Release Notes for Cisco ASR 1000 Series, Cisco IOS XE Bengaluru 17.4.x

First Published: 2020-12-18

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 The In-Service Software Upgrade(ISSU) in ASR 1000 is being migrated to an install workflow that provides a step-by-step upgrade/downgrade. Starting from IOS-XE 17.6.1 the following items will be disabled:

- The ISSU load version command set including **issu loadversion** , **issu runversion** , **issu acceptversion** and **issu commitversion**
- Dual IOSd ISSU commands
- Bundle mode ISSU workflow

Note Starting with Cisco IOS XE 17.3.x, with the introduction of Smart Licensing Using Policy, even if you configure a hostname for a product instance or device, only the Unique Device Identifier (UDI) is displayed. This change in the display can be observed in all licensing utilities and user interfaces where the hostname was displayed in earlier releases. It does not affect any licensing functionality. There is no workaround for this limitation.

The licensing utilities and user interfaces that are affected by this limitation include only the following:

- Cisco Smart Software Manager (CSSM),
- Cisco Smart License Utility (CSLU), and
- Smart Software Manager On-Prem (SSM On-Prem).

New and Enhanced Software Features for Cisco IOS XE Bengaluru 17.4.X

Table 1: New Software Features in Cisco ASR 1000 Series Release Cisco IOS XE 17.4.x

Feature	Description
NBAR Support on the EVC Service Instance	To classify the data packets, enable NBAR FIA-trace data for NBAR on the EFP interface. Quality of service (QoS) takes action on the output interface based on the NBAR traffic classification result..
EVPN Over MPLS with Distributed Anycast Gateways	Distributed anycast gateway (DAG) is a default gateway addressing mechanism in a BGP EVPN fabric. This feature enables the use of same gateway IP and MAC address across all the devices in an EVPN over MPLS network. This ensures that every device functions as the default gateway for the workloads directly connected to it. Additionally, it also, facilitates flexible workload placement, host mobility, and optimal traffic forwarding across the BGP EVPN fabric.
Configure Performance Measurement	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.
Link Aggregation Group compatibility with Service Group	QOS policy is now extended on L2VPN, L3VPN and service-group together on port-channel interface.

Feature	Description
Show commands for troubleshooting	The following command are added for troubleshooting CPU and memory usage: • **show processes cpu** • **show processes memory** • **show avc sd-service info summary** • **show avc sd-service info detailed | inc DCS** • **show processes cpu** • **show processes memory** • **show version**
Micro BFD Support with LACP	Micro-BFD, which is supported for the physical member-links within a port-channel is now configured to receive BFD events and to create BFD sessions per member-link. The member-links can now receive BFD events after you enable Micro-BFD for the port-channel member-links.
Configuring Smart Licensing using Web UI	You can use the Web UI to configure Smart Licensing on Cisco ASR 1000 platforms. For more information, see *Web UI Online Help*.
Configuring the Same Global Address for Static NAT and PAT	You can now configure the same global address within static NAT and static PAT. This configuration is supported only on outside static NAT.
BGP Large Community	The BGP large communities support a routing policy to control the distribution of routing information. The BGP large communities attribute provides the capability of tagging routes and modifying BGP routing policy on the device. BGP large communities can be appended or removed selectively on the large community attribute as the route travels from device to device.
Configuring Stateless Static NAT	Static Network Address Translation (NAT) allows the user to configure one-to-one translations of the inside local addresses to the outside global addresses. A new keyword stateless is introduced for Cisco IOS XE static NAT configuration and it applies only to static NAT command. When the static mapping is set to stateless, no sessions will be created for that traffic flow.

New and Enhanced Software Features for Cisco CUBE

Feature	Description
Hunt Stop for Server Groups	Server groups allow you to create simpler configurations by specifying a list of destination SIP servers for a single dial peer. When a call matches a dial peer that is configured with a server group, the destination is selected from the list of candidates based on a configured policy. If it is not possible to complete that call, the next candidate is selected. Alternatively, you can also choose to stop hunting through the group if a specified response code is received. If the call cannot be placed to any of the servers in the group, or hunting is stopped, call processing continues to the next preferred dial-peer.
VoIP Trace Serviceability Framework	VoIP Trace is a Cisco Unified Border Element (CUBE) serviceability framework, which provides a binary trace facility for persistently monitoring and troubleshooting SIP call issues. The VoIP Trace framework records both successful and failed calls. All call trace data is stored in system memory. In addition, data for calls with IEC errors is written to the logging buffer.
Smart License Using Policy	Smart Licensing using Policy reports license usage periodically based on an account policy, rather than requesting licenses based on past usage as in previous releases. Evaluation mode and license reservation are not supported. Frequent license requests used to go out from a device to CSSM in earlier versions. In the changed scenario, minimum reporting license usage is 8 hours. Now all the devices within a network follow the uniform approach of reporting their license usage to Smart Agent. The Smart Agent in turn creates a Resource Utilization Monitoring (RUM) report and dispatches to CSSM based on the Smart Agent reporting policy.
Clear Hung RTP Ports	When establishing a call, CUBE allocates several RTP ports that are based on the media that are negotiated for the session. Some ports remain assigned even after the call ends. In the current behavior, show voip rtp statscommand displays only the ports allocated from the global table, even if the ports are allocated from all the three tables (Global port, media IP address-based, and media VRF-based). Now this command is enhanced to display the ports allocated from all the three tables. The command also displays the hung ports and allows you to release those ports. Releasing the hung ports increases the efficiency of the routers as more ports are available to receive calls.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a gateway to the Cisco bug-tracking system, which maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. The BST provides you with detailed defect information about your products and software.

Resolved Bugs for Cisco IOS XE Bengaluru 17.4.2

Caveat ID Number	Description
CSCvw68171	Duplicate Bytes & Packet when Q in Q is configured
CSCvw11607	Crash in DSP causing an mcpcc-lc-ms core file

Open Bugs for Cisco IOS XE Bengaluru 17.4.2

Caveat ID Number	Description
CSCvw84883	DDNS feature triggers crash on 16.X/17.X releases due to memory corruption

Resolved and Open Bugs for Cisco IOS XE Bengaluru 17.4

Resolved Bugs for Cisco IOS XE Bengaluru 17.4

Caveat ID Number	Description
CSCuv97577	Mishandling of dsmpSession pointer causes a crash
CSCvt21732	On cEdge; cli output for zbfw statistics showing error
CSCvt53843	ucode crash on ESP-100 with CAPWAP traffic when CAPWAP stripping is enabled
CSCvt89441	IOS-XE device crashed with CGD shared memory corruption freed by FMAN-FP
CSCvu07639	UTD policy on global VPN does not work properly for DIA traffic
CSCvu10006	Performance monitor caused QoS miss classification
CSCvu11066	Umbrella custom dns config not in sync between confd and ios
CSCvu11115	IOS-XE MTP Fails to Interwork DTMF RFC2833 from Payload 100 to Payload 101
CSCvu22003	vManage FW dashboard doesn't show all matched applications
CSCvu27953	Crash due to a segmentation fault in the "IPsec background proc" process
CSCvu34009	Calls going through T1 are rejected with "no dsps found" Analog/TDM Hairpin calls
CSCvu34381	Packets are not dropped as expected in selfzone to zone vpn 0 firewall config
CSCvu43248	%IP-4-DUPADDR: Duplicate address issue at NAT-HSRP ISR4k router
CSCvu65669	Traffic drop from branch overlay ping to service side without zp vpn1 to vpn1 when FW & IPS enabled
CSCvu70571	SDWAN router ASR1001-X crashes when object-group service configuration is added
CSCvu77745	PMAN-3-PROCFAIL: Chassis 1 R0/0: pman: R0/0: The process keyman has failed (rc 139)
CSCvu89033	Template push error due to NAT-MIB process helper traceback/warm restart
CSCvu92879	Huge amount of Crypto PKI RECV memory leaks keep increasing during clients' SCEP enrollments.
CSCvv03229	Crash in sre_dp_traverse_dfa_legacy as SIP invite messages crosses a GRE Tunnel
CSCvv03800	ASR1002X lost all configuration after upgrade from 16.12 to 17.3

Caveat ID Number	Description
CSCvv04236	IOS-XE: IPv6 OSPF authentication ipsec - adjacency fails
CSCvv08341	Netconf deleting wrong IKEv2 parameters
CSCvv12401	ZBFW HA redundancy stuck in STANDBY-COLK-BULK. Bulksync Traceback seen in logs
CSCvv20380	Removing and Adding Bulk ACL leads to Tracebacks and Error-Objects
CSCvv26538	Crash due to a NULL pointer while bringing down PPPoE sessions.
CSCvv36247	Memory Leak in MallocLite / Crypto IKMP
CSCvv47691	Reload: IOS-XE router crashing due to DN mismatch
CSCvv58312	17.4 : Dataplane Crash due to driver cpp_drv_i95_read_cb observed on 4461 with traffic
CSCvv79273	Router may crash when using Stateful NAT64
CSCvv82330	When large number of policies are applied to a ASR1001-X running 17.3.1, traffic is dropped.
CSCvv83345	Summary/default-map routes getting ignored for p2p interface
CSCvw06719	"platform ipsec reassemble transit" tail-drops unencrypted IPv4 Fragments with specific payload
CSCvw56517	LMR Unable to hear first seconds of audio

Open Bugs for Cisco IOS XE Bengaluru 17.4

Caveat ID Number	Description
CSCvt58920	SIM failover within the same modem takes long time to detect LTE network for AT&T
CSCvw67128	SL Policy: purchase info should be protected and shouldn't be able to erase
CSCvu97660	dataplan crash seen at pppoe
CSCvv25049	Number of EoGRE sessions count are not matching on fugazi
CSCvv37866	Fluctuation of around 5-10% is seen in perf with IMIX profile in ESP100x/ESP200x with NBAR and FWALL
CSCvv54152	CDP on interfaces is not enabled when CDP is enabled globally on ASR Routers in controller mode
CSCvv78028	No responder-bytes from cEdge when UTD is enabled
CSCvv94743	Data Plane fails over L2TPv3 while disabling VLAN limit restrictions with ASR1002-HX

Caveat ID Number	Description
CSCvw11902	Passive FTP doesn't work with NAT
CSCvw13048	crash observed at NHRP while using summary-map
CSCvw13682	L3 connected lite session not coming up , stuck in data-plane(qfp)
CSCvw33113	Unexpected reload in NHRP when access to an invalid memory region
CSCvw34157	APPNAV CFT Crashes
CSCvw36629	cEdge: NATed tuple flips for HSL deleted flow
CSCvw39383	CPP ucode crash with fw_base_flow_create
CSCvw45264	Crash due to stuck thread while mpass function
CSCvw47640	ASR 1000 doing KS role for GETVPN is sending malformed rekey packets
CSCvw47800	HSL Export over VASI Interface causes Netflow v9 Template Flooding
CSCvw48800	unable to transfer 1500 byte IP packet when using BRI bundled Multilink
CSCvw48943	crypto ikev2 proposals are not processed separately
CSCvw54076	[SIT]: BFD sessions not established between Edges, with UTD enabled
CSCvw58560	FlexVPN reactivate primary peer feature does not work with secondary peer tracking
CSCvw62805	SDWAN ZBFW CPU punted traffic mishandling -- Out2In packet looped
CSCvw63366	telnet to SN from WCM after upgrade the CSR1k 17.3 to 17.4 CSR8k from vManage
CSCvw70009	ASR1K: fman_rp crash seen on 16.9.X when "show platform software nat RP active logging" is run
CSCvw70461	17.4 ZBFW:Classification of traffic not happening correctly sometimes when a rule in RS is edited.
CSCvw71941	QFP crash in cpp_ess_tc_tgt_if_fm_edit_helper
CSCvw73701	17.4 ZBFW:Stale ACL entries seen on ASR1K
CSCvw74921	APPNAV CFT crash on ISR

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-X
- 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
- 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

© 2020 Cisco Systems, Inc. All rights reserved.