Download RPC and Transfer Complete RPC to apply partial configuration on a CPE. It helps in the configuration of the CPE using download RPC method in CWMP instead of a manual configuration.
- **Enhanced VRF option for TCL socket**—In this release, the `-myvrf` keyword is added to the `fconfigure` command. This command specifies the options in a channel and enables you to associate a VRF table name with it.
- **Support for configuring GRE in tunnel encapsulation mode** —You can now configure a GRE tunnel in tunnel encapsulation mode in addition to the existing support for UDP tunnels.
- **QSFP-40/100-SRBD support**
- **MACSec on Port Channel**—This feature lets you configure MACsec encryption support on port channels therefore increasing the security of the traffic.
- **Improving NAT 44 performance**—This enhancement introduces `ip nat settings high` command that allows high connection set up rate for non-ALG NAT traffic.
- **VPN-ID in NetFlow exported packet**—This feature helps in identification of VPN using the MPLS VPN-ID.
- **Ingress and Egress Accounting MIB**—This feature allows the user to access all VxLAN accounting information in a single SNMP request.
- **DHCP unicast support on IOS-XE**—This feature introduces support for unicast mode on DHCP. This helps with splitting the horizon therefore improving security of the network.
- **Block BGP Dynamic Neighbor Sessions**—This feature allows you to block a router from establishing BGP dynamic neighbor sessions with certain nodes in a BGP peer group - these nodes are identified with their IP addresses. The ability to shut down or prevent the creation of BGP dynamic neighbor sessions is useful when a peer needs maintenance.
- **Support for Spoke Nodes as P Nodes in MPLS over DMVPN Phase 3**—This feature helps you configure a spoke node as either a P node or PE node in an MPLS over DMVPN deployment. To configure the spoke node, MP-BGP redistributes the route or label information between the spoke node and a PE node behind it.
- **LISP Support for TCP Authentication Option**—This feature helps you configure TCP Authentication Option (TCP AO) to prevent spoofed TCP segments in the sessions between an ETR and an MS.
- **EBGP Route Propagation without Policies**— This feature helps you configure an EBGP router to not propagate routes to and from an EBGP neighbor, when at least one inbound and one outbound policy are not configured for the neighbor.
- **Debug commands for PIM and VRF** — This release introduces debug commands for VRF (`debug condition vrf`) and PIM (`debug ip pim`) details. The `debug condition vrf` command lets you limit the debug output to a specific virtual routing and forwarding (VRF) instance. The `debug ip pim` command displays PIM packets received and transmitted, as well as PIM related events.
- **CUBE: Fax detect for IP-IP flows on IOS XE platform** — This release introduces support for fax detection for SIP calls and transfer on Cisco IOS XE platforms.

- [gNMI Protocol](#)— This release introduces support for gNMI protocol on ASR 1000 routers.

## New Hardware Supported for Cisco IOS XE Amsterdam 17.2.1r

- ESP-100X and ESP-200X—Cisco ASR 1000 ESP100-X and ESP-200X are QFP-based embedded services processors for the Cisco ASR1000 Series Routers. These ESP's are based on third-generation QFP ASIC. The ESP100-X contains one, third-generation QFP ASIC and the ESP200-X contains two, third-generation QFP ASIC.

## Resolved and Open Bugs for Cisco IOS XE Amsterdam 17.2.1r

### Resolved Bugs for Cisco IOS XE Amsterdam 17.2.1r

All resolved bugs for this release are available in the [Cisco Bug Search Tool](#) through the Resolved Bug Search.

Caveat ID Number	Description
<a href="#">CSCvg79330</a>	enable platform ipsec control plane conditional debug might cause FP/QFP IPsec outbound SA leak
<a href="#">CSCvp72039</a>	Ucode crash in infra with injected jumbo packet
<a href="#">CSCvq43550</a>	C1111-4P doesn't restart authentication for "clear authen session" if "authen open" the port
<a href="#">CSCvq47444</a>	CLI "config-exchange request" for any ikev2 profile has inconsistent behavior between IOS and confd
<a href="#">CSCvq71864</a>	Crash after executing "show archive config differences"
<a href="#">CSCvq75610</a>	freed rpi_parent is hit when deleting parent route by route update event
<a href="#">CSCvq81620</a>	Router crashes with ZBF HA sync.
<a href="#">CSCvq85556</a>	QoS configuration download failed when device reloading
<a href="#">CSCvq85913</a>	FlexVPN with password encryption -- after primary key change password in profile is not working
<a href="#">CSCvq87063</a>	getvpn suiteb:KS sends delete payload to gm's while scheduled rekey after primary KS dead/readded
<a href="#">CSCvq90361</a>	NHRP process crash on using same tunnel address on multiple spokes
<a href="#">CSCvq91046</a>	ASR1k crash in NAT code when processing PPTP traffic
<a href="#">CSCvq93850</a>	Passive FTP will fail when going over NAT and either client or server are off a SM-X-ES3
<a href="#">CSCvq98095</a>	Gi0/0/0 interface stays up/up and LED green after cable removed
<a href="#">CSCvq98949</a>	ASR1000-RP3: Punt Keepalive Failure (Punt LINK DOWN) or RP FREEZE

Caveat ID Number	Description
<a href="#">CSCVq98999</a>	ISR4451-X / 16.09.01 / Crash when IPSEC SA installation fails
<a href="#">CSCVq99498</a>	Crashes when trying to bring-up / bring-down IPsec crypto session for OSPFv3
<a href="#">CSCvr00983</a>	Unrecoverable Error with PVDm in 0/4 and Thule+dreamliner in 1/0 on ISR4300
<a href="#">CSCvr01327</a>	incorrect Total number of translations on show ip nat translations
<a href="#">CSCvr01454</a>	Punt fragment crash when receive EoGRE packets which have many fragments
<a href="#">CSCvr05193</a>	IOS PKI   Intermittently SubCA fails to rollover
<a href="#">CSCvr05214</a>	NAT translation table is removed before IKE SA deleted when idle timeout occur
<a href="#">CSCvr06666</a>	ISR4K Router CPP ucode Crash due IPv4 Fragmented packets
<a href="#">CSCvr12395</a>	vManage push "media-type rj45" when trying to configure duplex on ISR1k
<a href="#">CSCvr15127</a>	ASR1K/ISR4K Calls fade to no-way audio due to media inactivity detection after 20 minutes
<a href="#">CSCvr17167</a>	High memory utilization under "ezman" due to excessive parity error logging
<a href="#">CSCvr17169</a>	qfp ucode crash with media monitor
<a href="#">CSCvr18570</a>	When user cancel Call Forward All from the analog phone, user can't hear the confirmation tone
<a href="#">CSCvr24498</a>	keyman_rp Memory Leak
<a href="#">CSCvr26524</a>	Crash due to NBAR classification
<a href="#">CSCvr27554</a>	ASR1000-RP2/ASR1000-RP3: OIR after clock set doesn't save the time in RTC
<a href="#">CSCvr27777</a>	ASR1k - Egress byte count is innacurate
<a href="#">CSCvr31188</a>	GETVPN gikev2 Secondary KS doesn't push new policy after merging split condition
<a href="#">CSCvr33415</a>	Router may crash unexpectedly with Segmentation fault(11), Process = DSMP
<a href="#">CSCvr39932</a>	IPSEC install failed IPSEC_PAL_SA shows "unexpected number of parents"
<a href="#">CSCvr42776</a>	FMAN crashed after firewall reconfiguration
<a href="#">CSCvr42823</a>	Umbrella local domain bypass list is not programmed to DP, FMFP-3-OBJ_DWNLD_TO_DP_FAILED
<a href="#">CSCvr45917</a>	ASR1K DSP MIB cdspTotalChannels not responding
<a href="#">CSCvr48349</a>	ESP ucode crashed when running NAT with bpa (CGN)
<a href="#">CSCvr55746</a>	Device becomes unresponsive when configuring l2vpn context
<a href="#">CSCvr57565</a>	MGCP Calls with SRTP fail to connect with Cause Value=47 due to T.38 calls

Caveat ID Number	Description
<a href="#">CSCvr61217</a>	GetVPN-ISR4461// Getvpn traffic is failing with Transport mode with all the versions.
<a href="#">CSCvr65986</a>	ISR1K: dot1q-tunneling ports broadcast unknown unicast traffic to all other local switch ports
<a href="#">CSCvr76534</a>	ISR4k : Crash seen at Process Exec
<a href="#">CSCvr87906</a>	ISR4461: Large un-fragmented IPSEC packets cause router to crash
<a href="#">CSCvr89957</a>	CFT crashed frequently
<a href="#">CSCvr89973</a>	NIM interfaces go into shutdown after router bootup.
<a href="#">CSCvr93969</a>	C9800:ISSU: wncd crash@ crypto_engine_pk_crypto during ISSU downgrade scenario
<a href="#">CSCvr96597</a>	IOS-XE crash after doing a SCEP enrollment
<a href="#">CSCvr99034</a>	ISR 4K router crash during updating the OpenDNS bypass whitelist
<a href="#">CSCvs00410</a>	MKA session up but unable to pass data across link using AES-256-XPN cipher
<a href="#">CSCvs02000</a>	%IOSXE-3-PLATFORM: R0/0: kernel: DMA: Out of SW-IOMMU space
<a href="#">CSCvs04194</a>	Process = Exec crash seen on dmap longevity testbed with clear cry sa peer several times
<a href="#">CSCvs05043</a>	ESP40 crash in CGN mode after apply "ip nat setting mode cgn" and "no shut" interface
<a href="#">CSCvs07609</a>	Portchannel stats not working on ASR1002-HX
<a href="#">CSCvs08681</a>	Crash triggered with IPv6, IPv4, PPPoE, PortChannel and NAT
<a href="#">CSCvs09052</a>	ASR1K OTV: Incorrect MAC address count on EFP/BD QFP stats
<a href="#">CSCvs13960</a>	IWAN High CPU and Memory
<a href="#">CSCvs18317</a>	C1111X-8P Sku tagged to 4P software tag incorrectly
<a href="#">CSCvs29535</a>	IWAN crash related to DCA channel
<a href="#">CSCvs46484</a>	Standby RP2 crashes on ASR1009-X due to bulk sync in l2fib.
<a href="#">CSCvs60195</a>	ASR1K ucode crash after too many locks in ZBF pair setup
<a href="#">CSCvs70052</a>	ALG with NAT trigger a crash when a DNS writeback occurs
<a href="#">CSCvs86573</a>	Connect message is never forwarded to the calling side
<a href="#">CSCvs96719</a>	ASR1k: Unicast DHCPREQUEST dropped when received on a EoGRE tunnel configured with VRF

### Open Bugs for Cisco IOS XE Amsterdam 17.2.1r

All open bugs for this release are available in the [Cisco Bug Search Tool](#) through the Open Bug Search.

Caveat ID Number	Description
<a href="#">CSCvh24730</a>	PfRv3: Crash while Printing the Same TCA Message
<a href="#">CSCvp88044</a>	Performance Monitor crash
<a href="#">CSCvt15551</a>	Crash observed in QFP in ASR1001-X running 16.06.05 when GPM is running low
<a href="#">CSCvt33799</a>	Virtual address not reachable: "mac:0000:0c07:xxxx download to DP failed" for HSRP / VRRP over BDI.
<a href="#">CSCvs30625</a>	SRTP-RTP Crash on ASR with GCM Ciphers

## ROMmon Release Requirements

For more information on ROMmon support for Route Processors (RPs), Embedded Services Processors (ESPs), Modular Interface Processors (MIPs), and Shared Port Adapter Interface Processors (SIPs) on Cisco ASR 1000 Series Aggregation Services Routers, see <https://www.cisco.com/c/en/us/td/docs/routers/asr1000/rommon/asr1000-rommon-upg-guide.html>

## Related Documentation

- [Release Notes for Previous Versions of ASR 1000 Series Aggregation Services Routers](#)
- [Hardware Guides for Cisco ASR 1000 Series Aggregation Services Routers](#)
- [Configuration Guides for ASR 1000 Series Aggregation Services Routers](#)
- [Command Reference Guides for ASR 1000 Series Aggregation Services Routers](#)
- [Product Landing Page for ASR 1000 Series Aggregation Services Routers](#)
- [Datasheet for ASR 1000 Series Aggregation Services Routers](#)
- [Upgrading Field Programmable Hardware Devices for Cisco ASR 1000 Series Routers](#)
- [Cisco ASR 1000 Series Aggregation Services Routers ROMmon Upgrade Guide](#)
- [Field Notices](#)
- [Deferral Notices](#)
- [Cisco Bulletins](#)

