Release Notes for Cisco ASR 1000 Series, Cisco IOS XE Dublin 17.11.x

First Published: 2023-04-06

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 Dublin 17.11.1a is the first release for Cisco ASR 1000 Series Aggregation Services Routers in the Cisco IOS XE Dublin 17.11.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

Table 1: New Software Features in Cisco ASR 1000 Series Release Cisco IOS XE 17.11.1a

Feature	Description
Bridge Domain VIF Support on Layer 2 EVPN	This enhancement allows configuring a Layer 2 EVPN network to support a Bridge Domain Interface (BDI) to act as an interface to a routing domain. Also, you can attach one or more bridge domain VIF interfaces to an EVPN Layer 2 network.
Deprecation of Weak Ciphers	The minimum Rivest, Shamir, and Adleman (RSA) key pair size must be 2048 bits. The compliance shield on the device must be disabled using the **crypto engine compliance shield disable** command to use the weak RSA key.
Extending Dynamic Neighbor support for additional address families	From Cisco IOS XE Dublin 17.11.1a, this feature extends BGP dynamic neighbors support to the following address families: • L2VPN EVPN • L2VPN VPLS • IPv4 FlowSpec • IPv4 MDT • IPv4 Multicast • IPv4 MVPN • IPv6 FlowSpec • IPv6 Multicast • IPv6 MVPN • Link-State • NSAP • RT-filter
MAC and IP Addressing Learning from a Static ARP Alias Entry	This enhancement allows you to configure an EVPN VXLAN network to learn an EVPN MAC address and IP binding from a static Address Resolution Protocol (ARP) alias entry. After learning the MAC address and IP binding, an EVPN Type-2 route is advertised across the EVPN network.

Feature	Description
Quantum-Safe Encryption Using Post-Quantum Preshared Keys	This feature implements RFC 8784 and Cisco Secure Key Integration Protocol (SKIP) for quantum-safe encryption of IKEv2 and IPsec packets using Post-quantum Preshared Key (PPK). The PPKs configured manually are referred to as manual PPKs and the PPKs imported from an external key source (KS) using the SKIP protocol are referred to as dynamic PPKs. This feature is applicable to all IKEv2/IPsec VPNs such as FlexVPN (SVTI-DVTI) and DMVPN, except for GETVPN. See also Cisco IOS Security Command Reference.
Replication of Broadcast, Unknown-unicast, and Multicast Traffic	With this enhancement, the multi-destination Layer 2 broadcast, unknown-unicast, and multicast (BUM) traffic in an EVPN VXLAN network is replicated through a multicast group in the underlay network and forwarded to all the endpoints of the network.

Feature	Description	
Revised LISP Commands	The following LISP commands are revised:	
	Old Command	New Command
	show ip/ipv6 lisp all	**show lisp service ipv4/ipv6**
	show ip/ipv6 lisp instance-id alt	**show lisp instance-id ipv4/ipv6 alt**
	show ip/ipv6 lisp instance-id database	**show lisp instance-id ipv4/ipv6 database**
	show ip/ipv6 lisp forwarding	**show lisp ipv4/ipv6 instance-id forwarding**
	show ip/ipv6 lisp instance-id	**show lisp instance-id**
	show ip/ipv6 lisp locator-table	**show lisp locator-table**
	show ip/ipv6 lisp instance-id map-cache	**show lisp instance-id ipv4/ipv6 map-cache**
	show ip/ipv6 lisp instance-id route-import	**show lisp instance-id ipv4/ipv6 route-import**
	show ip/ipv6 lisp instance-id smr	**show lisp instance-id ipv4/ipv6 smr**
	show ip/ipv6 lisp instance-id statistics	

Feature	Description	
		show lisp instance-id ipv4/ipv6 statistics
	show lisp site	**show lisp server**
	show lisp site detail	**show lisp instance-id ipv4/ipv6 server detail**
	show lisp site name	**show lisp instance-id ipv4/ipv6 server name**
	show lisp site summary	**show lisp instance-id ipv4/ipv6 server summary**
	show lisp site rloc	**show lisp instance-id ipv4/ipv6 server rloc**
TE Metric Support for Segment Routing IS-IS Flex Algo	This feature adds support for TE metric as a metric type for IS-IS Flexible Algorithm. This allows the TE metric, along with IGP and delay metrics, to be used when running shortest path computations.	
Upgrade in IPsec Tunnel Scaling for High-End Aggregation	IPsec FlexVPN tunnel scale is improved for ASR1000-RP3 based modular platforms.	

Feature	Description
Smart Licensing Using Policy Features	
Snapshots for Product Activation Key (PAK) licenses	Starting with Cisco IOS XE Dublin 17.11.1a, the PAK-managing library is discontinued and the provision to take a snapshot is no longer available. Software images from Cisco IOS XE Dublin 17.11.1a onwards rely only on the snapshotted information about PAK licenses. For more information, see: Snapshots for PAK Licenses. If you have a PAK license without a snapshot, and you want to upgrade to Cisco IOS XE Dublin 17.11.1a or a later release, you will have to upgrade twice. First upgrade to one of the releases where the system can take a snapshot of the PAK license and complete DLC, and then again upgrade to the required, later release.

Resolved and Open Bugs for Cisco IOS XE 17.11.x

Resolved Bugs for Cisco IOS XE 17.11.1a

Bug ID	Description
CSCwd47940	PMTU Discovery is not working after interface flap.
CSCwd45402	MSR Unicast-To-Multicast not working if DST and SRC are the same in Service Reflect configuration.
CSCwc79115	Commit failure notification and alarm from device.
CSCwd16559	ARP request to reroute nexthop IP is not triggered if ARP entry not in ARP table.
CSCwd67198	uCode crash seen on C8300 after stopping NWPI trace.
CSCwe28204	Control connection over L3 TLOC extension failing as no NAT table entry created.
CSCwe22353	IpFormatErr drops on device when bridge-domain/EVC MAC learning limit is exhausted.
CSCwe09805	OID for SNMP monitoring of DSP resources are not working as expected.
CSCwd89012	Tested flap-based auto-suspension - Minimum duration value - no results as expected.
CSCwe29430	Critical process fpmd fault on rp_0_0 (rc=134).
CSCwd79089	Device crash when sending full line rate of traffic with >5 Intel AX210 stations.
CSCwd87195	NAT configuration with redundancy, mapping id and match-in-vrf options with no-alias support.
CSCwd81357	QoS classification not working for DSCP or ACL + MPLS EXP.
CSCwc99823	FMAN crash seen in SGACL@ fman_sgacl_calloc.
CSCwd90168	Unexpected Reload after running **show voice dsp** command while an ISDN call disconnects.
CSCwd44439	Device crashing at fman_sdwan_nh_indirect_delete_from_hash_table.

Bug ID	Description
CSCwd34941	NAT configuration with no-alias option is not preserved after reload.
CSCwc72588	Router should not allow weak cryptographic algorithms to be configured for IPSec.
CSCwd25107	Interface Vlan1 placed in shutdown state when configured with **ip address pool**.
CSCwc68069	RTP packets not forwarded when packet duplication enabled, no issue without duplication feature
CSCwe00946	System crash after disabling endpoint-tracker on tunnel interfaces.
CSCwe18058	Unexpected reload with IPS configured.
CSCwd61255	Data plane crash on device when making per-tunnel QoS configuration Changes with scale.
CSCwe01015	IKEv2/IPSec rekey failing when peer is behind NAT.
CSCwd65945	LR Interface which has NAT enabled is chosen for webex traffic.
CSCwe27241	NBAR classification error with custom app-aware routing policy.
CSCwc37465	Unable to push no-alias option on static NAT mapping from management system.
CSCwc67625	OU field is deprecated from CA/B Forum certificate authorities.
CSCwe33793	Memory allocation failure with extended antireplay enabled.
CSCwd44006	Control connection on device doesn't come-up with reverse proxy using enterprise certificate.
CSCwe23276	Change in the IPSec integrity parameters breaks the connectivity.
CSCwd46921	Device is not connecting to second vSmart after both assigned vSmart is down.
CSCwe16371	Device going in disabled state after **hw-module <slot> reload**.
CSCwd12330	Invalid TCP checksum in SYN flag packets passing through router.
CSCwd30578	Wired guest client stuck at IP_LEARN with DHCP packets not forwarded out of the foreign to anchor.
CSCwd81240	CPU utilization from the Linux kernel is at 100% due to btelnet.
CSCwe60059	Crash when using dial-peer groups with STCAPP.
CSCwd15487	Kernel crash is observed when modem-power-cycle is executed.
CSCwd67654	FNF stats are getting populated with unknown in egress/ingress interface in vpn0.
CSCwd38943	KS reject registration from a public IP.
CSCwb59113	BFD session gets NAT translated with static ip over dialer interface.

Bug ID	Description
CSCwe03614	MAC address of ATM interface is not included in inform message.
CSCwb46968	Device template attachment causes PPPoE commands to be removed from ethernet interface.
CSCwe19084	NAT: Traffic is not translated to the same global address though PAP is configured.
CSCwe69783	Device loses its config during a triggered resync process if lines are in an off-hook state.
CSCwd71586	BFD sessions flapping on an interface with SYMNAT may lead to IPSec crash.
CSCwe41946	DTMF is failing through IOS MTP during call on-hold.
CSCwd85580	Device unexpected reload after set **ospfv3 authentication null** command.
CSCwd06923	Stale IP alias left after NAT statement got removed.
CSCwc48427	BFD issues with clear_omp -> non-PWK + non-VRRP scenario only.
CSCwd28593	Control connection flap after shutting down.
CSCwd47123	ISG uses identifier mac-address 0000.0000.0000 when DHCP LQ does not reply.
CSCwd81813	Startup-config not parsed correctly after upgrading.
CSCwe34808	FMAN FP leak due to the **punt-policer** command.
CSCwe32862	Router IOS-XE crash while executing AES crypto functions.
CSCwe53849	Observed crash in CPP, UCode & FMAN while upgrading with crypto module present.
CSCwe25076	ALG breaks NBAR recognition impacting application firewall performance.
CSCwd68994	ISAKMP profile doesn't match as per configured certificate maps.
CSCwd79572	FW policy with app-family rule with FQDN causes traffic drop for other sequences.
CSCwe91988	Need to disable CSDL compliance check for NPE images.

Open Bugs for Cisco IOS XE 17.11.1a

Bug ID	Description
CSCwd42523	Same label is assigned to different VRFs.
CSCwd45508	Device does not form BFD across serial link when upgrading.
CSCwe49509	Some BFD tunnel went down after migrating.
CSCwe37123	Device uses excessive memory when configuring ACLs with large object groups.
CSCwe19394	Device may boot up into prev_packages.conf due to power outage.

Bug ID	Description
CSCwe18276	Route-map not getting effect when its applied in OMP for BGP routes.
CSCwe40024	98% memory utilization for device.
CSCwd68111	Device object group called in ZBFW gives error after upgrade.
CSCwe49684	SDWAN BFD sessions keeps flapping intermittently.
CSCwe52971	BFD tunnels remain in down state.

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.

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 results 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 DevNet.
- 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.