Release Notes for Cisco 1000 Series Integrated Services Routers, Cisco IOS XE Cupertino 17.7.x

First Published: 2021-12-17

Last Modified: 2022-06-23

Full Cisco Trademarks with Software License

About Cisco 1000 Series Integrated Services Routers

The Cisco 1000 Series Integrated Services Routers (also referred to as router in this document) are powerful fixed branch routers based on the Cisco IOS XE operating system. They are multi-core routers with separate core for data plane and control plane. There are two primary models with 8 LAN ports and 4 LAN ports. Features such as Smart Licensing, VDSL2 and ADSL2/2+, 802.11ac with Wave 2, 4G LTE-Advanced and 3G/4G LTE and LTEA Omnidirectional Dipole Antenna (LTE-ANTM-SMA-D) are supported on the router.

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

Note Starting with Cisco IOS XE Amsterdam 17.3.2, 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).

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 and Software Features

New and Changed Hardware Features

There are no new or enhanced features introduced in this release.

New and Changed Software Features

Table 1: New Software Features

Feature	Description
Marking Packets Sent Via ATM Interface With COS(BITP) Value	This feature introduces the **set cos 3** command using which, you can configure the router to mark the packets with a cos (bitp) value. The marked packets are indicators of priority for the user and based on the priority level, bandwidth will be allocated.
Multicast - mcast 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.
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.
Storm Control Support for Cisco 1000 Integrated Services Routers	This feature prevents LAN ports from being disrupted by a unicast, broadcast, or multicast traffic storm on physical interfaces. It allows user to define the threshold rate of the traffic storm and choose the action that would be taken in storm.
YANG Configuration Models for CUBE	From Cisco IOS XE Cupertino 17.7.1a, YANG models are available to configure and manage CUBE as part of the Cisco SD-WAN solution.
YANG Model Version 1.1	Cisco IOS XE Cupertino 17.7.1a uses the YANG version 1.0; however, you can download the Cisco IOS XE YANG models in 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 version 1.1 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	

Feature	Description
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.
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

Feature	Description
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 ISR1000 ROMMON Compatibility Matrix

The following table lists the ROMmon releases supported in Cisco IOS XE 16.x.x releases and Cisco IOS XE 17.x.x releases

Note To identify the manufacturing date, use the **show license udi** command. For example:

```
Router#show license udi
UDI: PID:C1131-8PLTEPWB,SN:FGLxxxxLCQ6
```

The xxxx in the command output represents the manufacturing date.

- If the manufacturing date is greater than or equal to 0x2535, the recommended ROMmon version is 17.6(1r).
- If the manufacturing date is less than 0x2535, you can upgrade to the recommended ROMmon version 17.5(1r) or later.
- The minimal or recommended ROMmon version for devices using Cisco IOS XE 17.5 to 17.7 is 17.5(1r) or later.

Table 2: Minimum and Recommended ROMmon Releases Supported on Cisco 1000 Series Integrated Services Routers

Cisco IOS XE Release	Minimum ROMmon Release for IOS XE	Recommended ROMmon Release for IOS XE
16.6.x	16.6(1r)	16.6(1r)
16.7.x	16.6(1r)	16.6(1r)
16.8.x	16.8(1r)	16.8(1r)
16.9.x	16.9(1r)	16.9(1r)
16.10.x	16.9(1r)	16.9(1r)
16.11.x	16.9(1r)	16.9(1r)
16.12.x	16.9(1r)	16.12(1r)
17.2.x	16.9(1r)	16.12(1r)
17.3.x	16.12(2r)	16.12(2r)
17.4.x	16.12(2r)	16.12(2r)

Cisco IOS XE Release	Minimum ROMmon Release for IOS XE	Recommended ROMmon Release for IOS XE
17.5.x	17.5(1r)	17.5(1r)
17.6.x	17.5(1r)	17.5(1r)
17.7.x	17.5(1r)	17.5(1r)

Resolved Bugs in Cisco IOS XE 17.7.2

Bug ID	Description
CSCwa17720	Device rebooted due to watchdogs after issuing the commands sh crypto mib ipsec commands.
CSCwa11150	E1 configurations (under serial interface) lost after reload.
CSCwa76260	IKEv2 deprecated ciphers denied by crypto engine CDSL - PSB security compliance - DES, 3DES, DH1/2/5.
CSCwa49902	MGCP automatic configuration fails after IOS-XE upgrade on device.
CSCwa15085	Router crash due to stuck thread with appnav-xe dual controller mode.
CSCvx28426	Router may crash due to crypto IKMP process.
CSCwa80474	IKEv2 deprecated ciphers denied by crypto engine CDSL - PSB security compliance - MD5, SHA1.
CSCwa15132	DMVPN over DMVPN with IPSEC - return packets are dropped with BadIpChecksum.
CSCwa30988	CoS preservation not working for the services EVPL and EPL tunnel.
CSCwa01293	ZBFW: Optimized policy traffic failure due to OG edit error.
CSCwa18177	Flapping bidirectional/unidirectional packet capture option with ipv4 filter for long time failed.

Open Bugs in Cisco IOS XE 17.7.2

Bug ID	Description
CSCwb38501	Device support IGMP on voice vlan.
CSCwa51582	IP device-tracking not functional with voice VLAN configured.
CSCvz65764	Peer MSS value showing incorrect.
CSCwb25137	[XE NAT] Source address translation for multicast traffic fails with route-map.
CSCwb78423	Excessive packet loss observed during DMVPN tunnel flapping.

Bug ID	Description
CSCwb02142	Traceback: fman_fp_image core after clearing packet-trace conditions.
CSCwb66749	When configuration ip nat inside/outside on VASI intereface, ack/seq number abnormal.
CSCwb32059	Cellular interface tracker down but NAT route persists in the service VPN routing table.
CSCwb74821	Yang-management process confd is not running.
CSCwa13553	QFP core due to NAT scaling issue.
CSCwb11389	NAT translation stops suddenly (ip nat inside does not work).
CSCwb51238	Router reload unexpectedly two times when enter netflow show command.
CSCwb61073	BQS Failure - QoS policy is missing in hardware for some virtual-access tunnels after session flaps.
CSCwa66916	SCCP auto-configuration issues with multiple protocols.
CSCwb25913	After configuring match input-interface on class-map, router goes into a reboot loop.
CSCwb55683	Large number of IPSec tunnel flapping occurs when underlay is restored.
CSCvz89354	Device crashes due to CPUHOG when walking ciscoFlashMIB.
CSCwb08186	E1 R2 - dnis-digits cli not working.
CSCvz91309	Crash due to IOSXE-WATCHDOG due to management port traffic storm.
CSCwb12647	Device crash for stuck threads in cpp on packet processing.
CSCwa48512	CoR intercepted DNS reply packets dropped with drop code 52 (FirewallL4Insp) if UTD enabled.
CSCwb41907	CPP uCode crash due to ipc congestion from dp to cp.
CSCwb74917	Device incorrectly drops ip fragments due to reassembly timeout.
CSCwa67398	NAT translations do not work for FTP traffic.
CSCwb76509	Assert failure while showing FTM (Forwarding Traffic Manager) data in NH TYPE switch case.
CSCwa84919	Revocation-check crl none does not failover to NONE DNAC-CA.
CSCwb78173	CSDL failure: IPSec QM use of DES by encrypt proc is denied.
CSCwb46649	NAT translation do not show (or use) correct timeout value for an established TCP session.
CSCwb68897	Total output drops counter in show interface on port-channel does not work properly.
CSCvw50622	Nhrp network resolution not working with link-local ipv6 address.

Bug ID	Description
CSCvz34668	Static mapping for the hub lost on one of the spokes.
CSCwa74499	ZBFW seeing the SIP ALG incorrectly dropping traffic and resetting connection.
CSCwb76866	CSDL failure: Use of MD5 by IPSEC key engine is denied.
CSCwa68540	FTP data traffic broken when UTD IPS enabled in both service VPN.
CSCwb79138	Device after the upgrade starts dropping GRE tunnel packets.

Resolved Bugs in Cisco IOS XE 17.7.1a

Bug ID	Description
CSCvz89043	Prevent SIP services from being blocked even if license usage ACK was not received
CSCvr91128	NAT HA - stale tcp sessions in standby router
CSCvx71735	IOS-XE Device may experience an unexpected reset in SNMP ENGINE when polling cEigrpInterfaceEntry
CSCvy17964	Traceback seen when cwmp wan default interface changed
CSCvy18284	Poor IPsec throughput performance with IPsec throughput license on IOS-XE routers
CSCvy24239	GD B2B crash at ipv4_nat_ha_rcv_stby_sess_del_notify_rsp
CSCvy26572	[SWI : #01080538] LTE is not reestablishing after reset of the modem
CSCvy34102	CPP ucode crash with route-map and overload at ipv4_nat_rmap_walk_find.
CSCvy35044	Signature update failure - SSL-CERTIFICATE_VERIFY_FAILED
CSCvy36311	CWMP: Portmapping with space in description field rejected after reload
CSCvy39019	CWMP: WANPPPConnection not reset when PPP credentials changed
CSCvy68270	CWMP wrong parameter value
CSCvy97578	Need Active/Active ZBFW support for Inter-vrf TCP traffic
CSCvx62167	Route-map corruption when configured using Netconf with ncclient manager
CSCvy08748	OSPF summary-address is not generated though candidate exists
CSCvy22343	Crash after reapplying BGP/ attempt to initialize an initialized wavl tree
CSCvy27721	IOS-XE Router may experience unexpected reboot with X25 RBP
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

Bug ID	Description
CSCvy54964	Large tx/rx rate on Dialer interface in show interface output.
CSCvy64796	RIP Yang [17.7] offset-list with interface config not shown in ios running-config
CSCvy69555	Unable to fetch eigrp prefix, nexthop, omptag, and route origin
CSCvy93946	Removal of SHA-1 HMAC Impacting ability to SSH
CSCvy99942	Netconf: Logging to syslog stops working in certain scenarios
CSCvz04059	17.6: EFT: Replicated EBGP routes from global table replacing native IBGP routes in VRF.
CSCvz21812	QoS policy update with random-detect dscp configuration get rejected on device side.
CSCvy34805	Consecutive Multicast Crashes in ISR4000
CSCvy38743	CISCO-CLASS-BASED-QOS-MIB doesn't work with LTE Cellular interface on ISR1100X after reload
CSCvy92696	Cosmetic: Logging host configuration inconsistent between sdwan and IOS configuration
CSCvz30670	Qos issue on IPv6 Virtual access (tunnel ipsec) interface
CSCvz14745	Memory leak seen when using DNS with IP SLA
CSCvz98446	VG400 crashed when changing Debug Level
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
CSCvy83154	MAG is not detecting the path UP after several reboots
CSCvw16093	Secure key agent trace levels set to Noise by default
CSCvy29106	Device crashed on a Eigrp enabled device when Netconf get operation was used
CSCvy23400	MC-LAG feature cannot preserve administratively shut down sub-interfaces
CSCvw13682	L3 connected lite session not coming up , stuck in data-plane(qfp)
CSCvt66541	Crypto PKI-CRL-IO process crash when PKI trustpoint is being deleted
CSCwa26599	FN980 new signed Telit modem firmware FN980M_38.02.X92 upgrade failed
CSCvz58895	IOS-XE unable to export elliptic curve key
CSCvy53210	ASR1002-HX running ISG w/ IOS v17.3.3 Crashed and caused a major outage of 40K EoGRE sessions
CSCvz84437	Cisco8500L // 17.6.1a// Unexpected reload due IPV6 UDP fragment header in VxLAN

Bug ID	Description
CSCvy91121	SSS manager Crash seen on latest polaris_dev image
CSCvy63983	Device showing wrong interface status in GUI
CSCvy24754	Netconf-yang: no special characters allowed in ACL

Open Bugs in Cisco IOS XE 17.7.1a

Bug ID	Description
CSCvz20285	The image info not updated in packages.conf when upgrading in autonomous mode
CSCvz41067	IP Community-list config out of sync
CSCvz72871	Multicast traffic received over DMVPN tunnel are dropped on RP and not forwarded downstream.
CSCvz86580	Unable to remove the BGP neighbor statement through vManage template.
CSCwa27659	Virtual VRRP IP address unreachable from the BACKUP VRRP.
CSCwa22665	Memory leak in scaled EIGRP DMVPN implementation due to EIGRP: mgd_timer
CSCvy55408	Router multiple crash - session hash corrupted
CSCwa07494	IPSec tunnel not passing traffic when IPSec tunnel is sourced from VASI interface
CSCvz92954	C8000v UTD container does not come up after a reboot
CSCwa20814	Device hitting vulnerability CVE 2008-5161
CSCvw06937	SNMv3 traps failing with initial configuration
CSCwa46001	VRRP traffic sent while the device boots will congest the interface queue causing taildrops
CSCvz55553	BGP routes refreshing in the routing table after adding bgp advertise-best-external

Related Information

- Hardware Installation Guide
- Software Configuration Guide
- Smart Licensing using Policy

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.