Release Notes for Cisco 4000 Series ISRs, Cisco IOS XE Bengaluru 17.5.x

First Published: 2021-03-22

Last Modified: 2021-03-31

Cisco 4000 Series Integrated Services Routers Overview

Note Cisco IOS XE Bengaluru 17.5.1a is the first release for Cisco 4000 Series Integrated Services Routers in the Cisco IOS XE Bengaluru 17.5.1 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	

Note Starting with Cisco IOS XE Amsterdam 17.3.2 release, 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).

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 Begaluru 17.5.1a 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 How to Install and Upgrade the Software section of the Software Configuration Guide for the Cisco 4000 Series ISRs.

Recommended Firmware Versions

The following table lists the recommended Rommon and CPLD versions for Cisco IOS XE 17.2.x onwards releases.

Table 1: Recommended Firmware Versions

Cisco 4000 Series ISRs	Existing RoMmon	Cisco Field-Programmable Devices	CCO URL for the CPLD Image
Cisco 4461 ISR	16.12(2r)	21102941	isr_4400v2_cpld_update_v20.SPA.bin isr4400v2hwprogrammable040100.SPA.pkg
Cisco 4451 ISR	16.12(2r)	19042950	isr4400_cpld_update_v20.SPA.bin
Cisco 4431 ISR	16.12(2r)	19042950	isr4400_cpld_update_v20.SPA.bin
Cisco 4351 ISR	16.12(2r)	19040541	isr4300_cpld_update_v20.SPA.bin
Cisco 4331 ISR	16.12(2r)	19040541	isr4300_cpld_update_v20.SPA.bin
Cisco 4321 ISR	16.12(2r)	19040541	isr4300_cpld_update_v20.SPA.bin
Cisco 4221 ISR	16.12(2r)	19042420	isr4200_cpld_update_v20.SPA.bin

Note Cisco 4461 ISR may require two upgrade packages to upgrade to 21102941. See CPLD-4-1 Release Notes.

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 Hardware Features in Cisco IOS XE 17.5.1

There are no new hardware features for this release.

New Software Features in Cisco 4000 Series ISRs Release Cisco IOS XE 17.5.1

Table 2: New Software Features in Cisco 4000 Series ISRs Release Cisco IOS XE Bengaluru 17.5.1

Feature	Description
Capability to limit IPv6 Mroutes Per VRF	This feature lets you configure a limit to the number of mroutes on an interface. By limiting the mroutes, you can avoid the risk of flooding the network with mroutes therefore protecting the router from resource overload and also preventing DoS attacks.
Cisco IS-IS Local Unequal Cost Multipath	The Segment Routing—IS-IS UCMP feature allows you to load balance outgoing traffic across all IGP ECMP paths proportionally to the interface bandwidth.
Configuring Dynamic ARP Inspection	Dynamic ARP Inspection (DAI) validates Address Resolution Protocol (ARP) packets in a network. With DAI, you can intercept, log, and discard ARP packets with invalid MAC address to IP address bindings. This capability protects the network from certain man-in-the-middle attacks.
Configuring EVPN VXLAN External Connectivity	You can configure the EVPN VXLAN external connectivity for enterprise routers. External connectivity refers to the movement of Layer 2 and Layer 3 traffic between an EVPN VXLAN network and an external network. This enables the EVPN VXLAN network to exchange routes with the externally connected network.
Configuring Interface Template	An interface template is a container of configurations or policies that can be applied to specific ports. This feature allows you to configure an IPV4 or IPv6 ACL in the interface template for the Cisco SM-X EtherSwitch module.
Configuring IPv6 First Hop Security	The Switch Integrated Security Feature (SISF) based device tracking feature is part of the suit of first hop security features. This feature allows to track the presence, location, and movement of end-nodes in the network. The First Hop Security features are supported as a part of device tracking policy: • Static IPv6 Address Bind • IPv6 Address Glean, Inspection, and Guard • IPv6 Device Tracking • IPv6 Binding Recovery
Configuring Per-Interface Per-Cause Punt Policer	The per-interface per-cause (PIPC) punt policing is an enhancement to the punt policing and monitoring feature that allows you to configure the limit on traffic per interface. Starting from the Cisco IOS XE 17.5.1 release, you can set the per-interface per-cause rate for all the control plane punted traffic. This rate causes any traffic beyond the set limit to be dropped, therefore allowing you to control the traffic during conditions such as L2 storming.

Feature	Description
ISIS: Flex Algo: Support for Affinity Include any/all	This feature allows you to customize IGP shortest path computation according to your needs. You can assign custom SR prefix-SIDs to forward the packets beyond link-cost-based SPF. As a result, a traffic engineered path is automatically computed by the IGP to any destination reachable by the IGP.
Traffic Steering by Dropping Invalid Paths	If the SR-TE Policy has no valid paths defined, the paths are dropped and traffic being steered through the policy falls back to the default (unconstrained IGP) forwarding path. Also, when a SR-TE policy carrying best-effort traffic fails, traffic is re-routed and this impacts the SLA for premium traffic.To solve this issue, if the SR-TE policy fails, the traffic in the data plane is dropped but kept in the controlplane. Therefore, other SR policies, potentially carrying premium traffic, are not impacted.
Tunnel Path MTU discovery on MPLS-enabled GRE tunnel	You can now use the tunnel mpls-ip-only command to configure how the Do Not Fragment bit from the payload is copied into the tunnel packets IP header.If the Do Not Fragment bit is not set, the payload is fragmented if an IP packet exceeds the MTU set for the interface.
View traffic counters for SR-TE policies	You can now view the traffic counters of SR-TE policies using the show segment-routing traffic-eng policy command.
License Management for Smart Licensing Using Policy, Using Cisco vManage	Cisco SD-WAN operates together with Cisco SSM to provide license management through Cisco vManage for devices operating with Cisco SD-WAN. For this you have to implement a topology where Cisco vManage is connected to CSSM. For information about this topology, see the Connected to CSSM Through a Controller, and to know how to implement it, see the Workflow for Topology: Connected to CSSM Through a Controller sections of the *Smart Licensing Using Policy for Cisco Enterprise Routing Platforms* guide. For more information about Cisco vManage, see the License Management for Smart Licensing Using Policysection of the *Cisco SD-WAN Getting Start Guide*. For a more detailed overview on Cisco Licensing, go to cisco.com/go/licensingguide.
Webex Calling VG400 Integration	Webex calling support for IOS XE based VG400 analog voice gateways to support interoperability between analog devices and Webex calling endpoints.

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

Using the Cisco Bug Search Tool

For more information about how to use the Cisco Bug Search Tool , including how to set email alerts for bugs and to save bugs and searches, see Bug Search Tool Help & FAQ .

Before You Begin

Note You must have a Cisco.com account to log in and access the Cisco Bug Search Tool . If you do not have one, you can register for an account.

Procedure

Step 1 In your browser, navigate to the Cisco Bug Search Tool .

Step 2 If you are redirected to a Log In page, enter your registered Cisco.com username and password and then, click Log In.

Step 3 To search for a specific bug, enter the bug ID in the Search For field and press Enter.

Step 4 To search for bugs related to a specific software release, do the following:

a) In the Product field, choose Series/Model from the drop-down list and then enter the product name in the text field. If you begin to type the product name, the Cisco Bug Search Tool provides you with a drop-down list of the top ten matches. If you do not see this product listed, continue typing to narrow the search results.

b) In the Releases field, enter the release for which you want to see bugs.

The Cisco Bug Search Tool displays a preview of the results of your search below your search criteria.

Step 5 To see more content about a specific bug, you can do the following:

- Mouse over a bug in the preview to display a pop-up with more information about that bug.
- Click on the hyperlinked bug headline to open a page with the detailed bug information.

Step 6 To restrict the results of a search, choose from one or more of the following filters:

Filter	Description
Modified Date	A predefined date range, such as last week or last six months.
Status	A specific type of bug, such as open or fixed.
Severity	The bug severity level as defined by Cisco. For definitions of the bug severity levels, see Bug Search Tool Help & FAQ .
Rating	The rating assigned to the bug by users of the Cisco Bug Search Tool .
Support Cases	Whether a support case has been opened or not.

Your search results update when you choose a filter.

Resolved and Open Bugs in Cisco 4000 Series Integrated Services Routers

Open Bugs - Cisco IOS XE 17.5.1

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

Caveat ID Number	Description
CSCvx07578	Cisco 4461 ISR: MACsec should secure mode not work with front panel GE
CSCvw69411	OC: unable to configure interface negotiation and speed via netconf rcp.
CSCvx32670	Wrong reload reason reflected after a power outage.

Caveat ID Number	Description
CSCvw79230	CTS enforcement doesn't work properly on Tunnels.

Resolved Bugs - Cisco IOS XE 17.5.1

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

Caveat ID Number	Description
CSCvv33576	IGMP snooping table not populated on Cisco 4000 Series ISR
CSCvw23041	Crash with high netflow traffic due to %CPPHA-3-FAILURE: R0/0: cpp_ha: CPP 0 failure Stuck Thread(s)
CSCvw47800	HSL Export over VASI Interface causes Netflow v9 Template Flooding
CSCvw48800	Unable to transfer 1500 byte IP packet when using BRI bundled Multilink
CSCvw91925	Cisco 4400 ISR: FHS Local entry stays down after configuring a SVI interface with same mac twice
CSCvw72995	Client is permitted with ip traffic when urlacl is configured to permit only https traffic
CSCvw23104	Dhcp snooping binding entries are not getting learnt again after delete-add vlan in snooping switch
CSCvw61132	%PARSER-5-HIDDEN: Warning!!! ' resume server /connect telnet server' is a hidden command.

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