

# 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
<a href="#">EPC support on LTE interface and FlexVPN interface</a>	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
<a href="#">Change of Authorization and Trustsec</a>	<p>This feature utilizes Posture Assessment capabilities 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.</p> <p>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</p>
<a href="#">Layer 2 Protocol Tunneling on Ports</a>	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
<a href="#">IP-SLA-HTTPS</a>	This feature has enhanced capabilities of IP SLA device tracking with HTTPS probes and helps to verify reachability in the network.
<a href="#">Software Configuration Guide for Catalyst Cellular Gateway</a>	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.
<a href="#">NBAR Support on the EVC Service Instance</a>	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.
<a href="#">VRF Support for CPE WAN Management Protocol</a>	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.
<a href="#">BGP Large Community</a>	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.
<a href="#">Consent Token Authorization Process for Dev Key Access</a>	<p>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.</p> <p><b>Note</b> An image that is signed with a dev-key does not boot due to the absence of dev public key for image verification.</p>
<a href="#">Configuring Stateless Static NAT</a>	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
<a href="#">CUBE: Hunt Stop for Server Groups</a>	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.
<a href="#">CUBE: VoIP Trace Serviceability Framework</a>	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.
<a href="#">CUBE: Clear Hung RTP Ports</a>	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, <b>show voip rtp stats</b> 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.
<a href="#">Unified CME: Smart License Using Policy</a>	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 <a href="https://cisco.com/go/licensingguide">https://cisco.com/go/licensingguide</a> .



**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.

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

## 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
<a href="#">CSCvw84883</a>	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
<a href="#">CSCvt06707</a>	C1111-LTE Observe data stalling after cellular interface has been loaded with data traffic for while
<a href="#">CSCvt71774</a>	C1111 HSRP preempt worked even though HSRP's preempt is not configured
<a href="#">CSCvu04426</a>	ISR1K/4K reloads with erroneous reload cause code
<a href="#">CSCvu65369</a>	Link auto-negotiation fails between C1111-4P ES-4 switch module and Meraki MX100
<a href="#">CSCvv02180</a>	C1113-8PLTEEAWA failed to boot: Package does not support : PID not supported in 17.4
<a href="#">CSCvv43027</a>	VDSL performance impacted if more than two vlan tags are used
<a href="#">CSCvv91575</a>	C1111-8P: NAT translations packet counter MIB OID counts unnecessary additional value
<a href="#">CSCvw31389</a>	pktlog functionality is broken
<a href="#">CSCvs30876</a>	Startup config ETH0/2/0 ???'not shut' command not added to the startup config
<a href="#">CSCvv37172</a>	License lost after "no license boot level <>" CLI followed by reset button
<a href="#">CSCvw49484</a>	Throughput achieved differs between runs and IXIA readings also misleading compared to EIO state
<a href="#">CSCvo44005</a>	ARP storm with varying source mac address causes memory depletion.

## Open Caveats in Cisco IOS XE Bengaluru 17.4.1a

Caveat ID Number	Description
<a href="#">CSCvw42048</a>	C1111 may drop sip messages when sip inspection and zbf
<a href="#">CSCvu65369</a>	Link auto-negotiation fails between C1111-4P ES-4 switch module and Meraki MX100
Caveat ID Number	Description
<a href="#">CSCvt58920</a>	SIM failover within the same modem takes long time to detect LTE network for AT&T
<a href="#">CSCvv44331</a>	AppQoe Clear Alarm is not generated from device
<a href="#">CSCvv68635</a>	Observed HTX core at tcpproxy_libuinet_pkt_process during longevity test
<a href="#">CSCvv78028</a>	No responder-bytes from cEdge when UTD is enabled
<a href="#">CSCvv79072</a>	25G license tags is retained and throughput throttled after upgrade from 17.3.1 to 17.3.2
<a href="#">CSCvv88621</a>	GETVPN: All GM will crash when Primary KS recovers its COOP role after network outage
<a href="#">CSCvv94743</a>	Data Plane fails over L2TPv3 while disabling VLAN limit restrictions with ASR1002-HX
<a href="#">CSCvw11902</a>	Passive FTP doesn't work with NAT
<a href="#">CSCvw13048</a>	crash observed at NHRP while using summary-map
<a href="#">CSCvw33113</a>	Unexpected reload in NHRP when access to an invalid memory region
<a href="#">CSCvw34157</a>	APPNAV CFT Crashes
<a href="#">CSCvw39383</a>	CPP ucode crash with fw_base_flow_create
<a href="#">CSCvw47800</a>	HSL Export over VASI Interface causes Netflow v9 Template Flooding
<a href="#">CSCvw48800</a>	unable to transfer 1500 byte IP packet when using BRI bundled Multilink
<a href="#">CSCvw48943</a>	crypto ikev2 proposals are not processed separately
<a href="#">CSCvw54076</a>	[SIT]: BFD sessions not established between Edges, with UTD enabled
<a href="#">CSCvw58560</a>	FlexVPN reactivate primary peer feature does not work with secondary peer tracking
<a href="#">CSCvw62805</a>	SDWAN ZBFW CPU punted traffic mishandling -- Out2In packet looped
<a href="#">CSCvw63366</a>	telnet to SN from WCM after upgrade the CSR1k 17.3 to 17.4 CSR8k from vManage
<a href="#">CSCvw65042</a>	SDWAN cEdge memory issue - packet trace failed to enable on 17.3.2
<a href="#">CSCvw70461</a>	17.4 ZBFW:Classification of traffic not happening correctly sometimes when a rule in RS is edited.

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

## Related Information

- [Hardware Installation Guide](#)
- [Software Configuration Guide](#)
- [Smart Licensing using Policy](#)

