Release Notes for Cisco ASR 1000 Series, Cisco IOS XE 17.14.x

First Published: 2024-04-30

Full Cisco Trademarks with Software License

About Cisco ASR 1000 Series Aggregation Services Routers

The Cisco ASR 1000 Series Routers carry a modular yet integrated design, so network operators can increase their network capacity and services without a hardware upgrade. The routers are engineered for reliability and performance, with industry-leading advancements in silicon and security to help your business succeed in a digital world that's always on. The Cisco ASR 1000 Series is supported by the Cisco IOS XE Software, a modular operating system with modular packaging, feature velocity, and powerful resiliency. The series is well suited for enterprises experiencing explosive network traffic and network service providers needing to deliver high-performance services.

Note For more information on the features and specifications of Cisco ASR 1000 Series Routers, refer to the Cisco ASR 1000 Series Routers datasheet.

For information on the End-of-Life and End-of-Sale Announcements for Cisco ASR 1000 Series routers, refer to the ASR 1000 Series End-of-Life and End-of-Sale Notices.

Note Cisco IOS XE 17.14.1a is the first release for Cisco ASR 1000 Series Aggregation Services Routers in the Cisco IOS XE 17.14.x release series.

Product Field Notice

Cisco publishes Field Notices to notify customers and partners about significant issues in Cisco products that typically require an upgrade, workaround or other user action. For more information, see https://www.cisco.com/c/en/us/support/web/field-notice-overview.html.

We recommend that you review the field notices to determine whether your software or hardware platforms are affected. You can access the field notices from https://www.cisco.com/c/en/us/support/web/tsd-products-field-notice-summary.html#%7Etab-product-categories.

New and Changed Hardware Features

There are no new hardware features for this release.

New and Changed Software Features in Cisco IOS XE 17.14.1a

Feature	Description
DC-PE Router in Cisco ACI to SR-MPLS Hand-off	From Cisco IOS XE 17.14.1a, Cisco ASR 1000 Series Aggregation Services Routers and Cisco Catalyst 8500 Series Edge Platforms can be used as intermediate DC-PE devices in Cisco ACI to SR-MPLS hand-off interconnection. SR-MPLS hand-off is an interconnection option that enables Cisco ACI to WAN interconnect using Segment Routing (SR) MPLS underlay.

Feature	Description
Enhanced IS-IS Fast Flooding	The IS-IS Fast Flooding feature optimizes LSP transmission to accelerate netwo convergence by dynamically adjusting the LSP rate based on receiver capability From Cisco IOS XE 17.14.1a, IS-IS Fast Flooding can be configured using the **router isis lsp-fast-flooding** command. The LSP transmission can be further customized with arguments such as **max-lsp-tx**, **psnp-interval**, and **per-interfa** within the same router isis command, and enhanced by using the **isis remote-psnp-delay** command. This feature is disabled by default, and requires manual configuration to enable.
Enhancement to the **show reload-history** Command	From Cisco IOS XE 17.14.1a, the **show reload-history** command is modified t **show reload history**. The output for the command is updated to include crash da Cisco High Availability (HA) status, and software version.
Increase in L2TPv3 Scalability	From Cisco IOS XE 17.14.1a, the capacity for unidimensional scalability of L2TP tunnel is increased to 12,000 for the following platforms: • Cisco ASR 1000 Series Aggregation Services Routers using RP3 with ESP200-X and ESP100-X • Cisco Catalyst 8500 Series Edge Platforms The scalability is increased to 8000 for Cisco Catalyst 8500L-8S4X Platform.
IP Endpoint Delay Measurement and Liveness Monitoring	This feature enables you to measure the end-to-end delay and monitor liveness towards either a specified IPv4 or IPv6 endpoint. From Cisco IOS XE 17.14.1a, you can be configure this feature using the performance-measuremen endpoint and performance-measurement delay-profile endpoint commands.
QFP Drops Threshold and Warning	From Cisco IOS XE 17.14.1a, this feature enables you to configure the warning threshold for each drop cause, and the total QFP drop in packets per second. If t configured threshold exceeds, then a rate-limited syslog warning is generated. Y can configure the threshold using the **platform qfp drops threshold** command

Feature	Description

Support for Suite B Ciphers with GET VPN	From Cisco IOS XE 17.14.1a, this enhancement introduces support for Suite B ciphers with GET VPN on the following platforms and its corresponding models:
	• Cisco ASR 1000 Series Aggregation Services Routers:
	  • ASR 1000 with ESP100-X
	• Cisco Catalyst 8300 Series Edge Platforms:
	  • C8300-1N1S-4T2X
	  • C8300-2N2S-6T
	• Cisco Catalyst 8200 Series Edge Platforms:
	  • C8200L-1N-4T
	• Cisco Catalyst 8500 Series Edge Platforms:
	  • C8500-12X4QC
	  • C8500L-8S4X
	• Cisco 1000 Series Integrated Services Routers:
	  • C1131
	  • C112X
	  • C116X
	  • C111X

Configuration Group Enhancements	This release introduces support for the following in Cisco SD-WAN Manager: • Transport Profiles • Management Profile • Service Profile • CLI Profile • Policy Object Profile

Feature	Description
Support to Configure VPN Solutions for SD-Routing devices	This release introduces support for the following VPN solutions: • FlexVPN • GETVPN • DMVPN • L3VPN These VPN solutions can be configured by using **Configuration** > **Configurati Groups** > **CLI Add-on Profile** option in Cisco SD-WAN Manager.
YANG Configurational Model Support for SD-Routing Devices	This release introduces support for the following YANG Configurational Mode • BGP • MPLS • RSVP • SNMP • AAA • QOS • ACL • DHCP
View Unmodelled Commands on SD-Routing Devices	After an SD-Routing device is deployed, you can view the unmodelled comman on Cisco SD-WAN Manager. The list of unmodelled commands are regenerated the device reboots
Configure Secure Service Edge	Secure Service Edge is a cloud solution that provides seamless, transparent, and secure Direct Internet Access (DIA) to protect against internet-based threats. Tl solution can be configured through Policy Groups by using Cisco SD-WAN Manager.
Voltage and Current Metrics	Power Entry Module (PEM) sensors are critical components in the device that a responsible for monitoring various aspects of the power supply, such as voltage current, and sometimes temperature, to ensure the device operates within safe a efficient parameters. From Cisco IOS XE 17.14.1a, you can use the show environment command to display the PEM sensor readings in mV (milli-volt) a mA (milli-ampere) for your devices.
Programmability Features	
gNMI: Stream Subscriptions with On-Change Mode	gNMI telemetry supports on-change subscriptions on the same set of models as other telemetry protocols.
gNMI - SubscribeResponse with sync_response	The sync_response is a boolean field that is part of the SubscribeResponse respon message. The sync_response message is sent after the first update message.

Feature	Description
Cisco Unified Border Element (CUBE) Features	
Secure SIP with TLS 1.3 support	From Cisco IOS XE 17.14.1a onwards, security of the communication between the client and the server is enhanced with the support of Transport Layer Security (TLS) version 1.3 and associated cipher suites.

Resolved and Open Bugs for Cisco IOS XE 17.14.x

Resolved Bugs for Cisco IOS XE 17.14.1a

Identifier	Headline
CSCwh94906	Device WLC segmentation fault crash with Network Mobility Services Protocol (NMSP).
CSCwi49846	ftmd crashed when SIG GRE tunnels configs are removed.
CSCwi55725	CLI config group issue.
CSCwi61369	Device may unexpectedly reload due to SIGABRT.
CSCwi35716	AAR backup preferred color not working as expected.
CSCwi53306	Unknown appID in ZBFW HSL log.
CSCwf84567	Unexpected reload after reconnecting.
CSCwi14178	Failed to connect to device: x.x.x.x Port: 830 user: vmanage-admin error: Connection failed.
CSCwj25493	Device crashed twice with Critical process linux_iosd_image fault on rp_0_0
CSCwi40603	Memory leak in the Crypto IKMP process.
CSCwf08658	Edge devices will flap the BFD sessions if we are in a non-equilibrium state and have symmetric NAT.
CSCwi35177	Device crash caused by continuous interface flap, interface associated with many IPSec interfaces.
CSCwj34010	TLOC extension is missing on the interface in device leading to incorrect control.
CSCwi60266	Device with enterprise certificates not forming control connections with controllers after upgrade.
CSCwi67983	Tracker state log is missing when DNS Query fails.
CSCwi53951	Packets with Unicast MAC get dropped on a Port Channel L2 Sub-intf after a device reboot.
CSCwb25507	CWMP: Add vendor specific parameter for NBAR protocol pack version.

Identifier	Headline
CSCwi53549	Device crash with reason: Critical process fman_fp_image fault on fp_0_0 (rc=134).
CSCwi82548	Crash in IKEv2 Cluster Load Balancer.
CSCwi51381	TrapOID of CISCO-BFD-STATE-CHANGE is different from MIB file.
CSCwh09033	Device unable to boot with module.
CSCwf00276	Packets with L2TP headers cause device to crash.
CSCwi78365	Trim installed certificate on upgrade.
CSCwi85293	IKEv2 IPv6 Cluster Load balance: Secondary in cluster unable to connect to cluster in case of FVRF.
CSCwi86698	No error message while using multicast address as system-ip in device.
CSCwj06622	Segmentation fault and core files are seen on OS in controller-managed due to speedtest.
CSCwi16111	IPv6 TCP adjust-MSS not working after delete and reconfigure.
CSCwi62230	SIG tunnel: 'SIG STATE' is showing blank value.
CSCwf98902	Unexpected reboot on OS during longevity test.
CSCwj27545	Device crashing due to ftmd.
CSCwi62239	%MGMTVRF-3-INTF_ATTACH_FAIL error after configuring loopback management VRF then removing it.
CSCwj70773	Unable to create a portchannel interface with maximum number limit

Open Bugs for Cisco IOS XE 17.14.1a

Identifier	Headline
CSCwj04575	Device crashed during SNMPwalk when removing SFP.
CSCwj25508	Device reports incorrect DOM values over SNMP.
CSCwj48393	Service with no priority is not working as expected.
CSCwj48421	%CRYPTO-4-RECVD_PKT_INV_SPI: decaps: received IPSEC packet has an invalid SPI.
CSCwj03621	Ping with smaller packet size is failing on MACSEC enabled port.
CSCwj09284	Unexpected reboot in device due to SSL.
CSCwj40589	Endpoint tracker using DNS does not log DOWN message when DNS server reachability is lost.
CSCwj26085	Control connections in TLS with mode manage goes to trying state with UTD.

Identifier	Headline
CSCwj45177	"dmidecode: command not found" error seen executing **show certificate validity**.
CSCwj34578	NAT46 translations are dropped when device is also Carrier Supporting Carrier CE.
CSCwi81026	BFD Sessions Flapping During IPSEC Rekey in Scaled Environment.
CSCwj45130	Segmentation Fault - Process = IPSEC dummy packet process.
CSCwi59854	**show policy service-path** command gives inconsistent results with app name specified.
CSCwj02661	UTD signature update failure and device not recording the update.
CSCwj43905	Unexpected reboot due to uCode failure.
CSCwj02628	Speed-test not working for the device.
CSCwi77159	Some of the objects of CISCO-SDWAN-APP-ROUTE-MIB are not implemented.
CSCwj40223	AppRouteStatisticsTable sequence misordered in CISCO-SDWAN-APP-ROUTE-MIB or OS returns the wrong order.
CSCwj49946	Device | cpp-mcplo-ucode | None PPPoE get session.
CSCwj32347	DIA Endpoint tracker not working with ECMP routes when Loopback is used as Source.
CSCwj27108	Device not balancing traffic to default route.
CSCwj49941	DNS-snoop-agent has TCAM entry with all zeros for some regex patterns.
CSCwj31354	Template push failure due to service timestamps.
CSCwj30334	CVLA uCode crash when attempting merge on used block.
CSCwj13681	Device can only store 64 FQDN patterns, but the configuration allows entry of more than 64.

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.

Note After upgrading the ROMmon to version 17.3(1r), you cannot revert it to a version earlier than 17.3(1r) for the following platforms:

- ASR 1001-HX
- ASR 1002-HX

This restriction is only applicable for these platforms. If you have upgraded to ROMmon version 17.3(1r) on any other platform, reverting to an earlier version of ROMmon is permitted and does not cause any technical issues.

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
- 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
- Cisco Bulletins

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.

Documentation Feedback

To provide feedback about Cisco technical documentation, use the feedback form available in the right pane of every online document.

Troubleshooting

For the most up-to-date, detailed troubleshooting information, see the Cisco TAC website at https://www.cisco.com/en/US/support/index.html.

Go to **Products by Category** and choose your product from the list, or enter the name of your product. Look under **Troubleshoot and Alerts** to find information for the issue that you are experiencing.