Release Notes for Cisco 4000 Series ISRs, Cisco IOS XE Gibraltar 16.11.x

First Published: 2019-03-19

Last Modified: 2019-03-19

Cisco 4000 Series Integrated Services Routers Overview

Note Explore the Content Hub, the all new portal that offers an enhanced product documentation experience.

- Use faceted search to locate content that is most relevant to you.
- Create customized PDFs for ready reference.
- Benefit from context-based recommendations.

Get started with the Content Hub at content.cisco.com to craft a personalized documentation experience.

Do provide feedback about your experience with the Content Hub.

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).

Note The Cisco IOS XE Bengaluru 17.4.1a is the first release for Cisco 4000 Series Integrated Services Routers in the Cisco IOS XE Bengaluru 17.4.1 release series.

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.

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 Gibraltar 16.12.1a 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

Table 1: Recommended Firmware Versions, on page 3 provides information about the recommended Rommon and CPLD versions for releases prior to Cisco IOS XE Everest 16.4.1.

Table 1: Recommended Firmware Versions

Cisco 4000 Series ISRs	Existing RoMmon	Cisco Field-Programmable Devices
Cisco 4451 ISR	16.7(4r)	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	16.7(4r)	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	16.7(5r)	14101324
Cisco 4331 ISR	16.7(5r)	14101324
Cisco 4321 ISR	16.7(5r)	14101324
Cisco 4221 ISR	16.7(5r)	14101324

Upgrading the ROMMON Version on the Cisco 4000 Series ISR

For information about ROMMON compatability matrix, and ROMMON upgrading procedure, see the ROMMON Compatability Matrix and "ROMMON Overview and Basic Procedures" sections in the Upgrading Field-Programmable Hardware Devices for Cisco 4000 Series ISRs.

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.

Limitations and Restrictions

The following limitations and restrictions apply to all releases:

• Cisco Unified Threat Defense , on page 4

Cisco Unified Border Element

Cisco Unified Border Element on Cisco IOS XE Gibraltar Release 16.11.1 is not a recommended version for Media Forking and call flows that include Multicast Music On Hold (MMOH).

Unified CME and Unified SRST

Unified CME 12.6 and Unified SRST 12.6 on Cisco IOS XE Gibraltar Release 16.11.1 is not a recommended version for call flows that include Multicast Music On Hold (MMOH).

Unified Secure SRST

Unified Secure SRST 12.6 on Cisco IOS XE Gibraltar Release 16.11.1 is not a recommended version for Unified Secure SCCP SRST and stcapp call flows.

Cisco Unified Threat Defense

The Cisco Unified Threat Defense (UTD) service requires a minimum of 1 to 4 GB of DRAM.

Cisco ISR-WAAS and AppNav-XE Service

The Cisco ISR-WAAS/AppNav service requires a system to be configured with a minimum of 8GB of DRAM and 16GB flash storage. For large service profiles, 16GB of DRAM and 32GB flash storage is required. Also, Cisco ISR-WAAS requires a minimum of 200GB SSD.

IPsec Traffic

IPsec traffic is restricted on the Cisco ISR 4451-X. The router has the same IPsec functionality as a Cisco ISR G2. The default behavior of the router will be as follows (unless an HSECK9 license is installed):

- If the limit of 1000 concurrent IPsec tunnels is exceeded, no more tunnels are allowed and the following error message appears:

```
%CERM-4-TUNNEL_LIMIT: Maximum tunnel limit of 1000 reached for Crypto functionality with
securityk9 technology package license.
```

- The throughput encrypted traffic supports 250 Mbps.
- The Cisco 4000 Series ISR does not currently support nested SA transformation such as:

```
crypto ipsec transform-set transform-1 ah-sha-hmac esp-3des esp-md5-hmac
crypto ipsec transform-set transform-1 ah-md5-hmac esp-3des esp-md5-hmac
```

- The Cisco 4000 Series ISR does not currently support COMP-LZS configuration.

USB Etoken

USB Etoken is not supported on Cisco IOS XE Denali 16.2.1.

Yang Data Models

Effective with Cisco IOS XE Everest 16.5.1b, the Cisco IOS XE YANG models are available in the form of individual feature modules with new module names, namespaces and prefixes. Revision statements embedded in the YANG files indicate if there has been a model revision.

Navigate to *https://github.com/YangModels/yang* > *vendor* > *cisco* > *xe* >*1651*, to see the new, main cisco-IOS-XE-native module and individual feature modules attached to this node.

There are also XPATH changes for the access-list in the *Cisco-IOS-XE-acl.yang* schema.

The *README.md* file in the above Github location highlights these and other changes with examples.

CTI Configuration

CME does not support CTI configurations on Cisco 4000 Series ISRs.

New and Changed Information

New Hardware Features in Cisco IOS XE Gibraltar 16.11.1a

There are no new hardware features for this release.

New Software Features in Cisco 4000 Series ISRs Release Cisco IOS XE Gibraltar 16.11.1a

The following features are supported by the Cisco 4000 Series Integrated Services Routers for Cisco IOS XE Gibraltar 16.11.1:

- Channel-Based Metrics Measurement—Configures the performance monitors used by PfRv3 to employ a data collection method combining metadata and traffic sampling to provide traffic metrics.

- Cisco Unified Border Element Smart Licensing—Cisco Unified Border Element Smart Licensing—Cisco Smart Software Licensing provides a simple cloud-based solution for managing and tracking the use of your licenses and entitlements across your business. License requirements for the use of CUBE trunk sessions are reported to Cisco Smart Licensing.

  For a more detailed overview on Cisco Licensing, go to https://cisco.com/go/licensingguide.

- CPE WAN Management Protocol for Cellular Interfaces—CPE WAN Management Protocol (CWMP), is used for communications between a customer premise equipment (CPE) and an auto-configuration server (ACS). The TR-069 Agent feature manages a collection of CPEs, with the primary capability for auto-configuration and dynamic service provisioning, software image management, status and performance monitoring and diagnostics. With the addition of CWMP support on cellular interfaces, an ACS can establish a connection with a CPE, over cellular network and implement traffic monitoring.

- Configuring Dynamic Application Policy Routing—Dynamic Application Policy Routing (DAPR) dynamically steers overlay and underlay egress application traffic flows between multihomed sites connected over RAR links (virtual-access interfaces). This feature extends the existing path management solution of PfRv2 to virtual access interfaces. DAPR routes your traffic based on policy criteria such as link preference and load balancing to meet performance requirements such as delay and jitter.

- Enhanced Policy Based Routing – Application-Based Routing—The Enhanced Policy-based Routing (ePBR) routing enables application-based routing. Application-based routing provides a flexible, device-agnostic policy routing solution, while also ensuring application performance.

- PfRv3 Intelligent Load Balance—The PfRv3 Intelligent Load Balance feature detects the remote bandwidth overrun at the earliest possible. It helps to reduce the packet drop caused by per tunnel QoS and increases the bandwidth utilization.

- FlexVPN Event Trace—Displays event trace messages for FlexVPN.

- IPv6 Object Group ACL—This feature extends object group-based policy application to IPv6 ACLs. The Object group for access control list (ACL) allows you to classify users, devices, or applications into groups and apply those groups to ACLs to create access control policies for those groups. Object group-based ACL approach reduces configuration size, makes ACLs easily readable and easier to manage, thus minimizing complex and larger ACL configurations.

- Kill Telemetry Subscription—The ability to delete a dynamic model driven telemetry dynamic subscription using either:
  - The clear telemetry ietf subscription Cisco IOS command, or
    - The <kill-subscription> RPC

- IPFIX Support for ETA—IP Flow Information Export (IPFIX) protocol is another way for transmitting traffic flow information over the network. Support for ipfix keyword in flow destinations was added.

- Mapping of Address and Port using Translation and Encapsulation—The MAP-E feature in this release complements the existing MAP-T capability by providing connectivity to IPv4 hosts across IPv6 domains on CE devices while encapsulating the original IPv4 packet. MAP-E also enables mapping of address between IPv6 and IPv4 addresses, and across transport layer ports. Additionally, the CE device performs NAPT44 translation between a customer private IPv4 address and the MAP-E NAT64 translation to ensure that different CE devices share a common public IPv4 address.

- NETCONF and RESTCONF Service Level Access Control Lists—Enable you to configure an IPv4 or IPv6 access control list (ACL) for NETCONF and RESTCONF sessions.Clients that do not conform to the configured ACL are not allowed to access the NETCONF or RESTCONF subsystems. When service-level ACLs are configured, NETCONF and RESTCONF connection requests are filtered based on the source IP address.

- PKI-EST CA Certs on Reykey—This feature enables client devices to obtain CA certificate automatically as part of rekey. The CA certificate certifies a new public key for a device.

- ROMMON Upgrade—ROMMON upgrade is a bootstrap program that initializes the hardware and boots the Cisco IOS XE software when you power on or reload a device.

- Security Enhanced (SE) Linux Permissive Mode—Makes it possible for the practical implementation of “principle of least privilege” by enforcing Mandatory Access Control (MAC) on the IOS-XE platform. SELinux provides the capability to define policies to control the access from an application process to any resource object, thereby allowing for the clear definition and confinement of process behavior. In this introductory release for the feature, operation in a permissive mode is available - with the intent of confining specific components (process or application) of the IOS-XE platform. In the permissive mode, access violation events are detected and system logs are generated, but the event or operation itself is not blocked. The solution operates mainly in an access violation detection mode. No user configuration is required for the feature. See Interface and Hardware Commands. (Network Essentials and Network Advantage)

- Security Readiness Criteria (SRC) Closure—Security Readiness Criteria (SRC) closure for Cisco Unified Border Element—SRC is a program to meet a set of security criteria before releasing the product offering to the customers. SRC helps to prioritize security requirements that are necessary to reduce the associated risk. For detailed information: see the following Cisco documents:
  - SRTP-SRTP Interworking
  - Network-Based Recording Using CUBE
  - Overview of Cisco Unified Border Element
  - Commands—authentication (dial peer), authentication (SIP UA), credentials (SIP UA)
  - Command—stun flowdata shared-secret

- Specific License Reservation—With Specific License Reservation, you can deploy a Smart License on a device without directly connecting it to the Cisco Cloud.

- SRC Closure-CME—In accordance with the SRC compliance requirements, Unified CME and Unified SRST 12.6 Release introduces support for Simple Network Management Protocol Version 3 (SNMPv3), Toll Fraud Prevention for Line Side SIP, and enforces adherence to password policy and encryption guidelines. Unified CME 12.6 and later releases do not support Graphical User Interface and Computer Telephony Integration (CTI) Computer Supported Telecommunications Applications (CSTA) protocol suite.

- Support for SCRYPT as Default Encryption Type: Support for SCRYPT as the Default Encryption Type: The CLI parser view supports SCRYPT as the default type from Cisco IOS XE Gibraltar 16.11.1. Additionally, the CLI parser view also supports the encryption type PBKDF2 from this release.

- Source Interface Support for ETA Netflow Records—Support for source-interface interface-name for ETA Netflow records was added.

- Show Commands for ETA—Simplified show commands to display ETA configurations, flow statistics, and export statistics for quick troubleshooting.

- Support Certificate CN/SAN Validation—

  Server Identity Validation on Cisco Unified Border Element—Cisco Unified Border Element supports server identity validation through Common Name (CN) and Subject Alternate Name (SAN) fields in the server certificate during client-side SIP/TLS connections. Validation of CN and SAN fields of the server certificate ensures that the server-side domain is a valid entity.

- Web User Interface—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. The following features are supported on Web User Interface from Cisco IOS XE Gibraltar 16.11.1:
  - Nat Statistics
  - IPv6 Support for AAA
  - For information on how to access the Web User Interface, see Configure the Router for Web User Interface section.

- YANG Data Models—For the list of Cisco IOS XE YANG models available with this release, navigate to https://github.com/YangModels/yang/tree/master/vendor/cisco/xe/16111. Revision statements embedded in the YANG files indicate if there has been a model revision. The README.md file in the same GitHub location highlights changes that have been made in the release.

Configure the Cellular Back-off Operation

For a router with 3G/4G interface, sometimes service provider network might be busy, congested, in maintenance or in fault state. In such circumstances, service provider network rejects session activation request from the router by returning reject cause code 33 as a response of the activation request. After the router receives the reject cause, the router uses the back-off operation with the pre-defined timer value which could be carrier-specific. While back-off operation is in progress, no new session activation request is sent out from the router. After the back-off period is up, new session activation request is sent out from the router.

Note: There is no command to disable the cellular back-off feature on the router.

The following example shows how to configure the cellular back-off feature to stop continuous session activation requests back to the router:

```
Router#show cell 0/2/0 all
Profile 1, Packet Session Status = INACTIVE
Profile 2, Packet Session Status = INACTIVE
Profile 3, Packet Session Status = INACTIVE
.
.
.
Success rate is 0 percent (0/5)
Router#show cell 0/2/0 c
Profile 1, Packet Session Status = INACTIVE
Profile 2, Packet Session Status = INACTIVE
Profile 3, Packet Session Status = INACTIVE
RouterCall end mode = 3GPP
RouterSession disconnect reason type = 3GPP specification defined(6)
RouterSession disconnect reason = Option unsubscribed(33)
RouterEnforcing cellular interface back-off
 Period of back-off = 1 minute(s)
Profile 4, Packet Session Status = INACTIVE
...
Profile 16, Packet Session Status = INACTIVE

.
.
.
Profile 16, Packet Session Status = INACTIVE
```

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.

Entering the Configuration Commands Manually

To enter the Cisco IOS commands manually, complete the following steps:

Before you begin

If you do not want to use the factory default configuration because the router already has a configuration, or for any other reason, you can use the procedure in this section to add each required command to the configuration.

Procedure

Step 1 Log on to the router through the Console port or through an Ethernet port.

Step 2 If you use the Console port, and no running configuration is present in the router, the Setup command Facility starts automatically, and displays the following text:

```
--- System Configuration Dialog ---

Continue with configuration dialog? [yes/no]:
```

Enter no so that you can enter Cisco IOS CLI commands directly.

If the Setup Command Facility does not start automatically, a running configuration is present, and you should go to the next step.

Step 3 When the router displays the user EXEC mode prompt, enter the **enable** command, and the enable password, if one is configured, as shown in the following example:

```
Router> enable
password password
```

Step 4 Enter config mode by entering the **configure terminal** command, as shown in the following example.

```
Router> config terminal
Router(config)#
```

Step 5 Using the command syntax shown, create a user account with privilege level 15.

Step 6 If no router interface is configured with an IP address, configure one so that you can access the router over the network. The following example shows the interface GigabitEthernet 0/0/0 configured.

```
Router(config)# interface gigabitethernet 0/0/0
Router(config-if)# ip address 10.10.10.1 255.255.255.248
Router(config-if)# no shutdown
Router(config-if)# exit
```

Step 7 Configure the router as an http server for nonsecure communication, or as an https server for secure communication. To configure the router as an http server, enter the **ip http server** command shown in the example:

```
Router(config)# ip http secure-server
```

Step 8 Configure the router for local authentication, by entering the ip http authentication local command, as shown in the example:

```
Router(config)# ip http authentication local
```

Step 9 Configure the vty lines for privilege level 15. For nonsecure access, enter the transport input telnet command. For secure access, enter the transport input telnet ssh command. An example of these commands follows:

```
Router(config)# line vty 0 4
Router(config-line)# privilege level 15
Router(config-line)# login local
Router(config-line)# transport input telnet
Router(config-line)# transport output telnet
Router(config-line)# transport input telnet ssh
Router(config-line)# transport output telnet ssh
Router(config-line)# exit
Router(config)# line vty 5 15
Router(config-line)# privilege level 15
Router(config-line)# login local
Router(config-line)# transport input telnet
Router(config-line)# transport output telnet
Router(config-line)# transport input telnet ssh
Router(config-line)# transport output telnet ssh
Router(config-line)# end
```

Resolved and Open Bugs

This section provides information about the caveats in Cisco 4000 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:

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

This section contains the following topics:

Open Bugs - Cisco IOS XE Gibraltar 16.11.a

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

Caveat ID Number	Description
CSCvo04856	DataPlane (DP) crash observed in MMOH call flow
CSCvo17113	Show call media Forking match failed.
CSCvo47436	IOSXE - firewall corrupts half open list
CSCvo60849	Crash noticed when routes are getting imported twice(from vpnv4 to vrf to evpn) with route churn
CSCvo66216	IPSec-Session count in "show crypto eli" reaches max causing VPN failure
CSCvo79193	Router configured with ZBFW reloads with a last reload reason of LocalSoft
CSCvo12799	Call is not getting connected in Forking Re-INVITE scenario.
CSCvo17113	Show call media forking match failed.
CSCvo04856	DataPlane (DP) crash observed in MMOH call flow.
CSCvo00221	Crash observed on secure srst with secure sccp and stcapp configs.

Resolved Bugs - Cisco IOS XE Gibraltar 16.11.1a

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

Caveat ID Number	Description
CSCvb03610	Watchdog crash after "% AAA/AUTHEN/CONT: Bad state in aaa_cont_login().".
CSCvh57657	NAT MIB not populated when using traditional NAT.
CSCvi32156	Router crashes when DMVPN tunnel moves accoss ports.
CSCvi58996	Several OID from CISCO-CLASS-BASED-QOS-MIB stop working when performing upgrade to Denali-16.3.x.
CSCvi63425	Cisco 4400 ISR router cpp crashed when configured HSRP with PMIPv6.
CSCvi79674	CPP 0 failure Stuck Thread resulting in Unexpected Reboot.
CSCvi81216	Cisco 4000 Series ISRs: Ping src Looback(lo is EID) has been dropped after reloading.

Caveat ID Number	Description
CSCvj02081	CPP crash on L2TP router.
CSCvj08248	Packet throughput drops down when enable tunnel visibility with single tcp flow(>1MPPS).
CSCvj11876	Provide Passthrough Reason in IOS-XE for AppNav.
CSCvj13382	IOS-XE FIPS mode is enabled by default in QFP even if it is not enabled in CLI.
CSCvj17326	Cisco 4400 ISR crashes in o2_cavm_pci_unlock when forwarding large packets for VPLS.
CSCvj20302	Cisco 4000 Series ISRs MTP not performing RFC2833 payload type conversion.
CSCvj47957	Packet trace does not work with re-injected UTD packets.
CSCvj50005	Cisco 4000 Series ISRs PPE ucode crash when processing ipsec traffic on CWS tunnel.
CSCvj50410	Cisco 4331 ISR no collisions count up on duplex mismatch condition.
CSCvj71853	"sdavc_ppdk.pack force" command not accepted during boot up.
CSCvj76662	GetVPN TBAR failure does not generate syslogs.
CSCvj78083	Path of Last Resort Sending Probes in standby state.
CSCvj86876	Cisco 4000 Series ISRs- IOS 16.8 - crypto-related issues seen with a single AF configured in VRF definition.
CSCvj89345	AVC license should be activated only in case of smart licensing model.
CSCvj90814	Crash due to Memory corruption in Cisco 4000 Series ISRs.
CSCvk00074	cBR-8 crash after issuing show platform hardware qfp active infrastructure bqs.
CSCvk02072	Hoot-n-holler multicast traffic marked with DSCP 0.
CSCvo47436	IOS XE - firewall corrupts half open list.
CSCvo49381	LISP to OSPF redistribution failing.
CSCvk12152	Unable to remove command ip nat inside destination.
CSCvk15062	Modification to ZBFW access-lists do not reflect in TCAM.
CSCvk34152	Invalid throughput level in the "show version" output.
CSCvk53938	IOS-XE : IPv6 ACL for Tunnel QoS not matched.
CSCvk63602	WAAS Policy Configuration push may caused AppNav Class-maps programming issue in TCAM.
CSCvk65072	Crash due ZBF + NAT.

Caveat ID Number	Description
CSCvm08377	IPSEC in DOWN-NEGOTIATING on HSRP Standby router with local-address config
CSCvm14346	Cisco 4000 Series ISR - Memory Corruption of mdl_tbl due to fia-history CLI
CSCvm20374	Router - CPUHog - SNMP ENGINE crashed with Watchdog timeout.
CSCvm56670	ACL dropping packets after updating it - %CPPEXMEM-3-NOMEM.
CSCvm76295	[SAP] syncfd fails to start on reload after upgrade to new ES image.
CSCvm80502	Traceroute not working when sourced from NAT Inside interface.
CSCvm94970	[UniScale]Crash seen on csr1k during NAT44 hsl scale test when clearing max NAT translations.
CSCvm96663	An IOS-XE router crashes after umbrella is configured.
CSCvn02419	Router crash occurs while running Dell software update.
CSCvn07614	Out of Band DTMF Events Not Passing to CUCM via SCCP When Using IOS MTP.
CSCvn13257	Unable to reconfigure VTY lines on Cisco 4221 once deleted
CSCvn31658	Removal of loopback interface causes router to crash and erases the conf register settings.
CSCvn37915	Crash in cpp_bqs_rm_yoda_proc_pend_fc_cb.
CSCvn40315	FMANFP-6-IPACCESSLOGP message have IP address byte reversed.
CSCvn46969	Cisco 4000 Series ISRs: hang up when executing "sh ip nat tran" with static NAT entries.
CSCvn51553	QFP crashes with a HW interrupt.
CSCvn82245	EIGRP session is not coming up if the dynamic PBR is applied on interface.
CSCvo00664	SUP Crash after running the command " show plat hard qfp act infr bqs debug qmrt_dump ".

Related Documentation

Platform-Specific Documentation

For information about the Cisco 4000 Series ISRs and associated services and modules, see:

Documentation Roadmap for the Cisco 4000 Series ISRs,Cisco IOS XE 16.x .

Cisco IOS Software Documentation

The Cisco IOS XE Fuji 16.x software documentation set consists of Cisco IOS XE Fuji 16.x configuration guides and Cisco IOS command references. The configuration guides are consolidated platform-independent configuration guides organized and presented by technology. There is one set of configuration guides and

command references for the Cisco IOS XE Fuji 16.x release train. These Cisco IOS command references support all Cisco platforms that are running any Cisco IOS XE Fuji 16.x software image.

See http://www.cisco.com/en/US/products/ps11174/tsd_products_support_series_home.html

Information in the configuration guides often includes related content that is shared across software releases and platforms.

Additionally, 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.

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.