Release Notes for Cisco ASR 1000 Series, Cisco IOS XE Bengaluru 17.5.x

First Published: 2020-03-23

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 Bengaluru 17.5.1a is the first release for Cisco ASR 1000 Series Aggregation Services Routers in the Cisco IOS XE Bengaluru 17.5.1a 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.

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 17.5.X

Table 1: New Software Features in Cisco ASR 1000 Series Release Cisco IOS XE 17.5.x

Feature	Description
Cisco IS-IS Local Unequal Cost Multipath	The Segment Routing—IS-IS UCMP feature allows you to load balance outgoing traffic across all IGP ECMP paths proportionally to the interface bandwidth.
Configuring Per-Interface Per-Cause Punt Policer	The per-interface per-cause (PIPC) punt policing is an enhancement to the punt policing and monitoring feature that allows you to configure the limit on traffic per interface. Starting from the Cisco IOS XE 17.5.1 release, you can set the per-interface per-cause rate for all the control plane punted traffic. This rate causes any traffic beyond the set limit to be dropped, therefore allowing you to control the traffic during conditions such as L2 storming.
Configuring ERSPAN	The Cisco DNA Traffic Telemetry Appliance supports the Encapsulated Remote Switching Port Analyzer (ERSPAN) feature on both source and destination ports. ERSPAN transports mirrored traffic over an IP network. You can configure the network devices to mirror traffic on specific ports or VLANs and send it over to the EA Telemetry Sensor for Deep packet inspection. The EA Telemetry Sensor receives and processes data from a port that is configured as ERSPAN.
Capability to limit IPv6 Mroutes per VRF	This feature lets you configure a limit to the number of mroutes on an interface. By limiting the mroutes, you can avoid the risk of flooding the network with mroutes therefore protecting the router from resource overload and also preventing DoS attacks.
Configuring EVPN VXLAN External Connectivity	You can configure the EVPN VXLAN external connectivity for enterprise routers. External connectivity refers to the movement of Layer 2 and Layer 3 traffic between an EVPN VXLAN network and an external network. This enables the EVPN VXLAN network to exchange routes with the externally connected network.
Enabling Segment Routing Flexible Algorithm with IS-IS:	Segment Routing Flexible Algorithm with IS-IS: Segment Routing Flexible Algorithm allows operators to customize IGP shortest path computation according to their own needs. An operator can assign custom SR prefix-SIDs to realize forwarding beyond link-cost-based SPF. As a result, Flexible Algorithm provides a traffic engineered path automatically computed by the IGP to any destination reachable by the IGP. This release also introduces support for the following functionalities: • Flex Algo prefix metric: Flex-algo prefix-metric allows to associate metric computed in given flex-algo with a prefix during prefix inter-level leaking or during inter-domain redistribution .This help to compute optimal inter-level or inter-domain path Support for affinities include any/all: Ability to pick and choose the links that they want. User can use a certain path without creating a label stack by using the Prefix SIDs or Adjacency SIDs. • TI LFA + uLoop Avoidance: Allows computation of Loop Free Alternate (LFA) paths. TI-LFA backup paths using the same constraints as the calculation of the primary paths for Flexible Algorithms, for IS-IS Inter-area leaking of Flexible Algorithm SIDs and prefixes and selectively filtering the paths that are installed to the MFI are also supported.

Feature	Description
License Management for Smart Licensing Using Policy, Using Cisco vManage	Cisco SD-WAN operates together with Cisco SSM to provide license management through Cisco vManage for devices operating with Cisco SD-WAN. For this you have to implement a topology where Cisco vManage is connected to CSSM. For information about this topology, see the Connected to CSSM Through a Controller, and to know how to implement it, see the Workflow for Topology: Connected to CSSM Through a Controller sections of the *Smart Licensing Using Policy for Cisco Enterprise Routing Platforms* guide. For more information about Cisco vManage, see the License Management for Smart Licensing Using Policy section of the *Cisco SD-WAN Getting Start Guide*. For a more detailed overview on Cisco Licensing, go to cisco.com/go/licensingguide
Support for 25G Interface	The ASR 1000 now supports an interface speed of 25G to prevent a single interface causing bottle necks to the overall performance of the router.
Traffic Steering by Dropping Invalid Paths	If the SR-TE Policy has no valid paths defined, the paths are dropped and traffic being steered through the policy falls back to the default (unconstrained IGP) forwarding path. Also, when a SR-TE policy carrying best-effort traffic fails, traffic is re-routed and this impacts the SLA for premium traffic.To solve this issue, if the SR-TE policy fails, the traffic in the data plane is dropped but kept in the controlplane. Therefore, other SR policies, potentially carrying premium traffic, are not impacted.
Tunnel Path MTU discovery on MPLS-enabled GRE tunnel	You can now use the tunnel mpls-ip-only command to configure how the Do Not Fragment bit from the payload is copied into the tunnel packets IP header. If the Do Not Fragment bit is not set, the payload is fragmented if an IP packet exceeds the MTU set for the interface.
View traffic counters for SR-TE policies	You can now view the traffic counters of SR-TE policies using the show segment-routing traffic-eng policy command.
View Traffic Counters for SR-TE Policies	The existing command show segment-routing traffic-eng policy is improved to display the traffic rate on the tunnel interface. No configuration is required to enable this feature.

New and Enhanced Software Features for Cisco CUBE

Feature	Description
Secure forking for non-secure flow in CUBE	Before Cisco IOS XE Bengaluru 17.5.1, Media Proxy supported nonsecure forking of nonsecure calls for both SIPREC and proprietary CUCM and secure forking of secure calls for proprietary CUCM. From Cisco IOS XE Bengaluru 17.5.1, proprietary CUCM supports a combination of secure and nonsecure forking and SIPREC supports secure forking of nonsecure calls using Media Proxy. The configured dial peers can be all secure, all nonsecure, or a combination of secure and nonsecure. The total number of recorders permitted is five. The first secure dial peer is used to set up the B2B call leg. The behavior in Cisco IOS XE Bengaluru 17.4.1 and earlier releases continues if there are no secure dial peers configured. You can use the media-recording proxy secure command to configure secure dial peers.

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 Bengaluru 17.5

Resolved Bugs for Cisco IOS XE Bengaluru 17.5

Caveat ID Number	Description
CSCvu97660	Dataplan crash seen at pppoe
CSCvv48647	C8500L-8S4X may crash during redundancy force-switchover when dual-RP is enabled
CSCvv54152	CDP on interfaces is not enabled when CDP is enabled globally on ASR Routers in controller mode
CSCvw12396	17.3:ASR1K:NTT:ESP200-X crashed while unbinding 100K PPPoX sessions
CSCvv25049	Fluctuation of around 5-10% is seen in perf with IMIX profile in ESP100x/ESP200x with NBAR and FWALL
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
CSCvw70009	ASR 1000 Series: fman_rp crash seen on 16.9.X when "show platform software nat RP active logging" is run
CSCvw70461	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	ZBFW: Stale ACL entries seen on ASR 1000 Series
CSCvw74921	APPNAV CFT crash on ISR
CSCvx35902	fman_rp: qos_hqf [L:1.0, N:0x3485061e18] (0p, 0c) download to FP failed resulting in a crash.
CSCvx26065	1006-X: Box rebooted after critical process cpp_cp_svr has failed (rc 134), 8K BFDs
CSCvv99281	BQS crash on PPPoE session churn overnight
CSCvx02965	17.5-ASR1k-9X,6X,13RU: fsck for harddisk always fails with error Device Busy.

Open Bugs for Cisco IOS XE Bengaluru 17.5

Caveat ID Number	Description
CSCvw94434	BQS crash seen at cpp_qm_event_proc_defer_cb
CSCvw98579	BQS crash seen in 17.3 while bringing up 30k PPPOE sessions
CSCvx69830	Cisco ASR 1000: BQS crash seen at cpp_qm_event_proc_defer_cb
CSCvr91128	NAT HA - stale tcp sessions in standby router
CSCvw13682	L3 connected lite session not coming up , stuck in data-plane(qfp)
CSCvw67366	ASR1002-X: Punt keepalive crashed due to bqs related interrupt
CSCvw90220	Crash at #12 0x00007f010f4cb9db in cpp_bqs_rm_yoda_get_flush_obj while subscriber bringup
CSCvx08118	ASR1001-X: Bug to further address CSCvt08179 : QFP crash due to hardware interrupt
CSCvx29526	Ping and traffic not working with qinq configuration with ethertype 0x9200 configured
CSCvx67019	High QFP utilization with stateless static bind
CSCvy24239	GD B2B crash at ipv4_nat_ha_rcv_stby_sess_del_notify_rsp
CSCvw79553	Sharkmuffin: OOS alarm notifications support for unsupported/swap EPA's on vManage.

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