Release Notes for Cisco 1000 Series ISRs, Cisco IOS XE Everest 16.6.x

First Published: 2017-09-20

Last Modified: 2019-04-15

New Hardware and Software Features for Cisco 1100 Series ISRs Release 16.6.x

This section describes the new and modified features that are supported on the Cisco 1100 Series ISRs.

Overview of Cisco 1100 Series Integrated Services Routers

The Cisco 1100 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.

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 following table lists the router models that belong to the Cisco 1100 Series ISRs.

Cisco 1100 Series ISRs	
C1111-8P	C1111-4P
C1111-8PLTEEA	C1111-4PLTEEA
C1111-8PLTELA	C1111-4PLTELA
C1111-8PWE	C1111-4PWE
C1111-8PWB	C1111-4PWB

Cisco 1100 Series ISRs	
C1111-8PWA	C1111-4PWA
C1111-8PWZ	C1111-4PWZ
C1111-8PWQ	C1111-4PWN
C1111-8PWN	C1111-4PWQ
C1111-8PWH	C1111-4PWH
C1111-8PWR	C1111-4PWR
C1111-8PWF	C1111-4PWF
C1111-8PLTEEAWE	C1111-4PWD
C1111-8PLTEEAWB	
C1111-8PLTEEAWA	
C1111-8PLTEEAWR	
C1111-8PLTELAWZ	
C1111-8PLTELAWN	
C1111-8PLTELAWQ	
C1111-8PLTELAWH	
C1111-8PLTELAWF	
C1111-8PLTELAWD	

C1101-4P
C1101-4PLTEP
C1101-4PLTEPWX

C1116-4P
C1116-4PLTEEA
C1116-4PWE
C1116-4PLTEEAWE

C1117-4P
C1117-4PLTEEA

C1117-4PLTELA
C1117-4PWE
C1117-4PWA
C1117-4PWZ
C1117-4PM
C1117-4PMLTEEA
C1117-4PMWE
C1117-4PLTEEAWE
C1117-4PLTEEAWA
C1117-4PLTELAWZ
C1117-4PMLTEEAWE

System Requirements

The following are the minimum system requirements:

- Memory: 4GB DDR4
- Flash Storage: 4GB

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 the ROMMON Version on the Cisco 1100 Series ISR

For information about ROMMON and upgrading procedure, see the "ROMMON Overview and Basic Procedures" section in the Hardware Installation Guide for the Cisco 1100 Series Integrated Services Routers.

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 Hardware Features in Cisco 1100 Series ISR Release 16.6.2

The following are the new hardware features in Cisco 1100 Series Integrated Service Routers in the 16.6.2 release:

- **Cisco 1100 Series Integrated Services Routers**–The Cisco 1100 Series ISRs are fixed branched routers based on the Cisco IOS XE Everest 16.6.2 operating system, multi-core data plane. The two types of platforms of Cisco 1100 Series ISRs are High-End and Midrange service and enterprise platforms. The Cisco 1100 Series ISR Software Configuration Guide explains supported features such as Smart Licensing, VDSL2 and ADSL2/2+, WLAN, 4G LTE-Advanced, and so on.

  Cisco® 1100 Series Integrated Services Routers (ISRs) with Cisco IOS® XE Software combine Internet access, comprehensive security, and wireless services (LTE Advanced 3.0 Wireless WAN and Wireless LAN), are single high-performance devices that are easy to deploy and manage. They are well suited for deployment as customer premises equipment (CPE) in enterprise branch offices, and in service provider managed-service environments.

New Software Features in Cisco 1000 Series ISR Release Cisco IOS XE Everest 16.6.1

- **AVC and NBAR2 Support**

  Cisco 1100 Series ISR devices support Cisco Application Visibility and Control (AVC) and Network-Based Application Recognition (NBAR2), beginning with Cisco IOS XE Everest 16.6.1. AVC and NBAR2 analyze network traffic and identify the applications associated with the traffic. This enables application-based network policies and application visibility.

  For more information, see:

  https://www.cisco.com/c/en/us/products/routers/avc-control.html

  https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_nbar/configuration/xe-16-6/qos-nbar-xe-16-6-book.html

New Hardware Features in Cisco 1100 Series ISR Release 16.6.2

The following are the new hardware features in Cisco 1100 Series Integrated Service Routers in the 16.6.2 release:

- **Cisco 1100 Series Integrated Services Routers**–The Cisco 1100 Series ISRs are fixed branched routers based on the Cisco IOS XE Everest 16.6.2 operating system, multi-core data plane. The two types of platforms of Cisco 1100 Series ISRs are High-End and Midrange service and enterprise platforms. The Cisco 1100 Series ISR Software Configuration Guide explains supported features such as Smart Licensing, VDSL2 and ADSL2/2+, WLAN, 4G LTE-Advanced, and so on.

  Cisco® 1100 Series Integrated Services Routers (ISRs) with Cisco IOS® XE Software combine Internet access, comprehensive security, and wireless services (LTE Advanced 3.0 Wireless WAN and Wireless LAN), are single high-performance devices that are easy to deploy and manage. They are well suited for deployment as customer premises equipment (CPE) in enterprise branch offices, and in service provider managed-service environments.

New Software Features in Cisco 1100 Series ISR Release 16.6.2

The following features are supported by the Cisco 1100 Series Integrated Services Routers for Cisco IOS XE Everest 16.6.2:

- **Encrypted Traffic Analytics**

  For detailed information, see the following Cisco documents:

  https://www.cisco.com/c/en/us/td/docs/routers/access/1100/software/configuration/xe-16-6/cisco_1100_series_swcfg_xe_16_6_x/encypt_traffic_anytcs.html

  https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Campus/CVD-Encrypted-Traffic-Analytics-Deployment-Guide-2017DEC.pdf

- Smart Licensing - Smart Licensing Client feature is a standardized licensing platform that simplifies the Cisco software experience and helps you to understand how Cisco software is used across your network. Smart Licensing is the next generation licensing platform for all Cisco software products.

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

- VDSL2 and ADSL 2/2+ - VDSL2 and ADSL2/2+ Cisco® C1100 Series Integrated Services Router provide highly reliable WAN connections for remote sites. These interfaces offer cost-effective virtualized WAN connections in both point-to-point and point-to-multipoint designs.

- Wireless Devices - Wireless devices (commonly configured as access points) provide a secure, affordable, and easy-to-use wireless LAN solution that combines mobility and flexibility with the enterprise-class features required by networking professionals.

- Cisco 4G LTE Advanced - Cisco 4G LTE-Advanced support the following major features: Global Positioning System (GPS) and National Marine Electronics Association (NMEA) streaming, Short Message Service (SMS), 3G/4G Simple Network Management Protocol (SNMP) MIB, SIM lock and unlock capabilities, Dual SIM, Auto SIM, NeMo, Public Land Mobile Network (PLMN) selection, IPv6, Multiple PDN, and LTE Link Recovery.

- Process Health Monitoring - Processes should provide monitoring and notification of their status/health to ensure correct operation. When a process fails, a syslog error message is displayed and either the process is restarted or the router is rebooted. A syslog error message is displayed when a monitor detects that a process is stuck or has crashed. If the process can be restarted, it is restarted; else, the router is restarted.

- Environmental Monitoring - The router provides a robust environment-monitoring system with several sensors that monitor the system temperatures. The following are some of the key functions of the environmental monitoring system: Monitoring temperature of CPUs, Motherboard, and Wifi, Recording abnormal events and generating notifications, Monitoring Simple Network Management Protocol (SNMP) traps, Generating and collecting Onboard Failure Logging (OBFL) data, Sending call home event notifications, Logging system error messages, and Displaying present settings and status.

- SFP Auto-Failover - When the media-type is not configured, the Auto-Detect feature is enabled by default. The Auto-Detect feature automatically detects the media that is connected and links up. If both the media are connected, whichever media comes up first is linked.

- Cellular IPv6 Address - IPv6 addresses are represented as a series of 16-bit hexadecimal fields separated by colons (:) in the format: x:x:x:x:x:x:x:x. Following are two examples of IPv6 addresses: 2001:CDBA:0000:0000:0000:0000:3257:9652 and 2001:CDBA::3257:9652 (zeros can be omitted).

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 Fast Ethernet 0 configured.

```
Router(config)# int FastEthernet0
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
```

Open and Resolved Caveats in Cisco IOS XE Everest 16.6.x

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

This section contains the following topics:

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.

Open Caveats in Cisco IOS XE Everest 16.6.9

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

Caveat ID Number	Description
CSCvt71774	C1111 HSRP preempt worked even though HSRP's preempt is not configured

Resolved Caveats in Cisco IOS XE Everest 16.6.9

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

Caveat ID Number	Description
CSCvg79590	Traffic passed with port unauthorized
CSCvs85642	ISR G3 router crashes when rtp-nte DTMF packet arrives at MTP + BDI
CSCvw57860	Duplicate entries seen in MAC filter table.

Resolved Caveats in Cisco IOS XE Everest 16.6.8

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

Caveat ID Number	Description
CSCvo97985	path-id discovery failure with "CENT throttle check fails, throttle type:0"
CSCvp23112	OBS: ping stop working on replacing MIP100 ->>> SIP40 >>>>>>MIP100
CSCvp94050	cpp_bqs_srt_yoda_csr_tree_seid_initialize:1744 is not in "placed" state
CSCvq43550	C1111-4P does not restart authentication for "clear authen session" if "authen open" the port
CSCvq61590	ESP reload due to cpp_cp_svr exception at cpp_bqs_exponent_cnt_validate
CSCvq81620	Router crashes with ZBF HA sync.
CSCvq93850	Passive FTP will fail when going over NAT and either client or server are off a SM-X-ES3
CSCvr00983	Unrecoverable Error with PVDM in 0/4 and Thule+dreamliner in 1/0 on ISR4300
CSCvr01454	Punt fragment crash when receive EoGRE packets which have many fragments
CSCvr43037	"sh macsec statistics int <>" and "sh macsec status interface <>" does not show output
CSCvr58352	Prince: Keepalive pkts dropped when serial link congested with data traffic
CSCvr89957	CFT crashed frequently
CSCvs28073	IOS-XE memory leak seen in 16.3.7 in IOSd due to update_sn_ao_state not deleting TDL bucket.
CSCvs53749	EVPN RMAC stale routes seen
CSCvs86573	Connect message is never forwarded to the calling side

Open Caveats in Cisco IOS XE Everest 16.6.8

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

Caveat ID Number	Description
CSCvr89973	NIM interfaces go into shutdown after router bootup.

Open Caveats in Cisco IOS XE Everest 16.6.7

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

Caveat ID Number	Description
CSCva53392	Polaris 16.3.1 : Machine and bus error failures in ESP20
CSCvd65197	IOSd crashed when dialer disconnect the ISDN call
CSCve54914	NDSSO vrf ha table to be populated correctly

Caveat ID Number	Description
CSCve78446	[1661]- Switch number is missing in stack merged logs.
CSCvf28977	ESP Crash with FP Switchover
CSCvf86185	NIM-SSD: Inventory of disk0 and disk1 are interchanged on Polaris 16.x
CSCvg23820	CTS PAC download fails with VRF config on non-managenent interface
CSCvh59431	Byte counters for physical interface and subinterface don't match
CSCvi36351	standby rp crash on removing member link from port-channel
CSCvj55210	Memory leaks at __be_PKI_keypair_name_get
CSCvk75838	netconf/yang or telemetry retrieval of /trustsec-state/cts-rolebased-policies breaks
CSCvm42345	Ping failing due to missing address resolution entry on the XTR
CSCvn39506	ISIS: system crashed when we configure ISIS on the interface.
CSCvo70549	CME SIP: BE4000 Smart Licensing - Extension Assigner temp registration uses endpoint license
CSCvo83960	ISR1100 router reloaded at posix_twheel_process_timers_inline
CSCvp70211	Crash when running show crypto map
CSCvp77521	Device-tracking tracking 0.0.0.0 mask ignored after Legacy IPDT to SISF conversion
CSCvp89419	Error messages seen when configuring "logging persistent protected" on ASR1K routers
CSCvp98673	Inband to OOB DTMF Fails to Be Passed On CUBE If Media Inactive Comes During Digit Processing
CSCvq43004	Need to check qfp ucode crash with RTCP traffic - chunk memory corruption in RTCP path
CSCvq43550	C1111-4P doesn't restart authentication for "clear authen session" if "authen open" the port
CSCvq61590	ESP reload due to cpp_cp_svr exception at cpp_bqs_exponent_cnt_validate
CSCvq69866	HSRPv2 crash whilst retrieving group from received packet
CSCvq73281	TLS connections in WebEx between CUBE and iCP/CUSP breaks intermittently
CSCvq75307	Crash due to watchdog after adding a prefix-list/ Route-map entry to existing route map.
CSCvq78692	mGRE L3VPN broken after reload
CSCvq81620	Router crashes with ZBF HA sync.

Caveat ID Number	Description
CSCvq85913	FlexVPN with password encryption -- after MasterKey change password in profile is not working
CSCvq90361	NHRP process crash on using same tunnel address on multiple spokes
CSCvq97906	"DHCPD Receive" process crash
CSCvr05406	LISP Map-cache not updated correctly after wired Host-mobility
CSCvr15253	Router Crashes while Parsing and Printing Voice Packet IEs
CSCvr17169	qfp ucode crash with media monitor
CSCvr32292	Router may crash due to segmentation fault after running EEM script

Resolved Caveats in Cisco IOS XE Everest 16.6.7

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

Caveat ID Number	Description
CSCvd77610	AAA always reports server down with non-management VRF also
CSCve57810	Amur failing over w/o 'fail next-method' or 'no-response next method'
CSCvg32153	"show interface port-channel" falsely reports output drops when there are no actual output drops
CSCvg82770	evc not work under vlan on TSN platform
CSCvh11088	Crash on OPF_CSR32_OPF_LOGIC_ERR_LEAF_INT__INT_START_OF_BURST_MARKER_ERR
CSCvh49874	FNF monitor download to DP failed after changing netflow record
CSCvh79264	Change the punt cause of packets whose destination is virtual IP from SUBNET_BCAST to FOR_US
CSCvh92659	BFD flaps everytime with dynamic tunnel creation in DMVPN
CSCvi22263	Crash when IOS is adapting shaping with Adaptive QoS over DMVPN configured
CSCvj00317	Memory leak VOIP *MallocLite*
CSCvj28921	High CPU due to Alignment Corrections - SMEF & IWAN
CSCvj72294	memory leak @ CCSIP_SPI_CONTR
CSCvj76866	Partial Power Failure in Stack Causes Interfaces to Become "shutdown"
CSCvj84601	Called-Station-Id attribute not included in Radius Access-Request
CSCvk17998	Rekey Timer are same for both the Server and Client

Caveat ID Number	Description
CSCvk51939	SSS Manager Traceback observer when test MLPPP
CSCvk63764	Driver code improvement for debug-ability of XAUI link issues
CSCvm10850	Crash after CPUHOG in ISDN L2D SRQ Process
CSCvm47690	Addition/Edits to numbered OG ACL using "access-list <>" command does not re-expand the ACL.
CSCvn00104	Software crash due to memory corruption after packet trace was enabled.
CSCvn01507	ISR not re-calculating the hash value correctly after payload change
CSCvn02456	Router crashes when the calls doesn't establish after making 2 calls when we set "max-conn 2"
CSCvn03502	SR: CFLOW input intf index is 0xffffffff for Service-engine DSP module interface
CSCvn23906	DHCP Server sends Renew ACKs to Clients with 00:00:00:00:00:00 MAC in L2 frame
CSCvn38960	pending objects seen which fp reload with OGACL config
CSCvn45732	Device crashing if we unconfigure the NTP on the device
CSCvn57892	High Memory utilization due to Wireless Manager IOSD process
CSCvn71373	IOS-XE routers cannot boot due to a bootflash problem
CSCvn78961	Subscribers cannot re-login due to CoA time-out (lite-sessions in routed mode)
CSCvo03458	PKI "revocation check crl none" does not fallback if CRL not reachable
CSCvo04856	DataPlane (DP) crash observed in MMOH call flow
CSCvo06817	Router crash while executing show commands using '|' (pipe) to filter the output.
CSCvo08740	TCP 3WAY handshake fail for redirected packet using PBHK
CSCvo10145	Memory overlay crash when using include-cui
CSCvo10491	PnP Agent should detect image upgrade scenario and configure dialer to bring up cellular interface
CSCvo11786	SCCP Application does not clear failed sockets leading to leak and socket pool exhaustion
CSCvo12745	Packet drop occurs after acl permit configurations
CSCvo12799	Call is not getting connected in Forking Re-INVITE scenario
CSCvo17287	ASR1001-X crashed upon receiving Radius Access-Accept message
CSCvo21122	Memory leak at hman process

Caveat ID Number	Description
CSCvo36031	WSMA crash formatting show command output
CSCvo46138	Stuck CPP Thread while processing H323 packet
CSCvo46405	qfp ucode crashed with sRTP traffic - chunk memory corruption
CSCvo47376	Cisco REST API Container for IOS XE Software Authentication Bypass Vulnerability
CSCvo55194	After RSP switchover label imposition was not programmed in Software on APS standby router
CSCvo57768	NetFlow issue 3850 switch not sending TCP flags
CSCvo58098	CTS PACS not downloading to the devices
CSCvo61610	FXS - no busy tone is generated on remote-onhook condition with call pickup scenario
CSCvo65415	ASR1k crashes by handling DHCP packet
CSCvo66216	IPSec-Session count in "show crypto eli" reaches max causing VPN failure
CSCvo70504	Missing Calling-Station-ID in Accounting Ticket for Web-Tal locations
CSCvo71721	When sending account-logon ISG do not reply with ACK nor NACK.
CSCvo73897	[SDA] [PI changes] No audio during first few seconds of voice call between 2 Fabric Edge
CSCvo73954	ASR1001-HX: Excessive pause frames (IEEE802.3x compliant) affect traffic on other interfaces
CSCvo74486	IOS-XE ACL port information preserved after encapsulation
CSCvo87827	Crash when polling IPForwarding MIB
CSCvo90060	Wrong label programming leading to traffic drop
CSCvo92514	SDP attribute list corruption causes voice gateway crash
CSCvo94211	Traffic stops flowing on Xconnect tunnel when upgraded to 16.9.2
CSCvp08353	Add ERROR message over IOS console when HSPRDA TCAM region gets full
CSCvp10711	Hierarchical QoS stops working on GRE tunnel if dest route flaps between 2nd tunnel and physical int
CSCvp24405	Router crash after adding macsec reply-protection command on an interface
CSCvp24911	SRTP ROC Stress: CPP crash with 6000+ concurrent calls - g729
CSCvp24981	When FQDN used for APN, IOS DNS resolves FQDN to IP, but GTP stays in DNS pending and IP 0.0.0.0
CSCvp25052	ISR4K: Router crash due to twice memory release

Caveat ID Number	Description
CSCvp27220	Tail drops on IPSLA sender when using scaled udp-jitter probes
CSCvp31779	Router Running IOS-XE 16 Crashes when Stopping EPC with ACL
CSCvp32910	CHUNKBADROOTCHUNKPTR: Bad root chunk pointer in chunk header post SSO - ASR1K
CSCvp33578	Crash at the moment of deleting a DVTI
CSCvp34230	CUBE HA - Global bind is removed during interface flap
CSCvp38317	MGCP GW doesn't reset SSRC/ROC on receiving MDCX with new IP/port/SDP parameter for SRTP call.
CSCvp38424	On-Prem DMVPN fails to establish a dynamic tunnel between Spoke nodes.
CSCvp38852	[SDA] 1st ARP getting dropped due to stale SISF IP-MAC binding
CSCvp39597	Crashes with GRE tunnels configured with QOS over Multilink Frame-relay interfaces
CSCvp42709	ISR44xx NO_PUNT_KEEPALIVE kernel crash due to CP drivers stuck punt and IPC rings
CSCvp47006	QoS counter didn't generate at ASR1001-X
CSCvp47723	ISR4K CME no way audio on calls across E1/PRI, reboot resolves for sometime
CSCvp48213	CSR1000v loses ssh/telnet connectivity on AWS and is unable to ping Elastic IP
CSCvp56596	ISR4K crashes after voice register reset command is applied
CSCvp56737	Counters of interfaces are reporting inexistent peaks
CSCvp59848	ASR1001-x crash while configuring policy-map
CSCvp63616	Crash due to too many DSPs
CSCvp65151	CPP Stuck thread when processing IPv6 traffic
CSCvp67530	Corrupt free block of memory with high availability config for Session Initiation Protocol
CSCvp69393	Router crashes after snmpget to OID related to NHRP
CSCvp70443	isdn cause-location command support for switch-type primary-ntt
CSCvp72220	crash at sisf_show_counters after entering show device-tracking counters command
CSCvp72379	ip dns primary command does not get removed
CSCvp74674	QoS fails to apply to tunnel2 when underlying tunnel1 reachability change
CSCvp77100	ASR1k: Crypto Engine remains in stuck state post dataplane crash

Caveat ID Number	Description
CSCvp84831	name-ip_address mapping is bypassed when the ip domain command is configured on Cisco C1111X Router
CSCvp86216	Router ucode crash with NAT with interface flap
CSCvp87488	no login on-success log CLI does not persist across device reloads
CSCvp92334	Crash after Media monitor look up.
CSCvp96418	ISR4k BRI ping failure with WIC-1B-S/T-V3 with ISDN 128 leased line
CSCvp99884	CUBE not passing History-Info header in 181 Call is being forwarded
CSCvq00263	Device crashed @ radius_io_stats_timer_handler due to dynamic-author
CSCvq02003	ASR1002-X High Platform CPU for process mcpcc-lc-ms
CSCvq02215	ASR1K-X WATCHDOG crashes while printing to console
CSCvq04828	VRF aware reverse DNS lookup not working
CSCvq10660	ASR1006-X: cpp_cp_svr: QFP0.0 CPP Driver LOCKDOWN encountered due to previous fatal error
CSCvq10663	NAT SIP Contact Header changed to port 512
CSCvq12723	DPDK: Performing Shut/No-Shut with traffic running can cause packets to silently drop on TX
CSCvq18793	NIM-2FXS/4FXOP crashing due to DSP failed to reply properly
CSCvq19808	Egress shaping on port-channel sub-intf tail dropping traffic long before rate
CSCvq23869	ASR 1k sub-interface counters wrong.
CSCvq25297	BRI leased line can't come up automatically after remove/insert one side's cable
CSCvq29575	Voice gateway crash due to segmentation fault in process CCSIP_DNS
CSCvq30306	IOSXE: IOMD / TDL leak seen with tdl_response_xcode_stat_side_t
CSCvq31129	AppNav: Optimization failed with Asymmetrical traffic, VRF, FNF and NBAR
CSCvq32736	ARM - Marvell 7040 SoC Hardware Erratum - Kernel Driver Fix
CSCvq36130	Router is on Bootloop after QoS configuration.
CSCvq39121	ISR4k crash during packet inspection due to stuck thread
CSCvq45088	asr1k BDI not working properly for packet fragmentation - very small fragments are getting dropped
CSCvq49000	Supervisor reloaded due to cpp_cp_svr process crashing

Caveat ID Number	Description
CSCvq50202	Class-attributes duplicated after EAP reauthen. in ISG radius proxy scenario
CSCvq57205	Recording failures with XMF media forking and SIP preservation timer
CSCvq57862	cable-detect command not reflecting proper status in Analog ports on IOS-XE platforms
CSCvq58144	cpp_cp_svr crash in cpp_bqs_rm_yoda_select_sch_exponent
CSCvq58237	Supervisor reload due to cpp_cp_svr crash.
CSCvq58265	ASR1K BGP PIC Repair path broke after link flap
CSCvq58378	Crash after exiting RADIUS server configuration mode.
CSCvq58520	after reload dial-peers with ports that have the 'signal did' command show operational state none
CSCvq72560	More connections are getting passthrough with reason SNG_OVERLOAD
CSCvq74418	connectivity is broken on ingress-replication L2DP/VXLAN
CSCvq75610	IWAN router crash after upgrading to 16.3.8
CSCvq92102	VG450: SCCP crashing router while shutdown the process
CSCvq98949	ASR1000-RP3: Punt Keepalive Failure (Punt LINK DOWN) or RP FREEZE

Open Caveats in Cisco IOS XE Everest 16.6.6

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

Caveat ID Number	Description
CSCvk15062	Modification to ZBFW access-lists do not reflect in TCAM
CSCvn01507	ISR not re-calculating the hash value correctly after payload change
CSCvo60849	Crash noticed when routes are getting imported twice(from vpnv4 to vrf to evpn) with route churn
CSCvo62122	IOS-XE Router may crash when attempting to Fragment Corrupted IPv4 Packet
CSCvo66216	IPSec-Session count in "show crypto eli" reaches max causing VPN failure
CSCvo74486	IOS-XE ACL port information preserved after encapsulation
CSCvp03110	After Configuring a New VRF Routes Are Not Imported From WAN Into l2vpn EVPN For Unrelated VRF
CSCvp05946	TSN: Umbrella not working when umbrella in and out are configured on SVI

Resolved Caveats in Cisco IOS XE Everest 16.6.6

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

Caveat ID Number	Description
CSCvb87675	BGP event crash@bgp_afpriv_imp_is_imported_path
CSCvg23363	Virtual-access interface MTU wrongly set when using ipsec ipv4
CSCvh57657	NAT MIB not populated when using traditional NAT
CSCvh77984	Router shows "Flash disk quota exceeded" during the reload, but it still has 60% of free memory left
CSCvk32822	QoS stats process crash
CSCvk62792	IKE Fragmentation payload incorrectly marked as critical
CSCvm06270	ICMP unrechables are not sent to the client on C1117 platform
CSCvm17883	Standby switch crashes when adding a host name to an object-group
CSCvm51112	"clear crypto sa vrf MyVrf" triggers crash after updating pre-shared-keys
CSCvm56670	ACL dropping packets after updating it - %CPPEXMEM-3-NOMEM
CSCvm64865	[EIGRP] a summary route is updated by an external route
CSCvm75066	MPLSoVPN: Change behavior of default route in NHRP. Must insert 0.0.0.0/0 instead of /32
CSCvm76452	IPSec background crash while sending SNMP trap
CSCvn02419	Device running IOS-XE 16 Polaris Sees Crash When Performing NAT ALG on FTP Packet
CSCvn18790	Cube crash with %SDP-3-SDP_PTR_ERROR
CSCvn23226	NHRP process is crashing
CSCvn27449	PBR doesn't work for dialer intf when it doesn't have fixed ip address
CSCvn36359	CUBE doesn't forward INVITE with "midcal-signalling passthru media-change" during a video escalation
CSCvn56017	Crash while processing ISIS updates when DiffServ-TE is enabled
CSCvn59020	Modified EIGRP timers on Virtual-Template put all associated Vi interfaces into passive mode
CSCvn77783	class-attributes support in ISG radius proxy scenario
CSCvn83172	Router reloads on 'show track' command when there is track object for deleted serial sub-interface.

Caveat ID Number	Description
CSCvo00585	Split DNS in case of UDP query to WAN interface IP via LAN interface
CSCvo03743	zbfw with ip sla icmp echos builds tcp syn session
CSCvo24170	Crash due to chunk corruption in ISIS code
CSCvo27553	PKI incorrect fingerprint calulation during CA authentication
CSCvo62584	DHCP discover packets were being dropped at firewall since UDP source port as 0.

Open Caveats in Cisco IOS XE Everest 16.6.5

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

Table 1: Open Caveats

Caveat ID Number	Description
CSCvg03519	16.6.1A: TSN router crashed with pppoe session after changing encapsulation on peer
CSCvg24729	TSN: GLC-GE-100FX V02, the link can not up when configure "media-type sfp".

Table 2: Resolved Caveats

Caveat ID Number	Description
CSCvm06270	ICMP unrechables are not sent to the client on C1117 platform.

Resolved Caveats in Cisco IOS XE Everest 16.6.5

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

Caveat ID Number	Description
CSCvk52512	C1100 router stops forwarding traffic when doing bulk configurations on device via telnet
CSCvj74614	ISR1111-4P Ping issue between LAN inetrface and directly connected switch.
CSCvm63888	Recommit of CSCvj74614 in throttle v166 ISR1111-4P Ping issue between LAN inetrface.

Open and Resolved Caveats for Cisco IOS XE Everest 16.6.1

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

Table 3: Open Caveats

Caveat ID Number	Description
CSCvg03519	16.6.1A: TSN router crashed with pppoe session after changing encapsulation on peer

Caveat ID Number	Description
CSCvg24729	TSN: GLC-GE-100FX V02, the link can not up when configure "media-type sfp".

Table 4: Resolved Caveats

Caveat ID Number	Description
CSCve31171	16.6.1A: TSN router crashed with pppoe session after changing encapsulation on peer
CSCvg17891	GETVPN suite-B does not work on TSN routers

Related Documentation

Cisco IOS Software Documentation

The Cisco IOS XE Everest 16.x software documentation set consists of Cisco IOS XE Everest 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 Everest 16.x release train. These Cisco IOS command references support all Cisco platforms that are running any Cisco IOS XE Everest 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.