Release Notes for Cisco 1000 Series Integrated Services Routers, Cisco IOS XE Bengaluru 17.4.x

First Published: 2020-12-18

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 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).

New and Enhanced-Hardware and Software Features

New and Changed Hardware Features

New Hardware Features

There are no new hardware features in the Cisco IOS XE Amsterdam 17.3.1 release.

New and Changed Software Features

Table 1: New Software Features in Cisco 1000 Series ISRs Release Cisco IOS XE Bengaluru 17.4.1a

Feature	Description
EPC support on LTE interface and FlexVPN interface	Embedded Packet Capture (EPC) is an onboard packet capture facility that allows network administrators to capture packets flowing to, through, and from a device. This feature facilitates troubleshooting by gathering information about packet format.

Feature	Description
Change of Authorization and Trustsec	This feature utilizes Posture Assessment capabilites to validate the compliance of endpoints according to security policies of your enterprise. Identity Services Engine (ISE) Posture functions are integrated into Cisco 1100 Integrated Services Routers. Change of Authorization (CoA) provides a mechanism to change the attributes of an authentication,authorization, and accounting (AAA) session after it is authenticated. Identity-Based Networking Services supports change of authorization (CoA) commands for session query,reauthentication, and termination, port bounce and port shutdown, and service template activation and deactivation
Layer 2 Protocol Tunneling on Ports	You can now configure L2CP X for tunneling, this allows to forward all other l2cp with the DST MAC 01:00:0C:CD:CD:D0 except X with the DST MAC 01:00:0C:CD:CD:D0
IP-SLA-HTTPS	This feature has enhanced capabilities of IP SLA device tracking with HTTPS probes and helps to verify reachability in the network.
Software Configuration Guide for Catalyst Cellular Gateway	Cisco Catalyst Cellular Gateways combine the latest in cellular technology with deployment flexibility, investment protection, and ease of management, with both traditional and SD-WAN deployments.
NBAR Support on the EVC Service Instance	To classify the data packets, enable NBAR FIA-trace data on the Ethernet flow point (EFP) interface. Quality of service (QoS) takes action on the EPF interface based on the results from the NBAR traffic classification.
VRF Support for CPE WAN Management Protocol	The digital subscriber line (DSL) Forum's TR-069, CPE WAN Management Protocol (CWMP), is used for communications between a customer premise equipment (CPE) and an auto-configuration server (ACS). With the VRF Support for CPE WAN Management Protocol, the traffic in global IP table is routed with VRF. This helps to improve the security and also transports the TR069 agent within the VRF.
BGP Large Community	The BGP large communities provide the capability for tagging routes and modifying BGP routing policy on routers. BGP large communities can be appended or removed selectively on the large community attribute as the route travels from router to router.
Consent Token Authorization Process for Dev Key Access	With the introduction of the dev-key install functionality, a subset of Cisco IOS XE platforms that support dev-key functionality are shipped only with a release public key. **Note** An image that is signed with a dev-key does not boot due to the absence of dev public key for image verification.
Configuring Stateless Static NAT	Static Network Address Translation (NAT) allows the user to configure one-to-one translations of the inside local addresses to the outside global addresses. A new keyword stateless is introduced for Cisco IOS XE static NAT configuration and it applies only to static NAT command. When the static mapping is set to stateless, no sessions will be created for that traffic flow.

Table 2: New CUBE, Unified SRST and Unified CME Software Features in Release Cisco IOS XE Bengaluru 17.4.1a

Feature	Description
CUBE: Hunt Stop for Server Groups	With server groups, you can create simpler configurations by specifying a list of destination SIP servers for a single dial peer. When a call matches a dial peer that is configured with a server group, the destination is selected from the list of candidates based on a configured policy. If it is not possible to complete that call, the next candidate is selected. Alternatively, you can also choose to stop hunting through the group if a specified response code is received. If the call cannot be placed to any of the servers in the group, or hunting is stopped, call processing continues to the next preferred dial-peer.
CUBE: VoIP Trace Serviceability Framework	VoIP Trace is a Cisco Unified Border Element (CUBE) serviceability framework, which provides a binary trace facility for persistently monitoring and troubleshooting SIP call issues. The VoIP Trace framework records both successful and failed calls. All call trace data is stored in system memory. In addition, data for calls with IEC errors is written to the logging buffer.
CUBE: Clear Hung RTP Ports	When establishing a call, CUBE allocates several RTP ports that are based on the media that are negotiated for the session. Some ports remain assigned even after the call ends. In the current behavior, **show voip rtp stats**command displays only the ports allocated from the global table, even if the ports are allocated from all the three tables (Global port, media IP address-based, and media VRF-based). Now this command is enhanced to display the ports allocated from all the three tables. The command also displays the hung ports and allows you to release those ports. Releasing the hung ports increases the efficiency of the routers as more ports are available to receive calls.
Unified CME: Smart License Using Policy	Smart Licensing using Policy reports license usage periodically based on an account policy, rather than requesting licenses based on past usage as in previous releases. Evaluation mode and license reservation are not supported. License usage is reported to Smart Agent three minutes after the last configuration change. Now all the devices within a network follow the uniform approach of reporting their license usage to Smart Agent. The Smart Agent in turn creates a Resource Utilization Monitoring (RUM) report and dispatches to CSSM based on the Smart Agent reporting policy. For a more detailed overview on Cisco Licensing, go to https://cisco.com/go/licensingguide.

Note All pyang models are not fully compliant with all the IETF guidelines. For some pyang models, the errors and warnings display while executing pyang with .lintflag; these are currently deemed to be non-critical as they do not impact the semantic of the models or prevent the models from being used as part of toolchains. To determine the issues with the pyang models, ensure to enable the pyang.lintflag and then run the check-models.sh script.

It is recommended to ignore *LEAFREF_IDENTIFIER_NOT_FOUND* and *STRICT_XPATH_FUNCTIONS* errors.

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

Table 3: Minimum and Recommended ROMmon Releases Supported on Cisco 1000 Series Integrated Services Routers

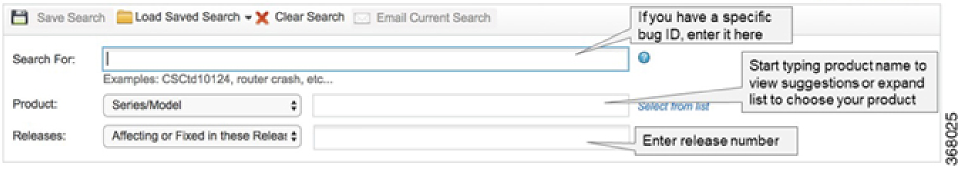
Cisco IOS XE Release	Minimum ROMmon Release Supported for IOS XE	Recommended ROMmon Release Supported for IOS XE
16.6.x	16.6(1r)	16.6(1r)
16.7.x	16.6(1r)	16.6(1r)
16.8.x	16.8(1r)	16.8(1r)
16.9.x	16.9(1r)	16.9(1r)
16.10.x	16.9(1r)	16.9(1r)
16.11.x	16.9(1r)	16.9(1r)
16.12.x	16.9(1r)	16.12(1r)
17.2.x	16.9(1r)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

Resolved and Open Caveats

About the Cisco Bug Search Tool

Use the Cisco Bug Search Tool to access open and resolved bugs for a release.

The tool allows you to search for a specific bug ID, or for all bugs specific to a product and a release.

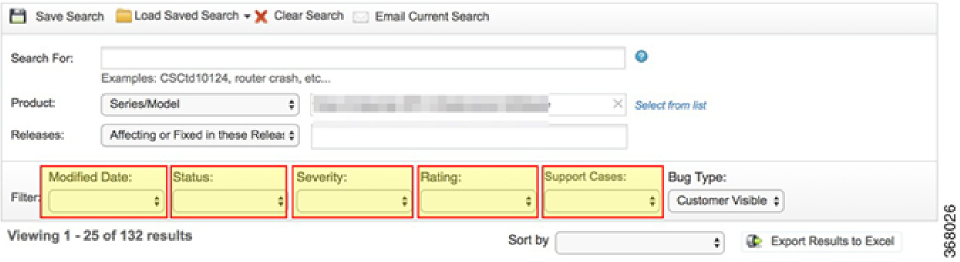


If you have a specific bug ID, enter it here

Start typing product name to view suggestions or expand list to choose your product

Enter release number

You can filter the search results by last modified date, bug status (open, resolved), severity, rating, and support cases.



Search For:

Examples: CSCtd10124, router crash, etc...

Product: Series/Model

Releases: Affecting or Fixed in these Releas

Filter: Modified Date: | Status: | Severity: | Rating: | Support Cases: | Bug Type: Customer Visible

Viewing 1 - 25 of 132 results

Resolved Bugs - Cisco IOS XE Bengaluru 17.4.2

No resolved bugs for this release.

Open Bugs for Cisco IOS XE Bengaluru 17.4.2

Caveat ID Number	Description
CSCvw84883	DDNS feature triggers crash on 16.X/17.X releases due to memory corruption

Resolved Bugs in Cisco IOS XE Bengaluru 17.4.1a

Caveat ID Number	Description
CSCvt06707	C1111-LTE Observe data stalling after cellular interface has been loaded with data traffic for while
CSCvt71774	C1111 HSRP preempt worked even though HSRP's preempt is not configured
CSCvu04426	ISR1K/4K reloads with erroneous reload cause code
CSCvu65369	Link auto-negotiation fails between C1111-4P ES-4 switch module and Meraki MX100
CSCvv02180	C1113-8PLTEEAWA failed to boot: Package does not support : PID not supported in 17.4
CSCvv43027	VDSL performance impacted if more than two vlan tags are used
CSCvv91575	C1111-8P: NAT translations packet counter MIB OID counts unnecessary additional value
CSCvw31389	pktlog functionality is broken
CSCvs30876	Startup config ETH0/2/0 ???not shut' command not added to the startup config
CSCvv37172	License lost after "no license boot level <>" CLI followed by reset button
CSCvw49484	Throughput achieved differs between runs and IXIA readings also misleading compared to EIO state

Open Caveats in Cisco IOS XE Bengaluru 17.4.1a

Caveat ID Number	Description
CSCvw42048	C1111 may drop sip messages when sip inspection and zbf
CSCvu65369	Link auto-negotiation fails between C1111-4P ES-4 switch module and Meraki MX100

Caveat ID Number	Description
CSCvt58920	SIM failover within the same modem takes long time to detect LTE network for AT&T
CSCvv44331	AppQoe Clear Alarm is not generated from device
CSCvv68635	Observed HTX core at tcpproxy_libuinet_pkt_process during longevity test
CSCvv78028	No responder-bytes from cEdge when UTD is enabled
CSCvv79072	25G license tags is retained and throughput throttled after upgrade from 17.3.1 to 17.3.2
CSCvv88621	GETVPN: All GM will crash when Primary KS recovers its COOP role after network outage
CSCvv94743	Data Plane fails over L2TPv3 while disabling VLAN limit restrictions with ASR1002-HX
CSCvw11902	Passive FTP doesn't work with NAT
CSCvw13048	crash observed at NHRP while using summary-map
CSCvw33113	Unexpected reload in NHRP when access to an invalid memory region
CSCvw34157	APPNAV CFT Crashes
CSCvw39383	CPP ucode crash with fw_base_flow_create
CSCvw47800	HSL Export over VASI Interface causes Netflow v9 Template Flooding
CSCvw48800	unable to transfer 1500 byte IP packet when using BRI bundled Multilink
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
CSCvw63366	telnet to SN from WCM after upgrade the CSR1k 17.3 to 17.4 CSR8k from vManage
CSCvw65042	SDWAN cEdge memory issue - packet trace failed to enable on 17.3.2
CSCvw70461	17.4 ZBFW:Classification of traffic not happening correctly sometimes when a rule in RS is edited.

Caveat ID Number	Description
CSCvw71941	QFP crash in cpp_ess_tc_tgt_if_fm_edit_helper
CSCvw73701	17.4 ZBFW:Stale ACL entries seen on ASR1K
CSCvw74781	C1111 ARP resolution failure after shut/no shut operation
CSCvw74921	APPNAV CFT crash on ISR

Related Information

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