Release Notes for Cisco ASR 1000 Series, Cisco IOS XE 17.13.x

First Published: 2023-12-16

Full Cisco Trademarks with Software License

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

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 17.13.1a is the first release for Cisco ASR 1000 Series Aggregation Services Routers in the Cisco IOS XE 17.13.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 17.13.1a

Feature	Description
Application Performance Monitor	The Application Performance Monitor feature is a simplified framework that ena intent-based performance monitors. With this feature, you can view real-time, en performance filtered by client segments, network segments, and server segments

Feature	Description
Cisco SD-Routing Cloud OnRamp for Multicloud	Cisco SD-Routing Cloud OnRamp for Multicloud extends enterprise WAN to pu solution helps to integrate public cloud infrastructure into the Cisco Catalyst these capabilities, the devices can access the applications hosted in the cloud.
Disable multi-part TLVs for ISIS	From Cisco IOS XE 17.13.1a, you can disable multi-part TLVs for prefix-rea and (MT)IS-Neighbor in ISIS by using the **multi-part-tlv disable** command.
Enhancements to BGP Maximum Prefix	• Discard Extra Prefixes: This enhancement introduces the **neighbor maxi** command to drop all excess prefixes received from the neighbor when th prefixes exceed the maximum limit. • Logging enhancement: The logging system is enhanced to support a per n 60 seconds.
Initiating GARP for NAT Mapping	This feature introduces support for configuring retry time intervals for GARP interface. You can configure this feature using the global **ip arp nat-garp-ret static** commands.
Schedule Software Upgrade on SD-Routing Devices	With this feature, you can upgrade the software image on the supported Cisc an option to schedule the upgrade process at specified time. This allows you t to the software upgrade process.
SD-Routing Configuration Group	The Configuration Group feature provides a simple, reusable, and structured SD-Routing device using Cisco Catalyst SD-WAN Manager.
Segment Routing over IPv6 Dataplane	From Cisco IOS XE 17.13.1a, Segment Routing is supported over the IPv6 da Protocol (BGP) on L3VPN networks using On-Demand Next Hop (ODN).
Speed Test for SD-Routing Devices	Cisco SD-WAN Manager allows you to measure the network speed and avail device and an iPerf3 server. The speed tests measure upload speed from the s or specified iPerf3 server, and measure download speed from the iPerf3 serve
Strength Enforcement for IKE Security Association (SA)	This feature ensures that the strength of the IKE (IKEv1 and IKEv2) SA encry or equal to the strength of its child IPsec SA encryption cipher. To enable this feature, use the **crypto ipsec ike sa-strength-enforcement** co
Support for Flexible NetFlow Application Visibility on SD-Routing Devices	The Flexible NetFlow (FNF) feature provides statistics on packets flowing th to identify the tunnel or service VPNs. Also, it provides visibility for all the tra VPN0 on Cisco SD-Routing devices by using the Application Intelligence En
Support for Packet Capture for SD-Routing	This feature allows you to capture the bidirectional IPv6 traffic data to troubl SD-Routing devices.
Support for Persistence of BGP Dynamic Neighbors	From IOS XE 17.13.1a, the device maintains the neighbor information even aft To configure this, use the **bgp listen persistent** command for all dynamic neig **peer-group persistent** command for specific neighbors.
Support for Security-Enhanced Linux	SELinux (Security-Enhanced Linux) is a solution designed to incorporate a s access control (MAC) architecture into Cisco IOS XE platforms. From Cisco IOS XE 17.13.1a, SELinux is enabled by default in Enforcing m platforms.

Feature	Description
Support for Suite B ciphers with GET VPN	This enhancement introduces support for Suite B ciphers with GET VPN on the fo • Cisco ASR 1000 Series Aggregation Services Routers • ASR1009-X + ESP200-X • Cisco Catalyst 8000V Edge Software • Cisco Catalyst 8200 Series Edge Platforms • C8200-1N-4T • Cisco Catalyst 8300 Series Edge Platforms • C8300-2N2S-4T2X • C8300-1N1S-6T • Cisco Catalyst 8500 Series Edge Platforms • C8500-12X • C8500-20X6C
Using VASI in NTPv6 Environment	You can use the VRF-Aware Software Infrastructure Scale feature in the NTPv6 inter-VRF communication, such as access control lists (ACLs), Network Address policing, and zone-based firewalls, for MPLS traffic or IPv4 and IPv6 traffic flow Virtual Routing and Forwarding (VRF) instances. The VASI interfaces support re Processor (RP) and Forwarding Processor (FP).
View Packet Drops History	From Cisco IOS XE 17.13.1a, you can use the **show drops history qfp** comman the QFP drops on the Cisco ASR 1000 Series and Catalyst 8500 Series Edge Plat
Cisco Unified Border Element (CUBE) Features	
NAT Traversal using RTP Keepalive	From Cisco IOS XE 17.13.1a onwards, using RTP keepalive packets, CUBE supp in the NAT environment.

Resolved and Open Bugs for Cisco IOS XE 17.13.x

Resolved Bugs for Cisco IOS XE 17.13.1a

Bug ID	Description
CSCwh10813	Add a verbose log to indicate that grant ra-auto unconfigures the grant auto in the PKI server.
CSCwf25735	QoS more than four remark with set-cos does not work.
CSCwf44703	NAT64 prefix is not originated into OMP.
CSCwf14607	Crash observed exporting PKCS12 to terminal via SSH CLI.

Bug ID	Description
CSCwf71116	Static route keep advertising via OMP even though there is no route.
CSCwf45486	OMP to BGP Redistribution leads to incorrect AS_Path installation on chosen next-hop.

Open Bugs for Cisco IOS XE 17.13.1a

Bug ID	Description
CSCwh94906	Segmentation fault crash with Network Mobility Services Protocol (NMSP).
CSCwh84068	Device crash after changing NAT HSL configuration.
CSCwh77221	SNMP unable to poll SDWAN tunnel data after a minute.
CSCwh92627	Device port-channel stuck IHQ after remote LC flap.
CSCwi15930	Device failing to upgrade due to CDB issue.
CSCwi06843	Endpoint tracker triggers a CPU hog.
CSCwh76453	Tracker for TLOC extension is down even though TLOC is up and there is ICMP reachability.
CSCwi14178	Failed to connect to device : x.x.x.x Port: 830 user : vmanage-admin error : Connection failed.
CSCwi08171	Router may crash due to Crypto IKMP process.
CSCwh01678	Platform FTM crash with SIG enabled.
CSCwi05395	snmpbulkget cannot get loss, latency and jitter for ProbeClassTable & ClassIntervalTable OIDs.
CSCwi23562	When RADIUS down, and there is an IKE-AUTH request received, the device stops replying to DPD packets.
CSCwi21548	EntSensorStatus is displaying as Nonoperational when Iin and Iout value is 0 Amps.
CSCwi11807	snmpbulkget breaks the OID appRouteStatisticsTable after minute not returning the correct order.
CSCwi00369	Device lost security parameter after upgrade.
CSCwi06404	Device PKI related crash after failing a CRL Fetch.
CSCwi13563	IP SLA probe for End-point-tracker doesnt work once endpoint tracker is changed until reload.
CSCwh45579	Unexpected reload on device UCode core @l2_dst_output_goto_output_feature_ext_path.
CSCwh65016	Unexpected reboots on device due to QFP exception.

Bug ID	Description
CSCwh45169	Unexpected reboot while dispalying information from cleared SSS session.
CSCwi15688	Unexpected NAT translation occurs in a specific network.
CSCwf00276	Packets with L2TP headers causes device to crash.
CSCwe54687	After removing the USB from the device, the files copied to it will be deleted.
CSCwh91136	Traffic not encrypted and droped over IPSEC SVTI tunnel.
CSCwh89618	CRC errors seen with MACsec enabled on 100G ports.
CSCwi16015	SSE tunnels don't come up with Dialer interface. Relax check in IKE.
CSCwi22584	Device LACP Stays in SUSP state after link flap.
CSCwi19875	Device is unable to process hidden characters in a file while trying to use bootstrap method.
CSCwh50380	Continuous trackeys at process: sessmgrd_rp_0.
CSCwh52440	IP SLA doesn't have checks for ICMP probes to be sent on source interface.
CSCwh65973	CLI template attach fails to config **encapsulation aal5mux ppp dialer** under DSL ATM.
CSCwh73587	Unable to configure PPPoE-client under ATM PVC.
CSCwi35177	Router crash caused by continuous interface flap, interface associated to many IPSec interfaces.
CSCwh73573	**show ppp al** displays PPP-Server IP even though no IP is configured on BRAS/PPP-Server.
CSCwi30529	Template push fail when AAA authorization is set to local.

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
- 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.

© 2023 Cisco Systems, Inc. All rights reserved.