Release Notes for Cisco 4000 Series ISRs, Cisco IOS XE Cupertino 17.7.x

First Published: 2021-12-17

Cisco 4000 Series Integrated Services Routers Overview

Note Cisco IOS XE Cupertino 17.7.1a is the first release for Cisco 4000 Series Integrated Services Routers in the Cisco IOS XE 17.7.x release series.

The Cisco 4000 Series ISRs are modular routers with LAN and WAN connections that can be configured by means of interface modules, including Cisco Enhanced Service Modules (SM-Xs), and Network Interface Modules (NIMs).

The following table lists the router models that belong to the Cisco 4000 Series ISRs.

Cisco 4400 Series ISR	Cisco 4300 Series ISR	Cisco 4200 Series ISR
Cisco 4431 ISR	Cisco 4321 ISR	Cisco 4221 ISR
Cisco 4451 ISR	Cisco 4331 ISR	
Cisco 4461 ISR	Cisco 4351 ISR	

System Requirements

The following are the minimum system requirements:

Note There is no change in the system requirements from the earlier releases.

- Memory: 4GB DDR3 up to 16GB
- Hard Drive: 200GB or higher (Optional). (The hard drive is only required for running services such as Cisco ISR-WAAS.)
- Flash Storage: 4GB to 32GB

Note There is no change in the flash storage size from the earlier releases. The flash storage size must be equal to the system memory size.

- NIMs and SM-Xs: Modules (Optional)
- NIM SSD (Optional)

For more information, see the Cisco 4000 Series ISRs Data Sheet.

Note For more information on the Cisco WAAS IOS-XE interoperability, refer to the WAAS release notes: https://www.cisco.com/c/en/us/support/routers/wide-area-application-services-waas-software/products-release-notes-list.html

Determining the Software Version

You can use the following commands to verify your software version:

- For a consolidated package, use the **show version** command
- For individual sub-packages, use the **show version installed** command

Upgrading to a New Software Release

To install or upgrade, obtain a Cisco IOS XE 17.7.x consolidated package (image) from Cisco.com. You can find software images at http://software.cisco.com/download/navigator.html. To run the router using individual sub-packages, you also must first download the consolidated package and extract the individual sub-packages from a consolidated package.

Note When you upgrade from one Cisco IOS XE release to another, you may see *%Invalid IPV6 address* error in the console log file. To rectify this error, enter global configuration mode, and re-enter the missing IPv6 alias commands and save the configuration. The commands will be persistent on subsequent reloads.

For more information on upgrading the software, see the Installing the Software section of the Software Configuration Guide for the Cisco 4000 Series ISRs.

Recommended Firmware Versions

Table 1: Recommended Firmware Versions, on page 2 lists the recommended Rommon and CPLD versions for Cisco IOS XE 17.x.x releases.

Table 1: Recommended Firmware Versions

Cisco 4000 Series ISRs	Existing RoMmon	Cisco Field-Programmable Devices
Cisco 4461 ISR	16.12(2r)	15010638 **Note** Upgrade CLI output has a typo and it would show the version incorrectly as 15010738 instead of 15010638. This does not impact the upgrade.

Cisco 4000 Series ISRs	Existing RoMmon	Cisco Field-Programmable Devices
Cisco 4451 ISR	16.12(2r)	15010638 **Note** Upgrade CLI output has a typo and it would show the version incorrectly as 15010738 instead of 15010638. This does not impact the upgrade.
Cisco 4431 ISR	16.12(2r)	15010638 **Note** Upgrade CLI output has a typo and it would show the version incorrectly as 15010738 instead of 15010638. This does not impact the upgrade.
Cisco 4351 ISR	16.12(2r)	14101324
Cisco 4331 ISR	16.12(2r)	14101324
Cisco 4321 ISR	16.12(2r)	14101324
Cisco 4221 ISR	16.12(2r)	14101324

Upgrading Field-Programmable Hardware Devices

The hardware-programmable firmware is upgraded when Cisco 4000 Series ISR contains an incompatible version of the hardware-programmable firmware. To do this upgrade, a hardware-programmable firmware package is released to customers.

Generally, an upgrade is necessary only when a system message indicates one of the field-programmable devices on the Cisco 4000 Series ISR needs an upgrade, or a Cisco technical support representative suggests an upgrade.

From Cisco IOS XE Release 3.10S onwards, you must upgrade the CPLD firmware to support the incompatible versions of the firmware on the Cisco 4000 Series ISR. For upgrade procedures, see the Upgrading Field-Programmable Hardware Devices for Cisco 4000 Series ISRs.

Feature Navigator

You can use Cisco Feature Navigator to find information about feature, platform, and software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn . An account on cisco.com is not required.

New and Changed Information

New and Changed Hardware Features

There are no new hardware features for this release.

New and Changed Software Features

Table 2: New Software Features in Cisco IOS XE 17.7.1a

Feature	Description
Cisco ThousandEyes Enterprise Application Hosting	The Cisco ThousandEyes Enterprise Agent Application introduces the functionality to inherit the Domain Name Server (DNS) information from the device. With this enhancement, the DNS field in vManage ThousandEyes feature template is an optional parameter.
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.
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.
Support for NGE Cipher Suites	This feature supports the Next Generation Encryption (NGE) cipher suites for secure voice signaling and secure media. These cipher suites are applicable for both STCAPP analog phone and SCCP DSPFarm conferencing service. These cipher suites provide confidentiality, integrity, and authenticity to validate messages.
TLS Support on IOS-XE Dataplane	You can now configure Cisco 4000 Series Integrated Services Router to accept remote user access to enterprise networks. This remote access is provided through a Secure Socket Layer (SSL)-enabled SSL VPN gateway that permits remote users to establish a secure VPN tunnel.
Cisco Unified Border Element (CUBE) Features	
CUBE: Secure Web Socket-based Media Forking on Cisco 4431, 4451-X, and 4461 Integrated Services Routers	From Cisco IOS XE Cupertino 17.7.1a, CUBE can use WebSockets to handle media forking with Cloud Speech Services on the Cisco 4431, 4451-X, and 4461 Integrated Services Routers platforms, apart from the existing support on Cisco Catalyst 8000V Edge platform.
CUBE: YANG Configuration Models	From Cisco IOS XE Cupertino 17.7.1a, YANG models are available to configure and manage CUBE.
Programmability Features	
Converting IOS Commands to XML	This feature helps to automatically translate IOS commands into relevant NETCONF-XML or RESTCONF/JSON request messages.

Feature	Description
YANG Model Version 1.1	Cisco IOS XE Cupertino 17.7.1a uses the YANG version 1.0; however, you can download the 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 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.
Smart Licensing Using Policy Features	
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.

Feature	Description
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.
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).

Configure the Router for Web User Interface

This section explains how to configure the router to access Web User Interface. Web User Interface require the following basic configuration to connect to the router and manage it.

- An HTTP or HTTPs server must be enabled with local authentication.
- A local user account with privilege level 15 and accompanying password must be configured.
- Vty line with protocol ssh/telnet must be enabled with local authentication. This is needed for interactive commands.
- For more information on how to configure the router for Web User Interface, see Cisco 4000 Series ISRs Software Configuration Guide, Cisco IOS XE 17.

Resolved and Open Bugs

This section provides information about the bugs in Cisco 4000 Series Integrated Services Routers and describe unexpected behavior. Severity 1 bugs are the most serious bugs. Severity 2 bugs are less serious. Severity 3 bugs are moderate bugs. This section includes severity 1, severity 2, and selected severity 3 bugs.

The open and resolved bugs for this release are accessible through the Cisco Bug Search Tool . This web-based tool provides you with access to the Cisco bug tracking system, which maintains information about bugs and vulnerabilities in this product and other Cisco hardware and software products. Within the Cisco Bug Search Tool, each bug is given a unique identifier (ID) with a pattern of CSCxxNNNNN, where x is any letter (a-z) and N is any number (0-9). The bug IDs are frequently referenced in Cisco documentation, such as Security Advisories, Field Notices and other Cisco support documents. Technical Assistance Center (TAC) engineers

or other Cisco staff can also provide you with the ID for a specific bug. The Cisco Bug Search Tool enables you to filter the bugs so that you only see those in which you are interested.

In addition to being able to search for a specific bug ID, or for all bugs in a product and release, you can filter the open and/or resolved bugs by one or more of the following criteria:

- Last modified date
- Status, such as fixed (resolved) or open
- Severity
- Support cases

You can save searches that you perform frequently. You can also bookmark the URL for a search and email the URL for those search results.

Note If the bug that you have requested cannot be displayed, this may be due to one or more of the following reasons: the bug ID does not exist, the bug does not have a customer-visible description yet, or the bug has been marked Cisco Confidential.

We recommend that you view the field notices for the current release to determine whether your software or hardware platforms are affected. You can access the field notices from the following location:

http://www.cisco.com/en/US/support/tsd_products_field_notice_summary.html

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 in Cisco 4000 Series Integrated Services Routers

This section contains the following topics:

Resolved Bugs - Cisco IOS XE 17.7.1a

All resolved bugs for this release are available in the Cisco Bug Search Tool.

Caveat ID Number	Description
CSCvz98446	VG400 crashed when changing Debug Level.
CSCvy38743	CISCO-CLASS-BASED-QOS-MIB does not work with LTE Cellular interface on ISR1100X after reload.
CSCvz76277	Hostname not allowed beginning with numbers.
CSCvy63924	Telemetry: IOS-XE Controller crashes after using 'show telemetry ietf subscription all' command.
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.

Caveat ID Number	Description
CSCvy53885	ip pim rp-candidate command removed after reload when group list is configured.
CSCvz71436	Call Placing issue from SCCP phones.
CSCvz21812	QoS policy update with "random-detect dscp" configuration get rejected on device side.
CSCvy54964	Large tx/rx rate on Dialer interface in show interface output.
CSCvy08748	OSPF summary-address is not generated though candidate exists.
CSCvy99942	Netconf: Logging to syslog stops working in certain scenarios.
CSCvx62167	Route-map corruption when configured using Netconf with ncclient manager.
CSCvw16093	Secure key agent trace levels set to Noise by default.
CSCvt66541	Crypto PKI-CRL-IO process crash when PKI trustpoint is being deleted.
CSCvy93946	Removal of SHA-1 HMAC Impacting ability to SSH.
CSCwa26599	FN980 new signed Telit modem firmware FN980M_38.02.X92 upgrade failed.
CSCvz58895	IOS-XE unable to export elliptic curve key.
CSCvy22343	Crash after reapplying BGP/ attempt to initialize an initialized wavl tree.
CSCvz84437	8500L // 17.6.1a// Unexpected reload due IPV6 UDP fragment header in VxLAN.
CSCvy63983	vManage showing wrong interface status in GUI.
CSCvy69555	Unable to fetch EIGRP prefix, nexthop, omptag, and route origin.
CSCvz04059	17.6: EFT: Replicated EBGP routes from global table replacing native IBGP routes in VRF.
CSCvy64796	RIP Yang [17.7] offset-list with interface config not shown in IOS running-config.

Open Bugs - Cisco IOS XE 17.7.1a

All open bugs for this release are available in the Cisco Bug Search Tool.

Caveat ID Number	Description
CSCvz92954	C8Kv UTD Container does not come up after a reboot.
CSCwa10809	Kernel crash with last reload reason "LocalSoftADR".
CSCwa07494	IPSec tunnel not passing traffic when IPSec tunnel is sourced from VASI interface.
CSCwa05014	C1121X running 17.3.4a reload: Critical process plogd fault on rp_0_0 (rc=75).
CSCwa46001	VRRP traffic sent while the device boots will congest the interface queue causing taildrops.

Caveat ID Number	Description
CSCwa36830	All ISR4K are showing symmetric in/out traffic on flexible netflow collector.
CSCvz72871	Multicast traffic received over DMVPN tunnel are dropped on RP and not forwarded downstream.
CSCwa27659	Virtual VRRP IP address unreachable from the BACKUP VRRP.
CSCvz41067	IP Community-list config out of sync in SD-WAN and IOS-XE.
CSCwa22665	Memory leak in scaled EIGRP DMVPN implementation due to EIGRP: mgd_timer.
CSCwa11150	E1 configurations (under Serial interface) lost after reload.
CSCvw06937	cEdge: SNMv3 traps failing with initial configuration.
CSCvz86580	Unable to remove the BGP neighbor statement through vManage template.
CSCvz20285	SD-WAN image info not updated in packages.conf when upgrading in autonomous mode.
CSCwa27762	Upgrade is failing on an ISR4331 with an UCS-E160S-M3/K9 module installed.

Related Documentation

- Release Notes for Previous Versions of Cisco 4000 Series ISRs
- Hardware Installation Guide for Cisco 4000 Series Integrated Services Routers
- Configuration Guides for Cisco 4000 Series ISRs
- Command Reference Guides for Cisco 4000 Series ISRs
- Product Landing Page for Cisco 4000 Series ISRs
- Datasheet for Cisco 4000 Series ISRs
- Upgrading Field-Programmable Hardware Devices for Cisco 4000 Series ISRs
- Field Notices
- Cisco Bulletins