Release Notes for Cisco ASR 1000 Series, Cisco IOS XE Cupertino 17.7.x

First Published: 2021-12-17

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.

Cisco ASR 1000 Series Routers are available in this options:

- Cisco ASR 1001-X Router
- Cisco ASR 1002-X Router
- Cisco ASR 1001-HX Router
- Cisco ASR 1002-HX Router
- Cisco ASR 1004 Router
- Cisco ASR 1006 Router
- Cisco ASR 1006-X Router
- Cisco ASR 1009-X Router
- Cisco ASR 1013 Router

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

Note Cisco IOS XE Cupertino 17.7.1a is the first release for Cisco ASR 1000 Series Aggregation Services Routers in the Cisco IOS XE Cupertino 17.7.x release series.

Note Starting from IOS XE 17.5, the following consolidated platforms (or with dual IOSd) will move to monolith packaging and will not enable upgrade/downgrade using separate packages:

- ASR 1001-X
- ASR 1001-HX
- ASR1002-X
- ASR 1002-HX

Instead, use the **install add file bootflash:<file name> activate commit** command to upgrade using a single image that combines all the separate packages improves the boot time.

Starting from IOS XE 17.6, the ISSU on Cisco ASR 1000 Series Aggregation Services Routers will migrate to an install workflow that provides step-by-step upgrade/downgrade commands.

The ISSU load version commands will be deprecated and these commands include:

- abortversion
- acceptversion
- checkversion
- commitversion
- config-sync
- image-version
- loadversion
- runversion.

Additionally, dual IOSd ISSU commands and Bundle mode ISSU workflows will also be disabled.

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.

New and Changed Software Features

Table 1: New Software Features in Cisco ASR 1000 Series Release Cisco IOS XE 17.7.1a

Feature	Description
Attaching Extended Color Communities to BGP VRF	This feature introduces new methods of attaching extended color communities to a prefix. A color community is an indicator of the bandwidth or latency level of the traffic being sent to the prefix and these are following new ways of attaching them to the prefix: VRF export coloring, VRF import coloring, Route Redistribution coloring into BGP and Neighbor inbound coloring.
EVPN VPWS over Preferred Path Fallback Disable	This enhancement allows you to configure an EVPN-VPWS over a preferred path using SR-TE policy. The command **preferred-path segment-routing traffic-eng policy** includes the fallback disable option, which allows you to configure fallback behaviour.
Flexible NetFlow Support on BD-VIF	This feature introduces Flexible NetFlow (FNF) support on Bridge Domain Virtual IP Interfaces (BD-VIF). Flexible Netflow provides improved optimization and performance, enhanced security, and increased flexibility and scalability to the network. You can configure FNF on a BD-VIF using the ip flow monitor command.
Multicast group calculation	The show ip multicast overlay-mapping command displays an underlay group address from the overlay group address which is used to troubleshoot or configure the network. The output includes the underlay group address that is within the configured SSM (Source Specific Multicast) address range.
Support For Autoroute Announce On ISIS	Autoroute announcement is a method to steer traffic away from congested links and therefore, helps to use the network efficiently. This enhancement provides ISIS as an alternative routing protocol for the autoroute announce feature that currently uses only OSPF.
Support for EVPN over MPLS IRB Multi-Homing	This feature enables redundant network connectivity via Multihoming by allowing a CE device to connect to more than one PE device therefore preventing disruptions in the network. This Multihoming IRB solution is supported on Cisco ASR 1000 routers through the following features: • IPv4 and IPv6 MAC-IP Binding • ARP and ND Synchronization • MAC-IP Proxy Route • L3 ECMP via MAC-IP Proxy Route • MAC-IP Mobility • Host discovery via subnet prefix • ARP and ND flooding suppression

Feature	Description
Tunnel protection for IPIP with NAT-T	When you configure the tunnel protection on an IPIP tunnel, the NAT-T configuration on the IPsec tunnel works as expected. However, the incoming packets are not processed though the Internet Security Association and Key Management Protocol and IPsec Security Association are correctly generated. To ensure that the tunnel protection on the IPIP tunnel works seamlessly, configure the tunnel mode GRE IP on both endpoints.
Cisco Unified Border Element (CUBE) Features	
YANG Configuration Models for CUBE	From IOS-XE Cupertino-17.7.1a, YANG models are now available to configure and manage CUBE.
YANG Model Version 1.1	Cisco IOS XE Cupertino 17.7.1a uses the YANG version 1.0; however, you can download the YANG version 1.1 from GitHub at https://github.com/YangModels/yang/tree/master/vendor/cisco/xe folder. For inquiries related to the migrate_yang_version.py script or the Cisco IOS XE YANG migration process, send an email to xe-yang-migration@cisco.com.
ZTP Configuration through YANG	ZTP is enabled through YANG models when NETCONF is enabled.
Programmability Features	
Converting IOS Commands to XML	This feature helps to automatically translate IOS commands into relevant NETCONF-XML or RESTCONF/JSON request messages.
Smart Licensing Using Policy Features	
Ability to save authorization code request and return in a file and simpler upload in the CSSM Web UI	If your product instance is in an air-gapped network, you can now save an SLAC request in a file on the product instance. The SLAC request file must be uploaded to the CSSM Web UI. You can then download the file containing the SLAC code and install it on the product instance. You can also upload a return request file in a similar manner. With this new method you do not have to gather and enter the required details on the CSSM Web UI to generate an SLAC. You also do not have to locate the product instance in the CSSM Web UI to return an authorization code. In the CSSM Web UI, you must upload the SLAC request or return file in the same way as you upload a RUM report. In the required Smart Account, navigate to **Reports** → **Usage Data Files**. See: No Connectivity to CSSM and No CSLU, Workflow for Topology: No Connectivity to CSSM and No CSLU, Saving a SLAC Request on the Product Instance, Removing and Returning an Authorization Code, Uploading Data or Requests to CSSM and Downloading a File
Account information included in the ACK and show command outputs	A RUM acknowledgement (ACK) includes the Smart Account and Virtual Account that was reported to, in CSSM. You can then display account information using various **show** commands. The account information that is displayed is always as per the latest available ACK on the product instance. See: show license summary, show license status, show license tech.

Feature	Description
CSLU support for Linux	CSLU can now be deployed on a machine (laptop or desktop) running Linux. See: CSLU, Workflow for Topology: Connected to CSSM Through CSLU, Workflow for Topology: CSLU Disconnected from CSSM.
Factory-installed trust code	For new hardware and software orders, a trust code is now installed at the time of manufacturing. **Note** You cannot use a factory-installed trust code to communicate with CSSM. See: Overview, Trust Code.
RUM Report optimization and availability of statistics	RUM report generation and related processes have been optimized. This includes a reduction in the time it takes to process RUM reports, better memory and disk space utilization, and visibility into the RUM reports on the product instance (how many there are, the processing state each one is in, if there are errors in any of them, and so on). See: RUM Report and Report Acknowledgement, Upgrades, Downgrades, show license rum, show license all, show license tech.
Support for trust code in additional topologies	A trust code is automatically obtained in topologies where the product instance initiates the sending of data to Cisco Smart License Utility (CSLU)and in topologies where the product instance is in an air-gapped network. See: Trust Code, Connected to CSSM Through CSLU, Tasks for Product Instance-Initiated Communication, CSLU Disconnected from CSSM, Tasks for Product Instance-Initiated Communication, No Connectivity to CSSM and No CSLU, Workflow for Topology: No Connectivity to CSSM and No CSLU.
Support to collect software version in a RUM report	If version privacy is disabled (**no license smart privacy version** global configuration command), the Cisco IOS-XE software version running on the product instance and the Smart Agent version information is *included* in the RUM report. See: license smart (global config).

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 and Open Bugs for Cisco IOS XE Cupertino 17.7.1a

Resolved Bugs for Cisco IOS XE 17.7.1a

Bug ID	Description
CSCvz98446	VG400 crashed when changing Debug Level
CSCvz58895	IOS-XE unable to export elliptic curve key
CSCvz65545	ISIS reports encode error when NSF cisco if configured for GRE tunnel number greater than 65535

Bug ID	Description
CSCwa26599	FN980 new signed Telit modem firmware FN980M_38.02.X92 upgrade failed
CSCvz86591	VRF-aware static NAT with route-map and reversible not working
CSCvy69846	Guestshell:.py files stored under /home/guestshell are lost after reboot on 1ng device
CSCvy73165	ASR1hx,GD:10G interfaces supports multirate:Mismatch in autoneg/speed in sh run and sh sdwan run
CSCvw16093	Secure key agent trace levels set to Noise by default
CSCwa10915	ASR1k PFRv3: Elephant flow will trigger performance monitor exporting more than 50% byte loss
CSCvz11362	ASR fails to install rekey causing traffic drop
CSCvt66541	Crypto PKI-CRL-IO process crash when PKI trustpoint is being deleted
CSCvy34805	Consecutive Multicast Crashes in ISR4K
CSCvy92696	Cosmetic: 'Logging host' configuration inconsistent between sdwan and IOS configuration
CSCvz30670	Qos issue on IPv6 Virtual access (tunnel ipsec) interface ASR1k
CSCvz14745	Memory leak seen when using DNS with IP SLA
CSCvy27721	IOS-XE Router may experience unexpected reboot with X25 RBP
CSCvy45095	ipv6 ebgp multihop session remains in "idle" state after removal and recreation of the config
CSCvy72210	Cisco IOS XE crash after executing 'show flowspec ipv4' command
CSCvy42216	"switchport trunk native vlan xx" gets removed when upgrading from 16.12.x to 17.3.3
CSCvy53885	ip pim rp-candidate command removed after reload when group list is configured
CSCvz21812	QoS policy update with "random-detect dscp" configuration get rejected on device side
CSCvy54964	Large tx/rx rate on Dialer interface in show interface output.
CSCvy23400	MC-LAG feature cannot preserve administratively shut down sub-interfaces
CSCvy99942	Netconf: Logging to syslog stops working in certain scenarios
CSCvy93946	Removal of SHA-1 HMAC Impacting ability to SSH
CSCvy83154	MAG is not detecting the path UP after several reboots
CSCvy29106	ASR1K crashed on a Eigrp enabled device when Netconf get operation was used
CSCvw13682	L3 connected lite session not coming up, stuck in data-plane(qfp)
CSCvx62167	Route-map corruption when configured using Netconf with ncclient manager

Bug ID	Description
CSCvy22343	Crash after reapplying BGP/ attempt to initialize an initialized wavl tree
CSCvy53210	ASR1002-HX running ISG w/ IOS v17.3.3 Crashed and caused a major outage of 40K EoGRE sessions
CSCvy91121	SSS manager Crash seen on latest polaris_dev image
CSCvy08748	OSPF summary-address isn't generated though candidate exists
CSCvy63983	vManage showing wrong interface status in GUI
CSCvy24754	Netconf-yang: no special characters allowed in ACL

Open Bugs for Cisco IOS XE 17.7.1a

Bug ID	Description
CSCvz67279	SELINUX-5-Mismatch Log on ASR1002HX and 8500 Platforms
CSCvz87460	ASR 1000-RP2|VID>V07|16.9.7 MD5 signature does not match failure while upgrading to 17.3(1r) rommon
CSCvz95158	ASR1K-HX: IPSec Led doesn't lit even though module is correctly installed
CSCwa12061	IOS 17.x/RP3 copy process / file transfer to USB fails for large files>2GB size
CSCvz92954	Device UTD Container doesn't come up after a reboot
CSCwa20814	Device hitting vulnerability CVE 2008-5161
CSCwa46001	VRRP traffic sent while the device boots will congest the interface queue causing taildrops
CSCwa42344	SDWAN crash seen @ IOSXE-WATCHDOG: Process = OSPF-101 Hello
CSCvz72871	Multicast traffic received over DMVPN tunnel are dropped on RP and not forwarded downstream.
CSCwa27659	virtual VRRP IP address unreachable from the BACKUP VRRP
CSCvz41067	IP Community-list config out of sync in sdwan and ios-xe
CSCwa22665	Memory leak in scaled EIGRP DMVPN implementation due to EIGRP: mgd_timer
CSCvw06937	SNMv3 traps failing with initial configuration
CSCvz86580	Unable to remove the BGP neighbor statement through vManage template.
CSCvz20285	SDWAN image info not updated in packages.conf when upgrading in autonomous mode
CSCvz55553	BGP routes refreshing in the routing table after adding "bgp advertise-best-external"

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
- Deferral Notices
- Cisco Bulletins

© 2021 Cisco Systems, Inc. All rights reserved.