Release Notes for Cisco ISR 1000 Series, Cisco IOS XE Amsterdam 17.x

First Published: 2019-10-24

Last Modified: 2019-12-03

About Cisco 1000 Series Integrated Services Routers

The Cisco 1000 Series Integrated Services Routers (ISR) 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 Cisco 1100 Series ISRs.

For more information on upgrading software, installing software, and ROMMON and upgrading procedures of Cisco 1100 Series Integrated Services Routers (ISRs), refer to the following:

- Software Configuration Guide for Cisco 1000 Series ISRs
- ROMMON Overview and Basic Procedures
- Cisco 1000 Series Integrated Services Routers Solution Overview
- Datasheet for 1000 Series Integrated Services Routers

Note Explore Content Hub, the all new portal that offers an enhanced product documentation experience. Content Hub offers the following features to personalize your content experience:

- Faceted Search to find relevant content
- Customized PDFs
- Contextual recommendations

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 Hardware Features

No new or changed hardware features for Cisco IOS XE Gibraltar 17.1.x release.

New and Changed Software Features

The following are the new software features introduced in Cisco IOS XEAmsterdam 17.1.x release:

- **Debug Messages for OSPF LSA MaxAge Events**:

  To display debug messages about OSPF LSA MaxAge events, use the following commands:

  debug ip ospf lsa-maxage

  debug ospfv3 lsa-maxage

- Group Domain of Interpretation: Group Domain of Interpretation (GDOI) includes the ability of a Key Server (KS) to provide a set of current Group Member (GM) devices with additional security associations. RFC 8263 has added the ability of a KS to request that the GM devices return an acknowledgement of its rekey message and specifies the acknowledgement method.

- Mapping of Address with Port Encapsulation for CPE Functionality Support: MAP-E for CPE Functionality Support is an IPv6 transition mechanism for transporting IPv4 packets across an IPv6 network using IP encapsulation. With MAP-E, the IPv4 address exhaustion is resolved using the multiple CPEs sharing the same public IPv4 address.

  Note MAP-E CPE functionality is supported from IOS XE Amsterdam 17.1.1 release.

- Stronger Network Time Protocol Authentication: The authentication keys of Network Time Protocol and Simple Network Time Protocol (SNTP) uses cryptographic options, such as CMAC, SHA-1, and SHA-256 to enhance the security of the message exchange of NTP and SNTP.

- **Suppression of ESI Re-frame Errors During Upgrade or OIR**: ESI re-frame errors are expected after an OIR or upgrade of a line card. These errors do not indicate faulty behaviour and need no troubleshooting. This feature supresses ESI re-frame error messages after an OIR or upgrade so that you need not investigate a normal behaviour.

- Link Delay Measurement for SR-TE: You can define and associate an Access Control List (ACL) with an SVTI to select traffic between specific source and destination proxies. By associating the ACL, you modify the default configuration that uses a single any any traffic selector. IPSec SAs are created for each non-any-any traffic selector, and thus, multiple SAs may be attached to an SVTI.

- **Web UI-RIP Support**: Supports an embedded GUI-based device-management tool that provides the ability to provision the router, simplifies device deployment and manageability, and enhances user experience.

  From Cisco IOS XE Amsterdam 17.1.1, the following feature is supported on Web User Interface:

  - Configuring the Routing Information Protocol

Open and Resolved Bugs for Cisco IOS XE Amsterdam 17.1.x

This section provides information about the caveats in Cisco 1100 Series Integrated Services Routers and describe unexpected behavior. Severity 1 caveats are the most serious caveats. Severity 2 caveats are less serious. Severity 3 caveats are moderate caveats. This section includes severity 1, severity 2, and selected severity 3 caveats.

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 defect that you have requested cannot be displayed, this may be due to one or more of the following reasons: the defect number does not exist, the defect does not have a customer-visible description yet, or the defect 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:

Product Field Notice Summary

Open Bugs in Cisco IOS XE Amsterdam 17.1.x

Caveat ID Number	Description
CSCvr13149	Multicast VRF Nat not working properly
CSCvr21113	APN password in clear text when configuring profile under cellular controller.
CSCvr26524	Crash due to NBAR classification
CSCvr43037	"sh macsec statistics int <>" and "sh macsec status interface <>" does not show output
CSCvr62666	IPSec background crash after entered command clear cry sa peer <ip address>
CSCvr89957	CFT crashed frequently
CSCvr89973	NIM interfaces go into shutdown after router bootup.
CSCvs00410	MKA session up but unable to pass data across link using AES-256-XPN cipher
CSCvs12349	NeMo tunnel is down after cellular interface config is overwritten

Caveat ID Number	Description
CSCvj71660	After IP change due to NAT IKEv2 IPSec Tunnel drops ESP packets but still responds to DPDs

Resolved Bugs in Cisco IOS XE Amsterdam 17.1.x

Caveat ID Number	Description
CSCvr43037	"sh macsec statistics int <>" and "sh macsec status interface <>" does not show output
CSCvb16018	TLS GW: Serviciability

Related Documentation

- Smart Licensing Guide for Access and Edge Routers
- Open Source Used In Cisco 1100 Series Integrated Services Router
- Command References Cisco 1000 Series Integrated Services Routers