Release Notes for Cisco 1000 Series Integrated Services Routers, Cisco IOS XE Gibraltar 16.12.x

First Published: 2019-07-18

Last Modified: 2022-09-19

Full Cisco Trademarks with Software License

About Cisco 1000 Series Integrated Services Routers

The Cisco 1000 Series Integrated Services Routers (also referred to as router in this document) 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 the router.

Product Field Notice

Cisco publishes Field Notices to notify customers and partners about significant issues in Cisco products that typically require an upgrade, workaround or other user action. For more information, see https://www.cisco.com/c/en/us/support/web/field-notice-overview.html.

We recommend that you review the field notices to determine whether your software or hardware platforms are affected. You can access the field notices from https://www.cisco.com/c/en/us/support/web/tsd-products-field-notice-summary.html#%7Etab-product-categories.

Hardware and Software Features - New and Enhanced

New Hardware Features

P-LTE-IN LTE and P-LTE-JN LTE pluggable module support on C1109 and C1121 platforms for Cisco IOS XE Gibraltar 16.12.1a release.

New Software Features

- Support for IEEE 802.1Q Tunneling and Layer 2 Protocol Tunneling: With IEEE 802.1Q Tunneling, service providers can now carry traffic of multiple customers across their networks while maintaining the VLAN and Layer 2 protocol configurations of each customer without restricting the traffic. Additionally, with Layer 2 protocol tunneling, service providers can now use either Layer 2 protocol tunneling independently or use it to enhance IEEE 802.1Q tunneling.

- IPv6 support for Encrypted Traffic Analytics: This feature extends support for Encrypted Traffic Analytics (ETA) to IPv6 addresses. ETA is used to identify malware communications in encrypted traffic. ETA uses passive monitoring, extraction of relevant data elements, and supervised machine learning with cloud-based global visibility.

- Support for Federal Information Processing Standards: FIPS are publicly announced standards developed by the United States federal government for use in computer systems by non-military government agencies and government contractors.

  With FIPS software, you can prevent use of non-FIPS compatible algorithms, this ensures that the device is configured to use only FIPS-approved algorithms. Some functionality in the computer systems may fail in the FIPS mode if the FIPS software attempts to use non-FIPS compliant algorithms.

- Cisco Discovery Protocol over IPV6 tunnels: Configure CDP over GRE IPv6 Tunnel to transport data from other protocols through an IPv6 network. This feature also allows routing of IPv6 packets between private networks across public networks with globally routed IPv6 addresses.

- **Perfect Forward Secrecy for GETVPN:** If a Group Member (GM) is compromised, an attacker may access saved long-term keys and messages. Use Perfect Forward Secrecy (PFS) for GETVPN so that the attacker cannot use the keys and messages to obtain the keys of past or future sessions to decrypt recorded or future communication.

- **Cisco Unified Border Element Support:** Cisco Unified Border Element (Cisco UBE) is supported on Cisco 1000 Series Integrated Services Routers running on Cisco IOS XE Gibraltar 16.12.1a release or later.

- **Multi-SA Support for SVTI:** With Multi-SA support, 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 can modify the default configuration that uses a single any any traffic selector.

- Web UI to Manage Cisco 1000 Series Integrated Services Routers: The Web UI lets you configure Cisco Unified Communications Manager Express (CUCM-E), File manager, and Trustsec on the Cisco 1000 Series Integrated Services Routers. To learn more, refer to the WebUI Online Help.

- 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/16121/BIC. 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.

> **Note** In Cisco IOS XE Release 16.12.3, the semantic version number for the YANG models is not updated and is therefore not accurate. However, this limitation does not impact the functionality of the YANG models.

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.

- You can use the Cisco IOS CLI to enter the necessary configuration commands.

ROMmon Compatibility Matrix

The following table lists the ROMmon releases supported in Cisco IOS XE 16.x.x releases.

Table 1: Minimum and Recommended ROMmon Releases Supported on Cisco 1000 Series Integrated Services Routers

Cisco IOS XE Release	Minimum ROMmon Release Supported for IOS XE	Recommended ROMmon Release Supported for IOS XE
16.6.x	16.6(1r)	16.6(1r)
16.7.x	16.6(1r)	16.6(1r)

Cisco IOS XE Release	Minimum ROMmon Release Supported for IOS XE	Recommended ROMmon Release Supported for IOS XE
16.8.x	16.8(1r)	16.8(1r)
16.9.x	16.9(1r)	16.9(1r)
16.10.x	16.9(1r)	16.9(1r)
16.11.x	16.9(1r)	16.9(1r)
16.12.x	16.9(1r)	16.12(1r)

Resolved and Open Caveats

About the Cisco Bug Search Tool

Use the Cisco Bug Search Tool to access open and resolved bugs for a release.

The tool allows you to search for a specific bug ID, or for all bugs specific to a product and a release.

You can filter the search results by last modified date, bug status (open, resolved), severity, rating, and support cases.

Resolved Bugs in Cisco IOS XE Gibraltar 16.12.8

Caveat ID Number	Description
CSCvy91615	OpenSSH vulnerability for IOS-XE platforms.
CSCwb08932	Standby switch crashed due to SISF BT mac move.
CSCvz80171	SIP call fails egress dial-peer uses session server-group and sip options-keepalive.
CSCwa27659	Virtual VRRP IP address unreachable from the BACKUP VRRP.
CSCwb26335	RSP3: Err reading data from table dmi-general: could not get boolean val for feature.side_effect_sync.

Caveat ID Number	Description
CSCvz77313	Device switch reload due to SFF8472.
CSCvw60355	DHCPv6: Memory allocation of DHCPv6 relay option results in crash.
CSCwb96964	Device crashes on creating telemetry subscription.
CSCwb24680	LLDP system description not correctly seen in ISE.
CSCwa82143	%SYS-2-INTSCHED: 'may_suspend' disabled -Process= HSRP IPv4 log generate during boot up.

Open Caveats in Cisco IOS XE Gibraltar 16.12.8

There are no open caveats for this release.

Resolved Bugs in Cisco IOS XE Gibraltar 16.12.7

Caveat ID Number	Description
CSCvy79950	Cannot force the switch to ask for option 12 to be assigened from the DHCP server.
CSCvz24267	Static NAT entry is injecting a route to Null0.
CSCvz69851	Missing iid_certs for AWS invite-only regions.
CSCvz57415	128.0.0.0/2 is installed into CEF as unusable on a PETR after EID-Prefix is removed.
CSCwa36699	Prefetch CRL Download Fails.

Open Caveats in Cisco IOS XE Gibraltar 16.12.7

There are no open caveats for this release.

Resolved Bugs in Cisco IOS XE Gibraltar 16.12.6

Caveat ID Number	Description
CSCvt35331	Console port goes unresponsive, reboot required to restore it.
CSCvw27787	NBAR not able to recognize application in a capwap-tunnel
CSCvw42048	C1111 vtcp may cause packet drop for sip packets causing phones to reset
CSCvw57860	Duplicate entries seen in MAC filter table.
CSCvw87300	IP address not correctly in SIP traffic
CSCvx01171	Smart Licensing: ISR4K Consumes Multiple Boost Performance Licenses
CSCvx15820	Subslot module C1111-ES-8 going out of service
CSCvx19135	ISR crashes when ZBFW ALG inspects tunneled packet

Caveat ID Number	Description
CSCvx64180	On ISR1113 CCM multicast frames dropped in upstream direction
CSCvx84617	ISR - Appnav service controller ucode crash during packet intercept from network
CSCvx85334	Port enters err-disabled state (BPDU guard) when LLDP packet with MAC DA:0180.c200.0000
CSCvx97718	VTCP frees rx buffer when packet with expected next sequence arrives with no payload; phones reset
CSCvy83154	MAG is not detecting the path UP after several reboots

Open Caveats in Cisco IOS XE Gibraltar 16.12.6

Caveat ID Number	Description
CSCvp46414	TunnelUnsupportedConfig drops seen during volume based rekey
CSCvq93257	Update new OID numbers to ciscoC83001N1S6G and ciscoC83001N1S4G2X in CISCO-PRODUCTS-MIB.my
CSCvr93635	Flows not moving to unutilized link even after the hard threshold
CSCvt89441	IOS-XE device crashed with CGD shared memory corruption freed by FMAN-FP
CSCvt99760	Crash when btrace modules exceed the initially max number of registration
CSCvy34805	Consecutive Multicast Crashes in ISR4K
CSCvy57684	ISR4k rebooted unexpectedly with reason LocalSoft
CSCvy94954	LA LED turns green when just inserted SFP-10G-LR on ISR4k without cable connecting
CSCvz07134	Router does not boot on recent 16.X releases with large service policy applied on the interface.
CSCvz13126	Ucode crash with test calls from the SIP trunk to the POTS lines
CSCvz14745	Memory leak seen when using DNS with IP SLA

Resolved Bugs in Cisco IOS XE Gibraltar 16.12.5

Caveat ID Number	Description
CSCvt58920	SIM failover within the same modem takes long time to detect LTE network for AT&T
CSCvu59956	IOS cannot boot with 16.12(1r) or later rommon due to cookie PID field incorrectly programmed
CSCvu65369	Link auto-negotiation fails between C1111-4P ES-4 switch module and Meraki MX100

Caveat ID Number	Description
CSCvu82189	Enabling guestshell gives "float division by zero"
CSCvu99045	NIM-1GE-CU-SFP/NIM-2GE-CU-SFP: Show interface output reports incorrect bandwidth
CSCvv01250	IGMP reports are forwarded to mrouter port untagged regardless of which VLAN the group is in
CSCvv02180	C1113-8PLTEEAWA failed to boot: Package does not support : PID not supported in 17.4
CSCvv05046	MTU on PPPoA not reaching 1500
CSCvv17730	IP DHCP Snooping not working for the voice vlan
CSCvv33246	DHCP Offer packet returns over the PMIP tunnel that received it on first place.
CSCvv33349	%IOSXE_INFRA-3-PUNT_ADDR_RES_ENCAP_ERR: seen repeatedly in LISP coworking with VASI
CSCvv36983	Unable to monitor AP Controller running 8.10 using web GUI
CSCvv37172	License lost after "no license boot level <>" CLI followed by reset button
CSCvv43027	VDSL performance impacted if more than two vlan tags are used
CSCvv43700	c1100 LTE router showing incorrect value in "sh ip route" output
CSCvv58919	Police to PPS is not configurable on ISR4K
CSCvv89089	VPN configuration through WebUI fails with an "Internal Error" when Pre-shared key contains "%"
CSCvw06780	DMVPN with ipv6 link-local address do not register to HUB
CSCvw11902	Passive FTP doesn't work with NAT
CSCvw16304	Async: First line of NIM/SM-async module get unexpected char when VDSL active
CSCvw19623	TTY session not freed up during partial configuration download
CSCvw31389	pktlog functionality is broken

Open Caveats in Cisco IOS XE Gibraltar 16.12.5

Caveat ID Number	Description
CSCvq93257	Update new OID numbers to ciscoC83001N1S6G and ciscoC83001N1S4G2X in CISCO-PRODUCTS-MIB.my
CSCvt35331	Console port goes unresponsive, reboot required to restore it.
CSCvt97975	TenGig SPA Module went down because of site power issue

Caveat ID Number	Description
CSCvw27787	NBAR not able to recognize application in a capwap-tunnel
CSCvw57860	Duplicate entries seen in MAC filter table.
CSCvw84042	IOS-xe does not correlate indices properly with cellular radio band output
CSCvw87300	IP address not correctly in SIP traffic
CSCvw96723	CP process crashed while I95 driver was adding an IPC response to the receive ring
CSCvx01171	Smart Licensing: ISR4K Consumes Multiple Boost Performance Licenses

Resolved Bugs in Cisco IOS XE Gibraltar 16.12.4

Caveat ID Number	Description
CSCvs28073	IOS-XE device has memory leak in linux_iosd-imag
CSCvu04552	OBS: NHRP Cache queue and cache limit
CSCvs63841	SDWAN ISR1100: No SW Image listed when .bin image booted from flash / usb
CSCvs96540	SDWAN device admin-tech has empty "show running config" in /tech/ios file
CSCvt06707	C1111-LTE Observe data stalling after cellular interface has been loaded with data traffic for while
CSCvt45843	Track omp is configured on cEdge C1100, but VRRP becomes Master while OMP is lost
CSCvt54305	Device crashed after Boost license expire
CSCvt71774	C1111 HSRP preempt worked even though HSRP's preempt is not configured
CSCvt42659	Possible Regression ISR4K Mgmt Port ACL Breakage or simply Day One Implementation As Designed
CSCvs88826	C11xx: secure rommon upgrade fail by power cycle device with IOS 16.12.01a

Open Caveats in Cisco IOS XE Gibraltar 16.12.4

Caveat ID Number	Description
CSCvu65369	Link auto-negotiation fails between C1111-4P ES-4 switch module and Meraki MX100
CSCvt35331	Console port goes unresponsive, reboot required to restore it
CSCvt48480	Flow monitor is removed from interface configuration on reload
CSCvu62273	CLI should be auto-upgraded from "tacacs-server" cli to newer version while upgrading

Note TACACS legacy command: Do not configure the legacy **tacacs-server host** command; this command is deprecated. If the software version running on your device is Cisco IOS XE Gibraltar 16.12.2 or a later release, using the legacy command can cause authentication failures. Use the tacacs server command in global configuration mode.

Resolved Bugs in Cisco IOS XE Gibraltar 16.12.3

Caveat ID Number	Description
CSCvr12395	vManage push "media-type rj45" when trying to configure duplex on ISR1k
CSCvr65986	ISR1K: dot1q-tunneling ports broadcast unknown unicast traffic to all other local switch ports
CSCvs18317	C1111X-8P Sku tagged to 4P software tag incorrectly
CSCvs20560	C1121 running IOS XE 16.12.2 installs backup BGP path instead of best path in RIB (IPv6 VRF BGP)
CSCvs26625	C1113/1112 does not train up in ADSL2+ mode when configured in "operating mode auto"

Open Caveats in Cisco IOS XE Gibraltar 16.12.3

Caveat ID Number	Description
CSCvs95815	C1111 telnet refused for link-local addresses when using ipv6 access class
CSCvs96525	Multiple crashes on C1111X-8P running 16.12.1e.0.66

Open Caveats in Cisco IOS XE Gibraltar 16.12.2s

Caveat ID Number	Description
NA	There are no open caveats in 16.12.2s

Resolved Bugs in Cisco IOS XE Gibraltar 16.12.2

Caveat ID Number	Description
CSCvt03982	IOS-XE NAT - protect customer data
CSCvp55170	Router crash when apply isis configuration.
CSCvq68449	QFP ucode crash while processing large packet with NBAR enabled
CSCvq43550	C1111-4P doesn't restart authentication for \"clear authen session\" if \"authen open\" the port
CSCvq81620	Router crashes with ZBF HA sync

Open Caveats in Cisco IOS XE Gibraltar 16.12.2

Caveat ID Number	Description
CSCvm79556	RSP3:VC stays down after Switchover (Error Local access circuit is not ready for label advertise)
CSCva53392	Polaris 16.3.1 : Machine and bus error failures in ESP20
CSCvp60827	Delay of 30 sec while creating a new config file for phone using tftp.
CSCvr33864	NIM-2GE-CU-SFP: Failed to boot up after upgrade

Resolved Bugs in Cisco IOS XE Gibraltar 16.12.1a

Caveat ID Number	Description
CSCvv54943	ISR1100: Bridge Domain does not pass traffic through SVI after an upgrade to 16.12.x onwards.
CSCvh92659	BFD flaps everytime with dynamic tunnel creation in DMVPN
CSCvn65889	TSN ROMmon: Modify FIT code to prevent booting C1100 images unless the PID is in FIT file
CSCvi26188	Watchdog crash within mgcpapp_free_sys_event_Q event dequeue loop after running 'ccm-manager config'
CSCvj28921	High CPU due to Alignment Corrections - SMEF & IWAN
CSCvk71047	Router fails to reserve necessary ports for VPN traffic (UDP 500 & 4500) for ISAKMP
CSCvm75066	MPLSoVPN: Change behavior of default route in NHRP. Must insert 0.0.0.0/0 instead of /32
CSCvm94112	DSM-3-INTERNAL: Internal Error : No DSM handle provided traceback on TDM voice gateway
CSCvn03502	SR: CFLOW input intf index is 0xffffffff for Service-engine DSP module interface
CSCvn49351	Async line not visible in show run and show int brief output but visible in show line output
CSCvn52019	Crashed while checking condition debug
CSCvn57165	Static Nat fails to translate SIP Trying L7 header
CSCvn58922	With 3 KS in COOP, overlapping KSSID range is not detected
CSCvn67870	Reorder ip nat configuration - to be placed after ip http configuration
CSCvn72208	RP3 Punt Interface May Drop Traffic Due to VLAN Filter Hardware
CSCvn76837	DMVPN Phase 2 shortcut triggered from a spoke behind PAT may end up in stuck DNX state

Caveat ID Number	Description
CSCvn78203	Router crashed when printing logs while constructing rekey packets GETVPN.
CSCvn78349	FlexVPN with password encryption - keyring aaa LIST password 6 xxxxx encrypted again upon reload
CSCvn81585	%CTS-3-SAP_MANUAL_PMKID_MISMATCH: PMKID Mismatch when master switch failover in a 6 switch stack.
CSCvn82063	Input CRC counter increasing on Tengi interface.
CSCvn82245	EIGRP session is not coming up if the dynamic PBR is applied on interface
CSCvn85422	Int index is 0 for the Cellular inteface in the exported flow
CSCvo00664	SUP reload after running the command " show plat hard qfp act infr bqs debug qmrt_dump "
CSCvo01298	Correction to Quick RP3 recovery after the Punt Path XAUI link goes down
CSCvo03458	PKI "revocation check crl none" does not fallback if CRL not reachable
CSCvo08132	BUILT-IN-2T+20X1GE - VLAN bytes and packets counters are frozen.
CSCvo09059	"no autostate" will auto add after re-configure svi interface
CSCvo11361	Priority queueing on port-channel interfaces causes frame re-ordering.
CSCvo11786	SCCP Application does not clear failed sockets leading to leak and socket pool exhaustion
CSCvo12745	Packet drop occurs after acl permit configurations
CSCvo17738	Cellular interface lte Network Selection Mode switches to manual
CSCvo19395	Router crashes when removing a crypto map
CSCvo20934	FMAN crash due to Flexible Netflow (fnf)
CSCvo27553	PKI incorrect fingerprint calulation during CA authentication
CSCvo30329	Router crashing after upgrade due to Crypto commands "Block overrun at 284B2160 (red zone 000110DF)"
CSCvo30641	Traceback: Error seen after tunnel flap: DATACORRUPTION-1-DATAINCONSISTENCY
CSCvo36188	Crash at NAT clear
CSCvo45257	mem leak in ios_portal_vty_run_cmd
CSCvo46127	MaxSusRate is not working with service class
CSCvo47436	IOSXE - firewall corrupts half open list

Caveat ID Number	Description
CSCvo47866	Crash at Process = SCCP Auto Config
CSCvo57746	CPUHOG while unconfiguring vrf with 1M vxlan static routes
CSCvo61610	FXS - no busy tone is generated on remote-onhook condition with call pickup scenario
CSCvo61772	"ip nat translation port-timeout" limited to overflows after reaching 16bit
CSCvo61914	GC NAT unable to detect dns packet
CSCvo66216	IPSec-Session count in "show crypto eli" reaches max causing VPN failure
CSCvo71445	MACSEC license is not being consumed for sub-interfaces
CSCvo74486	IOS-XE ACL port information preserved after encapsulation
CSCvo75992	tdl_fw_stats in FMAN logs errors
CSCvo83945	Ping failure on Port-channel sub interface when is using EVC in main port channel
CSCvo87488	GetCACaps is using wrong CA-IDENT when using enrollment profiles
CSCvo94211	Traffic stops flowing on Xconnect tunnel when upgraded to 16.9.2
CSCvp00271	Read and Write lock fix for ACL cache
CSCvp05070	Overlay BGP down when configured "ip nhrp server-only"
CSCvp16730	Incoming ESP packets with SPI value starting with 0xFF are dropped due to Invalid SPI error
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.
CSCvp46381	static nat which has been deleted is shown when show ip nat translation
CSCvp49863	Incomplete arp in management interface
CSCvp56737	Counters of interfaces are reporting inexistent peaks
CSCvp56753	PW MIB does not list all VCs when template is fwd ref, "show pwmib peer" returns nothing
CSCvp62811	Engine keyword missing after "show utd engine standard statistics url-filtering"
CSCvp63616	Crash due to too many DSPs
CSCvp70211	Crash when running show crypto map
CSCvp75121	Ucode crash when PfRv3 and IPv6 monitor are configured on the same tunnel with IPv6 VRF configured

Caveat ID Number	Description
CSCvp79470	C1100 Static PAT translations fail due to %FMFP-3-OBJ_DWNLD_TO_DP_FAILED:
CSCvp81102	IPsec SA installation fails with simultaneous negotiations despite fix for CSCve08418
CSCvp92334	Crash after Media monitor look up.
CSCvp95070	"encr aes 256" config removed from CDB & invisible to netconf/yang and restconf

Open Caveats in Cisco IOS XE Gibraltar 16.12.1a

Caveat ID Number	Description
CSCvg68226	Excluding cisco802TapMIB or ciscoTap2MIB should not require Lawful Intercept licence
CSCvp08353	Add ERROR message over IOS console when HSPRDA TCAM region gets full
CSCvp69393	Router crashes after snmpget to OID related to NHRP
CSCvp79485	DMVPN - Packet is encapsulated but not encrypted going out DMVPN tunnel
CSCvp96086	Cellular Backoff counters is not correct after modem reset :
CSCvq16878	Stale NAT Entries On Secondary Router
CSCvq25297	BRI leased line can't come up automatically after remove/insert one sides' cable
CSCvq25320	Get-Config using NETCONF interrupted if authenticated with TACACS+
CSCvq26821	Shaper of the internal crypto interface is incorrectly programmed
CSCvq31129	AppNav: Optimization failed with Asymmetrical traffic, VRF, FNF and NBAR
CSCvq31871	Router crashes with ZBF HA sync.
CSCvq36130	Router is on Bootloop after QoS configuration.
CSCvq36179	Interfaces with 'shutdown' configuration in UP state
CSCvq42239	F0: fman_fp unexpectedly crashed with exmem chunk alloc
CSCvq43550	C1111-4P doesn't restart authentication for "clear authen session" if "authen open" the port
CSCvq46526	DMVPN	Spoke to Spoke traffic fails when Tunnel initiated by Tunnel IP to tunnel IP pings.
CSCvq49000	Supervisor reloaded due to cpp_cp_svr process crashing

Related Information

- Hardware Installation Guide

- Software Configuration Guide

- Smart Licensing using Policy

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.

Documentation Feedback

To provide feedback about Cisco technical documentation, use the feedback form available in the right pane of every online document.

Troubleshooting

For the most up-to-date, detailed troubleshooting information, see the Cisco TAC website at https://www.cisco.com/en/US/support/index.html.

Go to **Products by Category** and choose your product from the list, or enter the name of your product. Look under **Troubleshoot and Alerts** to find information for the issue that you are experiencing.