Release Notes for Cisco 3800 Series Integrated Services Routers with Cisco IOS Release 12.4(15)XY

First Released: December 17, 2007
Last Revised: March 25, 2009
Cisco IOS Release 12.4(15)XY5
OL-15502-03 Fifth Release

These release notes describe new features and significant software components for the Cisco 3800 series routers that support the Cisco IOS Release 12.4(15)XY releases. These release notes are updated as needed. Use these release notes with the *Cross-Platform Release Notes for Cisco IOS Release 12.4T* and *About Cisco IOS Release Notes* .

For a list of the software caveats that apply to Cisco IOS Release 12.4(15)XY, see the "Caveats" section on page 13 and *Caveats for Cisco IOS Release 12.4(15)T*. The online caveats document is updated for every maintenance release.

Contents

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

System Requirements

This section describes the system requirements for Release 12.4(15)XY and includes the following sections:

Memory Requirements

Table 1 describes the memory requirements for the Cisco IOS feature sets supported by Cisco IOS Release 12.4(15)XY on the Cisco 3800 series routers.

Table 1 Required Memory for Cisco 3800 Series Routers with Cisco IOS Release 12.4(15)XY

Platform	Image Name	Feature Set	Image	Flash Memory (MB)	DRAM (MB)
Cisco 3825	Cisco 3825 Advanced Enterprise Services	Advanced Enterprise Services	adventerprisek9-mz	64	256
	Cisco 3825 AISK9-AESK9 Feature Set Factory Upgrade For Bundles	AISK9-AESK9 Feature Set Factory Upgrade For Bundles		64	256
	Cisco 3825 ASK9-AESK9 Feature Set Factory Upgrade For Bundles	ASK9-AESK9 Feature Set Factory Upgrade For Bundles		64	256
	Cisco 3825 SPSK9-AESK9 Feature Set Factory Upgrade For Bundles	SPSK9-AESK9 Feature Set Factory Upgrade For Bundles		64	256
	Cisco 3825 INT Voice/Video, IPIPGW, TDMIP GW AES	INT Voice/Video, IPIPGW, TDMIP GW AES	adventerprisek9_ivs-mz	64	256
	Cisco 3825 Advanced Enterprise Services With SNA Switching	Advanced Enterprise Services With SNA Switching	adventerprisek9_sna-mz	64	256
	Cisco 3825 Advanced IP Services	Advanced IP Services	advipservicesk9-mz	64	256
	Cisco 3825 ASK9-AISK9 Feature Set Factory Upgrade For Bundles	ASK9-AISK9 Feature Set Factory Upgrade For Bundles		64	256
	Cisco 3825 SPSK9-AISK9 Feature Set Factory Upgrade For Bundles	SPSK9-AISK9 Feature Set Factory Upgrade For Bundles		64	256

Table 1 Required Memory for Cisco 3800 Series Routers with Cisco IOS Release 12.4(15)XY (continued)

Platform	Image Name	Feature Set	Image	Flash Memory (MB)	DRAM (MB)
Cisco 3825	Cisco 3825 AISK9-AISK9 Feature Set Factory Upgrade For Bundles	AISK9-AISK9 Feature Set Factory Upgrade For Bundles	advipservicesk9-mz	64	256
	Cisco 3825 Advanced Security	Advanced Security	advsecurityk9-mz	64	256
	Cisco 3825 ASK9-ASK9 Feature Set Factory Upgrade For Bundles	ASK9-ASK9 Feature Set Factory Upgrade For Bundles		64	256
	Cisco 3825 Enterprise Base without Crypto	Enterprise Base without Crypto	entbase-mz	64	256
	Cisco 3825 Enterprise Base	Enterprise Base	entbasek9-mz	64	256
	Cisco 3825 Enterprise Services without Crypto	Enterprise Services without Crypto	entservices-mz		
	Cisco 3825 Enterprise Services	Enterprise Services	entservicesk9-mz	64	256
	Cisco 3825 SPSK9-ESK9 Feature Set Factory Upgrade For Bundles	SPSK9-ESK9 Feature Set Factory Upgrade For Bundles		64	256
	Cisco 3825 IP Base w/o Crypto	IP Base w/o Crypto	ipbase-mz	64	256
	Cisco 3825 IP Base	IP Base	ipbasek9-mz	64	256
	Cisco 3825 IP Voice w/o Crypto	IP Voice w/o Crypto	ipvoice-mz	64	256
	Cisco 3825 INT Voice/Video, IPIP GW, TDMIP GW	INT Voice/Video, IPIP GW, TDMIP GW	ipvoice_ivs-mz	64	256
	Cisco 3825 IP Voice	IP Voice	ipvoicek9-mz	64	256
	Cisco 3825 SP Services	SP Services	spservicesk9-mz	64	256
	Cisco 3825 SPSK9-SPSK9 Feature Set Factory Upgrade For Bundles	SPSK9-SPSK9 Feature Set Factory Upgrade For Bundles		64	256

Table 1 Required Memory for Cisco 3800 Series Routers with Cisco IOS Release 12.4(15)XY (continued)

Platform	Image Name	Feature Set	Image	Flash Memory (MB)	DRAM (MB)
Cisco 3845	Cisco 3845 Advanced Enterprise Services	Advanced Enterprise Services	adventerprisek9-mz	64	256
	Cisco 3845 AISK9-AESK9 Feat Set Factory Upgrade For Bundles	AISK9-AESK9 Feat Set Factory Upgrade For Bundles		64	256
	Cisco 3845 ASK9-AESK9 Feature Set Factory Upgrade For Bundles	ASK9-AESK9 Feature Set Factory Upgrade For Bundles		64	256
	Cisco 3845 SPSK9-AESK9 Feature Set Factory Upgrade For Bundles	SPSK9-AESK9 Feature Set Factory Upgrade For Bundles		64	256
	Cisco 3845 INT Voice/Video, IPIPGW, TDMIP GW AES	INT Voice/Video, IPIPGW, TDMIP GW AES	adventerprisek9_ivs-mz	64	256
	Cisco 3845 INT Voice/Video GK, IPIPGW, TDMIP GW AES, LI	INT Voice/Video GK, IPIPGW, TDMIP GW AES, LI	adventerprisek9_ivs_li-mz	64	256
	Cisco 3845 Advanced Enterprise Services With SNA Switching	Advanced Enterprise Services With SNA Switching	adventerprisek9_sna-mz	64	256
	Cisco 3845 Advanced IP Services	Advanced IP Services	advipservicesk9-mz	64	256
	Cisco 3845 ASK9-AESK9 Feature Set Factory Upgrade For Bundles	ASK9-AESK9 Feature Set Factory Upgrade For Bundles		64	256
	Cisco 3845 SPSK9-AISK9 Feature Set Factory Upgrade For Bundles	SPSK9-AISK9 Feature Set Factory Upgrade For Bundles		64	256
	Cisco 3845 AISK9-AISK9 Feat Set Factory Upgrade For Bundles	AISK9-AISK9 Feat Set Factory Upgrade For Bundles		64	256
	Cisco 3845 Advanced Security	Advanced Security	advsecurityk9-mz	64	256
	Cisco 3845 ASK9-ASK9 Feature Set Factory Upgrade For Bundles	ASK9-ASK9 Feature Set Factory Upgrade For Bundles		64	256
	Cisco 3845 Enterprise Base without Crypto	Enterprise Base without Crypto	entbase-mz	64	256
	Cisco 3845 Enterprise Base	Enterprise Base	entbasek9-mz	64	256
	Cisco 3845 Enterprise Services without Crypto	Enterprise Services without Crypto	entservices-mz	64	256

Table 1 Required Memory for Cisco 3800 Series Routers with Cisco IOS Release 12.4(15)XY (continued)

Platform	Image Name	Feature Set	Image	Flash Memory (MB)	DRAM (MB)
Cisco 3845	Cisco 3845 Enterprise Services	Enterprise Services	entservicesk9-mz	64	256
	Cisco 3845 SPSK9-ESK9 Feature Set Factory Upgrade For Bundles	SPSK9-ESK9 Feature Set Factory Upgrade For Bundles		64	256
	Cisco 3845 IP Base without Crypto	IP Base without Crypto	ipbase-mz	64	256
	Cisco 3845 IP Base	IP Base	ipbasek9-mz	64	256
	Cisco 3845 IP Voice without Crypto	IP Voice without Crypto	ipvoice-mz	64	256
	Cisco 3845 INT Voice/Video, IPIP GW, TDMIP GW	INT Voice/Video, IPIP GW, TDMIP GW	ipvoice_ivs-mz	64	256
	Cisco 3845 IP Voice	IP Voice	ipvoicek9-mz	64	256
	Cisco 3845 SP Services	SP Services	spservicesk9-mz	64	256
	Cisco 3845 SPSK9-SPSK9 Feature Set Factory Upgrade For Bundles	SPSK9-SPSK9 Feature Set Factory Upgrade For Bundles		64	256

Hardware Supported

Cisco IOS Release 12.4(15)XY supports the following Cisco 3800 series routers:

- Cisco 3825
- Cisco 3845

For descriptions of existing hardware features and supported modules, see the hardware installation guides, configuration and command reference guides, and additional documents specific to the Cisco 3800 series routers at:

http://www.cisco.com/en/US/products/ps5855/tsd_products_support_series_home.html

Determining the Software Version

To determine the version of Cisco IOS software currently running on your Cisco 3800 series router, see *About Cisco IOS Release Notes* located at http://www.cisco.com/en/US/docs/ios/12_4/12_4x/12_4xy15/ReleaseNote.html.

Upgrading to a New Software Release

For general information about upgrading to a new software release, see *About Cisco IOS Release Notes* located at http://www.cisco.com/en/US/docs/ios/12_4/12_4x/12_4xy15/ReleaseNote.html.

Feature Set Tables

For information about Feature Set Tables, see *About Cisco IOS Release Notes* located at http://www.cisco.com/en/US/docs/ios/12_4/12_4x/12_4xy15/ReleaseNote.html.

New and Changed Information

This section contains the following information:

New Hardware Features in Cisco IOS Release 12.4(15)XY5

There are no new hardware features in this release.

New Software Features in Cisco IOS Release 12.4(15)XY5

There are no new software features in this release.

New Hardware Features in Cisco IOS Release 12.4(15)XY4

There are no new hardware features in this release.

New Software Features in Cisco IOS Release 12.4(15)XY4

The are no new software features in this release.

New Hardware Features in Cisco IOS Release 12.4(15)XY3

There are no new hardware features in this release.

New Software Features in Cisco IOS Release 12.4(15)XY3

The are no new software features in this release.

New Hardware Features in Cisco IOS Release 12.4(15)XY2

There are no new hardware features in this release.

New Software Features in Cisco IOS Release 12.4(15)XY2

The are no new software features in this release.

New Hardware Features in Cisco IOS Release 12.4(15)XY1

There are no new hardware features in this release.

New Software Features in Cisco IOS Release 12.4(15)XY1

The new software features are:

- Transparent Tunneling of QSIG over SIP-TDM Gateway, page 7
- SIP SRTP fallback to non-secure RTP, page 8
- Pass data in SIP REFER to triggered INVITE, control media-cut through on SIP 18x response, page 8

Transparent Tunneling of QSIG over SIP-TDM Gateway

The “Transparent Tunneling of QSIG over SIP-TDM Gateway” feature provides transparent transport of QSIG-protocol ISDN messages across the SIP trunk. In 12.4(15)XY1, this solution is supported only for QSIG protocol messages, unlike H.323 gateways, which tunnel any raw message. This solution encapsulates QSIG messages within SIP message bodies using application/qsig MIME to tunnel between SIP endpoints. This solution does not add any QSIG services to SIP interworking.

In 12.4(15)XY1, QSIG tunneling is supported only on SIP-TDM gateways with ISDN PRI or BRI. So Cisco Unified Border Element (Cisco UBE), formerly known as the Cisco IOS Session Border Controller (SBC) or the Cisco Multiservice IP-to-IP Gateway, cannot yet utilise this feature.

SIP SRTP fallback to non-secure RTP

The "SIP SRTP fallback to non-secure RTP" feature provides compatibility with Cisco Unified Communications Manager, version 7.0 (formerly known as Cisco Unified CallManager). SRTP fallback to RTP was previously supported between two gateways. Now, with a new negotiation method introduced in 12.4(15)XY1, support for this feature is provided between the gateways and the Cisco Unified Communications Manager.

Pass data in SIP REFER to triggered INVITE, control media-cut through on SIP 18x response

The control media-cut through on SIP 18x response feature provides the ability to send media backward even before the call is established. So instead of allowing media to flow both ways only after the call is established, this feature allows the remote side to send a personalized ringback tone (usually music) as a response even before the call is established.

Doing only backward media cut-through on 18x messages affects the digit collection process (RFC 2833 mechanism) before the call is connected (SIP 200 OK message is sent and accepted). Since most of the SIP IVR deployments use RFC 2833 to collect digits before a call is connected, the current default behavior (bidirectional media cut-through on 18x) is retained.

The Pass data in SIP REFER to triggered INVITE feature provides the ability to map SIP REFER message data into SIP INVITE messages. This new feature allows you to send customer-specific information to triggered SIP INVITE messages using Call-Info as the URL header of the SIP REFER-TO message. Further, this feature allows the gateway to take SIP REFER data and create a new SIP INVITE message to a new destination when a call is being placed to an Interactive Voice Response (IVR) endpoint and the IVR refers the call to an agent or to another IVR system.

New Hardware Features in Cisco IOS Release 12.4(15)XY

The new hardware features are:

- Transport Optimization Service Module, page 9
- Cisco Intrusion Prevention System Advanced Integration Module (AIM-IPS), page 9

Transport Optimization Service Module

The Transport Optimization Service Module (TPO) is a Linux-based application that resides on a module that plugs into a host Cisco router running Cisco IOS software. To satisfy various system configurations, there are three types of modules as shown in Table 2.

Table 2 Transport Optimization Service Module

Module	Concurrent Connections	Memory Size	Description
AIM-TPO-1	1000	512 MB	Installed in the router and not accessible by the customer.
AIM-TPO-2	2000	1 GB	Installed in the router and not accessible by the customer.
NME-TPO	4000	1 GB	Can be removed and replaced by the customer.

The module is a standalone transport-optimization engine with own startup and run-time configurations. The module does not have an external console port. Instead, you launch and configure the module through the router, by means of a configuration session on the module. After the session, you return to the router CLI and clear the session.

This arrangement—host router plus module (the latter is also sometimes called an appliance or blade or, with installed software, a service or services engine)—provides a router-integrated application platform for accelerating data-intensive TCP-based applications. Such applications typically involve the following:

- Transport layer optimization
- L4 compression

The transport optimization service module is supported on the Cisco access routers Table 3:

Table 3 Supported Routers

Module	Cisco Router
AIM - TPO - 1	1841, 2801, 2811, 2821, 2851, 3825, 3845
AIM - TPO - 2	1841, 2801, 2811, 2821, 2851, 3825, 3845
NME - TPO	2811, 2821, 2851, 3825, 3845

Cisco Intrusion Prevention System Advanced Integration Module (AIM-IPS)

Cisco Intrusion Prevention System Advanced Integration Module (AIM-IPS) integrates and bring inline Cisco IPS functionality to Cisco access routers. You can install AIM-IPS in the Cisco 1841, Cisco 2800 series, and Cisco 3800 series routers.

New Software Features in Cisco IOS Release 12.4(15)XY

The new software features are:

Land Mobile Radio over IP Enhancement

Support for RFC 2833 was added to the Land Mobile Radio (LMR) gateway. This enhancement allows tones to be generated dynamically.

For more information, go to:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t7/feature/guide/gtlmrip.html

Cisco Unified SRST and Cisco Unified CME

Enhanced 911 Services for Cisco Unified SRST and Cisco Unified CME enables 911 operators to:

- Immediately pinpoint the location of the 911 caller based on the calling number
- Callback the 911 caller if a disconnect occurs

Before this feature was introduced, Cisco Unified CME supported only outbound calls to 911. With basic 911 functionality, calls were simply routed to a public safety answering point (PSAP). The 911 operator at the PSAP would then have to verbally gather the emergency information and location from the caller, before dispatching a response team from the ambulance service, fire department, or police department. Calls could not be routed to different PSAPs, based on the specific geographic areas that they cover.

With Enhanced 911 Services, 911 calls are selectively routed to the closest PSAP based on the caller's location. In addition, the caller's phone number and address automatically display on a terminal at the PSAP. Therefore, the PSAP can quickly dispatch emergency help, even if the caller is unable to communicate the location. Also, if the caller disconnects prematurely, the PSAP has the information it needs to contact the 911 caller.

HFC RIP Relay

The HFC RIP Relay feature allows the delivery of Routing Information Protocol (RIP) messages from a Cisco IOS router containing a cable High-Speed WAN Interface Card (HWIC) to the Hybrid Fiber-Coaxial (HFC) Cable Modem Termination system (CMTS) when they are on different subnets. Configuring a static IP address is now also supported on a cable modem interface.

For more information, see:
http://www.cisco.com/en/US/docs/ios/iproute/configuration/guide/irp_rip_hfc.html

G.722-64 and iLBC Codec

The G.722-64 and iLBC codecs are supported for Cisco Unified Communications Manager Express, Cisco Unified Border Elements (Cisco UBEs), DSP Farm, and voice gateways. Conferencing and universal transcoding are supported on both codecs.

Cisco Unified Border Element (Cisco UBE)

H.323 Video Calls Support for H.239 Signalling allows H.323 Video calls that include H.239 signalling to support Picture in Picture to be passed through the Cisco Unified Border Element. This feature enables over 200 new rooms of Business to Business Telepresence connections; Interworking of Secure RTP calls for SIP and H323 provides the ability to have a Secure RTP (sRTP) calls connected using H323 to SIP and SIP to SIP (FTS-8240-1); H323 Video Calls Support for H.235 Security - Supports H.235 Media Security enabled on H.323 Video Calls to be signalled through a Cisco Unified Border Element (Cisco UBE).

Default Audio Prompt Streaming Behavior Change

This feature changes the default behavior of the ivr prompt streamed command. If you do not use this command, audio prompts from HTTP URLs and other media types are not streamed during playback. Before this feature, the default was streaming for audio prompts from HTTP URLs and other media types during playback. See the link below for more information on the ivr prompt streamed command:

http://www.cisco.com/en/US/docs/ios/12_3t/voice/command/reference/vrht_i2_ps5207_TSD_Products_Command_Reference_Chapter.html#wp1102051

New Features in Release 12.4T

For information regarding the features supported in Cisco IOS Release 12.4T, see the Cross-Platform Release Notes links at : http://www.cisco.com/en/US/products/ps6441/prod_release_notes_list.html

Limitations and Restrictions

Limitations and Restriction - Release 12.4(15)XY

- Interoperability between Cisco Unified CME and Cisco Unified CCX is restricted to one Cisco Unified CCX per Cisco Unified CME.
- Support for Multi-Party Ad Hoc and Meet-Me Conferencing features is not provided.
- Only incoming calls from PSTN trunk are supported for deployment of the Interoperability feature. Other trunks, such as SIP and H.323, are supported as usual in Cisco Unified CME, however, not for customer calls to Cisco Unified CCX.
- Only SCCP phones can be configured as agent phones in Cisco Unified CME. The Cisco VG224 Analog Phone Gateway and analog and SIP phones are supported as usual in Cisco Unified CME, however, not as Cisco Unified CCX agent phones.
- Cisco Unified IP Phone 7931 cannot be configured as an agent phone in Cisco Unified CME. Cisco Unified IP Phone 7931s are supported as usual in Cisco Unified CME, however, not as Cisco Unified CCX agent phones.
- Shared-line appearance is not supported on Cisco Unified CCX agent phones in Cisco Unified CME. A directory number cannot be associated with more than one physical agent phone at one time.
- Overlaid lines are not supported on Cisco Unified CCX agent phones in Cisco Unified CME. More than one directory number cannot be associated with a single line button on an agent phone.
- Monitored mode for a line button is not supported on Cisco Unified CCX agent phones in Cisco Unified CME. An agent phone cannot be monitored by another phone
- For call forward and call pickup, the directory number of a Cisco Unified CCX agent cannot forward to a Cisco CRS route point.

Caveats

For general information on caveats and the bug toolkit, see *About Cisco IOS Release Notes* located at http://www.cisco.com/en/US/docs/ios/12_4/12_4x/12_4xy15/ReleaseNote.html.

This sections contains the following information:

Open Caveats - Release 12.4(15)XY5

Ther are no open caveats in this release.

Resolved Caveats - Release 12.4(15)XY5

- CSCsv04836

  Multiple Cisco products are affected by denial of service (DoS) vulnerabilities that manipulate the state of Transmission Control Protocol (TCP) connections. By manipulating the state of a TCP connection, an attacker could force the TCP connection to remain in a long-lived state, possibly indefinitely. If enough TCP connections are forced into a long-lived or indefinite state, resources on a system under attack may be consumed, preventing new TCP connections from being accepted. In some cases, a system reboot may be necessary to recover normal system operation. To exploit these vulnerabilities, an attacker must be able to complete a TCP three-way handshake with a vulnerable system.

  In addition to these vulnerabilities, Cisco Nexus 5000 devices contain a TCP DoS vulnerability that may result in a system crash. This additional vulnerability was found as a result of testing the TCP state manipulation vulnerabilities.

  Cisco has released free software updates for download from the Cisco website that address these vulnerabilities. Workarounds that mitigate these vulnerabilities are available.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090908-tcp24.shtml.

CSCsm97220

Devices that are running Cisco IOS Software and configured for Mobile IP Network Address Translation (NAT) Traversal feature or Mobile IPv6 are vulnerable to a denial of service (DoS) attack that may result in a blocked interface.

Cisco has released free software updates that address these vulnerabilities.

This advisory is posted at the following link
http://www.cisco.com/warp/public/707/cisco-sa-20090325-mobileip.shtml

CSCsr29468

Cisco IOS software contains a vulnerability in multiple features that could allow an attacker to cause a denial of service (DoS) condition on the affected device. A sequence of specially crafted TCP packets can cause the vulnerable device to reload.

Cisco has released free software updates that address this vulnerability.

Several mitigation strategies are outlined in the workarounds section of this advisory.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090325-tcp.shtml

CSCso04657

Symptom SSLVPN service stops accepting any new SSLVPN connections.

Conditions A device configured for SSLVPN may stop accepting any new SSLVPN connections, due to a vulnerability in the processing of new TCP connections for SSLVPN services. If “debug ip tcp transactions” is enabled and this vulnerability is triggered, debug messages with connection queue limit reached will be observed. This vulnerability is documented in two separate Cisco bug IDs, both of which are required for a full fix: CSCso04657 and CSCsg00102.

CSCsk40676 C1812 12.4.15.T / certain pkt size block inside interface of ezvpn conn.

Symptom The inside interface of a Cisco router running EZVPN may become unresponsive when sending ICMP messages from a remote VPN client connection.

Conditions Occurs when LZS compression is used on a Windows Vista client.

Workaround Disable LZS compression.

CSCse85652 HTTP should deny access if no enable password is configured.

CSCsg04630 7600BB: DHCP:STB crash MEM corruption at dhcpd_add_binding_to_radix_tree

CSCsj50526 Special-Services-Engine default booting from secondary boot loader.

Conditions When Special-Services-Engine (NME-RVPN) in a 3845 router is reset with **default-boot set**, it is booting from the secondary boot loader. By default, it should boot from the primary boot loader.

Workaround Try to set it via the **config** command instead of trying through **default-boot set** CLI.

CSCsk32970 ccm switchover fails as ACL does not deny properly.

Symptom Alternative packets are not being dropped by Extended ACL with deny statements in cef switching path.

Conditions When CEF is enabled.

Workaround Disable CEF or use standard ACL.

CSCsk58014 Module fails to boot up after reset.

Symptom The module will not return to the steady state after a reset.

Conditions This symptom is observed whenever the module is reset.

Workaround There is no workaround.

CSCsk61991 dsl controller with auto linemode is down with peer in 4-wire linemode.

Symptom Ping failure is seen over ATM interface in 4-wire line mode as the ATM interface does not come up.

Conditions With the UUT configured as auto the ATM interface continues to be down after the peer changes from 2-wire to 4-wire enhanced. This happens only on WIC-1SHDSL with UUT configured as auto which is not recommended.

Workaround Do not configure the line mode as auto.

CSCsk63655 MGCP gateway returns 524 instead of 200 for a valid LCO param in CRCX.

Symptom A Media Gateway Control Protocol (MGCP) gateway may return a 524 or 510 error code with the reason as "invalid local connection option" for a valid "L:" parameter in a CRCX message.

Conditions The symptoms can be observed on a router that is running Cisco IOS Interim Release 12.4(17.4)T1 or later, when the <CmdBold>debug mgcp parser<noCmdBold> command with verbose tracelevel is disabled.

Workaround Enable <CmdBold>debug mgcp parser<noCmdBold> with verbose tracelevel.

CSCsk70060 crafted packets to UDP port 2887 with AP HWIC may cause queue wedge.

Symptom Crafted packets to UDP port 2887 with AP HWIC may cause queue wedge.

Conditions The router must have AP HWIC installed, and UDP port 2887open.

Workaround None.

CSCsk92135 UUT with ADSL over POTS card goes to hang state while booting IOS.

Symptom Routers with ADSL over POTS card hang on booting Cisco IOS Release 12.4(16.14)T4 and above.

Conditions Issue seems to be specific to the ADSL over POTS card.

Workaround There is no workaround.

CSCsk93241 Chunk memory corruption on LFDp Input Proc.

Cisco IOS Software Multi Protocol Label Switching (MPLS) Forwarding Infrastructure (MFI) is vulnerable to a Denial of Service (DoS) attack from specially crafted packets. Only the MFI is affected by this vulnerability. Older Label Forwarding Information Base (LFIB) implementation, which is replaced by MFI, is not affected. Cisco has released free software updates that address this vulnerability.

This advisory is posted at

http://www.cisco.com/warp/public/707/cisco-sa-20080924-mfi.shtml

CSCsl04399 PRI FAX calls failing for E1 controller.

Symptom Fax call is aborted while testing PRI E1 feature.

Conditions Occurs in routers running a pre-release version of Cisco IOS Release 12.4(15)T2.

Workaround Use the **<CmdBold>fax rate disable<noCmdBold>** command to disable the fax relay feature under the VoIP dialpeer.

CSCsl22080 12.4.15T: WebVPN stops working with TCP connection queue limit reached.

Symptom WebVPN hangs after a few days of working. When this happens, no WebVPN connections are active and no new connections can be established. The **<CmdBold>debug ip tcp transaction<noCmdBold>** command shows <CmdBold>connection queue limit reached: port 443<noCmdBold> errors. The **<CmdBold>show tcp brief<noCmdBold>** command displays many sessions in SYNRCVD and TIMEWAIT states. Problem is recovered either by reload or by entering the **<CmdBold>clear tcp tcb *<noCmdBold>** command. There are few stale sessions in CLOSED state left after clearing TCP.

Conditions Issue seen in Cisco IOS Release 12.4.15T and Cisco IOS Release 12.4.15T1 when WebVPN is configured. The issue is intermittent and happens after a few days or weeks of working.

Workaround To restore TCP connectivity, issue **<CmdBold>clear tcp tcb *<noCmdBold>** or reload the router. Note that this will clear all TCP sessions on the router.

CSCsm45113 RIB installs duplicate routes for the same prefix.

Symptom Router may install duplicate routes or incorrect route netmask into routing table. It could happen on any routing protocol. Additionally, for OSPF, crash was observed.

Conditions The problem is triggered by SNMP polling of ipRouteTable MIB. The problem is introduced by CSCsj50773, see the Integrated-in field of CSCsj50773 for affected images.

Workaround Do not poll ipRouteTable MIB, poll newer replacement ipForward MIB, instead. The ipRouteTable MIB was replaced by ipForward MIB in RFC 1354.

Further Problem Description: The **<CmdBold>clear ip route *<noCmdBold>** command can correct the routing table until the next poll of ipRouteTable MIB.

CSCso18940 snmpwalk on 'ipRouteTable' returns error - OID not increasing.

CSCso60174 Multiple duplicate descriptions found for mmoip aaa commands.

CSCsq15993 PBR is not supported in CEF switching path on 12.4(15)XY release

CSCsr15478 Input Queue Wedging.

Symptom An input wedge is observed on an interface, when multicast traffic is flowing.

Conditions The symptom is observed in a DMVPN hub-spoke scenario with a point-to-multipoint (P2MP) GRE tunnel having tunnel protection configuration. When multicast traffic flows from hub to spoke through these tunnel interfaces, the incoming interface of the hub is getting wedged and even the ping to peer stops working.

Workaround There is no workaround, other than reloading the router.

CSCsu64215 ip tcp adjust-mss command results in packet loss for non-TCP traffic.

Open Caveats - Release 12.4(15)XY4

There are no open caveats in this release.

Resolved Caveats - Release 12.4(15)XY4

- CSCsq58779

  Cisco IOS devices that are configured for Cisco Unified Communications Manager Express (CME) and the Extension Mobility feature are vulnerable to a buffer overflow vulnerability. Successful exploitation of this vulnerability may result in the execution of arbitrary code or a Denial of Service (DoS) condition on an affected device.

  Cisco has released free software updates that address this vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090923-cme.shtml.

CSCso56129 %SYS-2-BADSHARE: Bad refcount in datagram_done monitoring cme/cue calls

Symptom Bad Refcount is seen with tracebacks.

Conditions Using AIM-IPS-K9 to monitor interfaces with ephones registered to the CME on the same router and have ephone check voice mail. This is in a branch in a box setup. UUT serves as a CME as well as having the voice mail AIM in the same router.

Workaround There is no workaround.

CSCso66843 CUBE and CME do not change embedded SSRC in RTCP packets

Symptom Different SSRC in RTCP compared to RTP after transcoding.

Conditions Voice call with transcoding in CUBE or CME.For a voice call passing through transcoding on CUBE or CME, the SSRC value contained within the RTCP is passed unchanged, whereas the SSRC value contained within the RTP is changed. This creates a mismatch between the SSRC between RTP and RTCP at the final destination.

Workaround There is no workaround.

CSCso67655 S2 CFD: Secure DSPFarm doesn't register after a reload of the router

Symptom After Reolad Secure Conference profile does not register with CCM.

Conditions This happens when a specific trustpoint is specified for CCM cert authentication during TLS handshake.

Workaround The workaround is not to specify the truspoint when configuring callmanger CCM using CLI "sccp ccm <ip address> tag version <x>.

CSCsq44013 View used twice with logging enabled

Symptom The CPE does not reply to the DNS query from the client for the first try, first response is being dropped.

Conditions This is seen on a router running 12.4T IOS image configured with split DNS.

Workaround There is no workaround.

Open Caveats - Release 12.4(15)XY3

There are no open caveats in this release.

Resolved Caveats - Release 12.4(15)XY3

CSCsk62253

Cisco IOS software contains two vulnerabilities within the Cisco IOS WebVPN or Cisco IOS SSLVPN feature (SSLVPN) that can be remotely exploited without authentication to cause a denial of service condition. Both vulnerabilities affect both Cisco IOS WebVPN and Cisco IOS SSLVPN features:

1. Crafted HTTPS packet will crash device - Cisco Bug ID CSCsk62253.
2. SSLVPN sessions cause a memory leak in the device - Cisco Bug ID CSCsw24700.

Cisco has released free software updates that address these vulnerabilities. There are no workarounds that mitigate these vulnerabilities. This advisory is posted at the following link: http://www.cisco.com/warp/public/707/cisco-sa-20090325-webvpn.shtml

CSCsk42759

Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS that can be exploited remotely to trigger a memory leak or to cause a reload of the Cisco IOS device.

Cisco has released free software updates that address these vulnerabilities. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities addressed in this advisory.

There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself, if administrators do not require the Cisco IOS device to provide voice over IP services.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20080924-sip.shtml.

CSCsl62609

Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS that can be exploited remotely to trigger a memory leak or to cause a reload of the Cisco IOS device.

Cisco has released free software updates that address these vulnerabilities. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities addressed in this advisory.

There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself, if administrators do not require the Cisco IOS device to provide voice over IP services.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20080924-sip.shtml.

CSCso81854

Multiple Cisco products are vulnerable to DNS cache poisoning attacks due to their use of insufficiently randomized DNS transaction IDs and UDP source ports in the DNS queries that they produce, which may allow an attacker to more easily forge DNS answers that can poison DNS caches.

To exploit this vulnerability an attacker must be able to cause a vulnerable DNS server to perform recursive DNS queries. Therefore, DNS servers that are only authoritative, or servers where recursion is not allowed, are not affected.

Cisco has released free software updates that address these vulnerabilities.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20080708-dns.shtml.

This security advisory is being published simultaneously with announcements from other affected organizations.

CSCsk42419

Symptom The Secure Shell server (SSH) implementation in Cisco IOS contains multiple vulnerabilities that allow unauthenticated users the ability to generate a spurious memory access error or, in certain cases, reload the device.

The IOS SSH server is an optional service that is disabled by default, but its use is highly recommended as a security best practice for management of Cisco IOS devices. SSH can be configured as part of the AutoSecure feature in the initial configuration of IOS devices, AutoSecure run after initial configuration, or manually. Devices that are not configured to accept SSH connections are not affected by these vulnerabilities.

Common Vulnerabilities and Exposures (CVE) identifier CVE-2008-1159 has been assigned to this bug.

The Security Advisory for this issue is posted at

http://www.cisco.com/warp/public/707/cisco-sa-20080521-ssh.shtml

CSCsk60020

Symptom The Secure Shell server (SSH) implementation in Cisco IOS contains multiple vulnerabilities that allow unauthenticated users the ability to generate a spurious memory access error or, in certain cases, reload the device.

The IOS SSH server is an optional service that is disabled by default, but its use is highly recommended as a security best practice for management of Cisco IOS devices. SSH can be configured as part of the AutoSecure feature in the initial configuration of IOS devices, AutoSecure run after initial configuration, or manually. Devices that are not configured to accept SSH connections are not affected by these vulnerabilities.

Common Vulnerabilities and Exposures (CVE) identifier CVE-2008-1159 has been assigned to this bug. The Security Advisory for this issue is posted at

http://www.cisco.com/warp/public/707/cisco-sa-20080521-ssh.shtml.

CSCsk29999 AIM-IPS-K9:TCP intercept not entering aggressive mode

Symptom When configuring the AIM-IPS-K9 with tcp intercept, the tcp intercept may not enter aggressive mode. Traffic is not impacted.

Conditions When the performance level of passing packets to the IPS application is below the window size at which the IPS application enters aggressive mode, it will not enter aggressive mode. On low-end platforms where the router is a constrictor on traffic sent to the card, this problem may be more pronounced.

Workaround Do not configure tcp intercept with AMI-IPS-K9.

CSCsl61734 CUBE slow start h323 to sip transfer = dead air

Symptom Slow start H323 to SIP calls may experience no-way audio if the call is transferred after initially connected.

Conditions This only occurs with slow start H323.

Workaround Use fast start H323.

CSCsl68798 %SYS-2-PAK_SUBBLOCK_SETSIZE traceback at control_plane_init() at boot

Symptom At boot-time an IOS device may generate tracebacks of the form:

```
*Mar 1 00:00:10.339:%SYS-2-PAK_SUBBLOCK_SETSIZE: 28 -Process= "Init", ipl= 3, pid= 3,
-Traceback= 0x601597F4 0x60260E80 0x602C3928 0x6014E588 0x6014E7E4 0x6028B680 0x6028B664
```

Conditions This behaviour is observed on an IOS device installed with 12.5(0.5) or later or 12.4(15)XY IOS releases.

Workaround There is no known workaround.

CSCsl88956 Primary nvram is not properly restored after it is corrupted

Symptom when the Cisco 28xx and 38xx routers is reloaded, they loose the running configuration and startup configuration.

Conditions If the last physical sector of nvram which is shared by nvram and licensing subsystem is corrupted, primary nvram is not restored properly.

Workaround There is no known workaround.

Open Caveats - Release 12.4(15)XY2

There are no open caveats in this release.

Resolved Caveats - Release 12.4(15)XY2

CSCsi01875 IPIP gateway rejects a second TCS

Symptom Placing a video call from a Polycom device. The call gets rejected because Polycom sends a TCS before receiving the TCS ACK.

Conditions Polycom video endpoints and IP gateway.

Workaround There is no workaround.

CSCse60897 call-manager-fallback does not allow more than 5 redirects

Symptom After 5 redirects, calls fail with busy tone when in call-manager-fallback.

Conditions The maximum redirects seem to be 5 only.

Workaround There is no workaround.

CSCsk09472 printf_ptr warnings still exist after CSCsj92597

Symptom The printf_ptr warnings that would appear during a build of the obj-m8500-c1800/c180x-broadband-mz no longer appear.

Workaround Moving the define for printf_ptr to another file solved the issue.

CSCsl70220 Entity hierarchy issue in 1805 device

Symptom The root entity is pointing to modem card instead of chassis.

Conditions It will affect SNMP based management application like CiscoView.

Workaround There is no workaround.

CSCsl72097 Alignment Error seen in 3800 while making E1/r2 call.

Symptom While making E1/r2 calls alignment tracebacks were seen. The traceback reported where for alignment corrections.

Conditions The alignment errors were seen as we were accessing (writing into) non-aligned address.

Workaround Write using PUTLONG which will do a 4-byte write on un-aligned memory will fix this issue.

CSCsm34933 Refresh Re-Invite disconnect call because CUBE does not send out 200 OK

Symptom In 12.4(15)XY, when cube receives the session refresh re-invite with sdp then it sends 100 trying but no 200 OK and therefore call gets dropped.

Conditions Call gets dropped since no 200 OK sent by CUBE

Workaround There is no workaround.

CSCsm44512 Router crash when unconfigure PVC from ATM interface

Symptom Router might crash if unconfig the PVC from ATM interface without shutting down the interface first.

Conditions Crash only observed when interface was up before the PVC removal.

Workaround Shut down the ATM interface first before the PVC removal.

CSCsm44792 input gain auto-control -9 is added automatically to voice-ports.

Symptom The command is added automatically to the voice-port configuration: input gain auto-control -9. In addition, this command can not be removed by the "no input gain auto-control -9". This issue causes voice issues to the VTG in the IPICS system.

Conditions This issue is seen after upgrading router from 12.4(6)T6 or 12.5(15)T1 to 12.(4)15XY.

Workaround No known workaround.

This is a sample configuration of the voice port: voice-port 0/2/0:0 voice-class permanent 1 auto-cut-through lmr m-lead audio-gate-in lmr e-lead voice input gain auto-control -9 no echo-cancel enable playout-delay nominal 100 playout-delay minimum high no comfort-noise timeouts call-disconnect 3 timeouts teardown lmr infinity timing hookflash-in 0 timing hangover 40 connection trunk 19990929090 description #0/2/0:0#0# INUSE 1221.

Open Caveats - Release 12.4(15)XY1

CSCsl22920 - IOS gw not tunneling ISDN ALERTING message over SIP

Symptom ISDN QSIG ALERTING message received from Destination PINX is not transparently transported to Originating PINX.

Conditions This is seen if the Destination PINX sends ISDN QSIG CALL_PROC with PI==1 in response to ISDN QSIG SETUP message.

Workaround There is no workaround.

Further Problem Description: ISDN QSIG CALL_PROC with PI==1 received from destination PINX is converted to SIP 183 Preogress at TGW and hence treated as ISDN QSIG PROGRESS at OGW/Originating PINX. Due to this 183 corresponding to ISDN QSIG ALERTING from Dest PINX is dropped at OGW.

Resolved Caveats - Release 12.4(15)XY1

There are no resolved caveats in this release.

Open Caveats - Cisco IOS Release 12.4(15)XY

There are no open caveats in this release.

Resolved Caveats - Cisco IOS Release 12.4(15)XY

CSCsj85065

A Cisco IOS device may crash while processing an SSL packet. This can happen during the termination of an SSL-based session. The offending packet is not malformed and is normally received as part of the packet exchange.

Cisco has released free software updates that address this vulnerability.

Aside from disabling affected services, there are no available workarounds to mitigate an exploit of this vulnerability.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20080924-ssl.shtml.

CSCsj81296 - Multiple RTP tracebacks seen on IPIPGW when transcoding calls

Symptom Multiple tracebacks are seen on 5400XM operating as an IPIPGW while transcoding calls from G.729r8 to G.711.

Conditions This issue is seen on 12.4(15)T under normal circumstances even with a single call.

Workaround There is no workaround

CSCsl41697 - After disconnect, fetching doc more than 20s causes VXML session leak

Symptom The VXML session is not released, causes memory leakage when loading VXML document and takes more than 20 second after the user is disconnected.

Workaround There is no workaround.

CSCsj81015 - IPIP Gateway crash ccsip_bridge

Symptom Cisco Multiservice IP-to-IP Gateway (IPIPGW) crashes during a stress scenario.

Conditions This symptom occurs in a stress scenario with 100 SIP-H323 calls + 150 SIP-H323 DTMF interworking (rtp-nte to h245-alpha) calls.

Workaround There is no workaround.

CSCsk60054 Configuration buffer full. Cannot display show run

Symptom Upon certain configuration changes, the running configuration might not be able to be displayed and the following error message might appear:

```
% Configuration buffer full, can't add command:!
%Aborting Save. Compress the config, Save it to flash or Free up space on device
```

Conditions The issue is seen either using or not using service compress-config on a Cisco IOS Router running CallManager Express (CME) when configuring more than 22 voice user-profiles

Workaround There is no workaround.

CSCsj66774- No video with CUVA 2.0.2 and 7970 8-3-1S registered to CME 4.1

Symptom No video is seen on PC's using CVTA with 7970 ip phones registered to a CME 4.1 system.

Conditions CVTA is being used with a 7970 phone running firmware 8.3.1S

Workaround Downgrade 7970 firmware to 8.2.2SR1

CSCsk48250 - SW_MGR-3-SM_ERROR: Tracebacks found while establishing l2tpv3 tunnel

Symptom SW_MGR-3-SM_ERROR: Tracebacks found while establishing l2tpv3 tunnel and the tunnel is not established.

Conditions This issue is seen in the image 12.4(17.4)T1.

Workaround There is no workaround.

CSCsk90315 - router crashes while making voice calls with RSVP configuration

CSCsk67885 - Loading sudialog with record utterance fail cause memory leakage

Symptom When VXML script loading sudialog with record utterance, but record utterance loading fails, the VXML session is not freed. This causes memory leakage.

Conditions Loading recording utterance failure is an error case. It could be caused by ASR server configuration problem, or IOS configuration problem.

Workaround There is no workaround.

CSCsk64021 - VXML failing during record - Can not submit a streaming recording

Symptom A VXML gateway intermittently fails to submit a recording.

Conditions This symptom is observed in Cisco IOS Release 12.4.

Workaround There is no workaround.

CSCsk97130 - VXML tree not release when subdialog root document is shared

Symptom For a VXML application, if the calling document and called document of a subdialog shared the same root document, the tree structure used for the root document will not be released after the call session is finished. This causes memory leakage.

CSCsk53133 - VXML session not freed when disconnect event return from subdialog

Symptom BVXML session is not freed with the disconnect event returned from subdialog, and the event handler has exit tag. BConditions:BNABWorkaround:BNA

CSCsj97602 - Memory leak on mem_pool:: in Dead pool

Symptom A Cisco access server may run out of free processor memory. This symptom can be seen in the <CmdBld>show process memory<noCmdBld> command. Increased memory utilization will be seen in the Dead pool.

Conditions This symptom has been observed only in access servers that participate in Cisco Customer Voice Portal (CVP). When a VXML application is configured with fetchaudio, the fetchaudio playout fails after user disconnect. The fetchaudio should have been removed from the prompt list, but it was not. This causes the session not to be freed when the application is finished.

Workaround A reload will temporarily free the leaked memory.

CSCsj34213 Traceback detected at AFW_Leg_Connect

CSCsk48052 - HQF:HQF support for HDLC32 driver for 36/26/37XX in Spidey

CSCsj49237 - Memory leak found at make_fact_attr_list_max

CSCsl03149 - CUBE: SIP-H.323 call - Bad enqeue message and Tracebacks seen

CSCsj27183 - Transcoding: Call fails for H323--SIP Fast start call

Symptom H323-->SIP interworking fails for a Fast start call when transcoding is enabled on an IPIPGW. Transcoding is done between G711ulaw and G729r8 codecs.

Conditions This failure is seen for H323--SIP--SIP--SIP and H323--SIP--SIP-- H323 call flows when transcoding is enabled on IPIPGW1. It is also seen on H323--H323--H323--SIP call flow for transcoding on IPIPGW2.This is seen only with a Fast Start call (both with H245 Tunnel enabled and disabled), and the call passes with a slow start call.

Workaround There is no workaround

CSCsl17037 - CME: Local Directory Issue

Symptom Directory numbers that are configured in local directory of CME are not being shown in Received Calls directory. The number and name shows while call in Ringing state but is not showing during Connected state.

Conditions Inbound Call

Workaround There is no workaround.

CSCsl04115 - CM call to CME when Put on Hold, CME Hears FastBusy instead of TOH

Symptom Cisco IP Phone placed on hold hears fastbusy instead of tone-on-hold. A Cisco IP Phone registered with a Cisco Unified CallManager Express (CME) may hear a fastbusy tone when placed on hold. This can occur when interworking with Cisco Unified CallManager (CCM) as shown here:

```
IPPhoneA---CM---H323---CME---IpPhoneB

-  Phone A calls Phone B
-  Phone A puts Phone B on Hold.
-  Instead of playing Tone On Hold, Phone B user hears a fastbusy tone.
```

Workaround This behavior was introduced in 12.4(15)T. Either downgrade the IOS version on the CUCME or configure music-on-hold (MOH) to be played from CUCM, instead of TOH

CSCsk83750 Unexpected number of hashed queues invalid after attaching policy

CSCsk80620 - Tracebacks at send_vtsp_setup_request_to_csm

Symptom Traceback is seen on vtsp_ic_notify.

Conditions Traceback observed during a modem call

Workaround There is no workaround.

CSCsk92440 Traceback seen at vtsp_ic_notify in AS5350

Symptom Traceback is seen on vtsp_ic_notify.

Conditions Traceback observed even after single e1-r2 call.

Workaround There is no workaround.

CSCsk96251 H323 calls fails when non-default signaling port is used

Symptom H323 calls fails when non-default signaling port is used in dialpeer session target.

```
example: session target ipv4:192.168.1.1:2437
```

Conditions Failure is seen only when any specific signaling port is configured.

Workaround Configure only IP address so that it picks the default signaling port.

```
example: session target ipv4:192.168.1.1
```

CSCsi21389 One-way multicast traffic over wireless

Symptom Routers that have the ability to use the optional 802.11b/g card, such as the Cisco ISR series do not pass multicast traffic across the wireless interface.

Conditions Cisco routers that have the 802.11 b/g HWIC card do not pass

Conditions multicast traffic across the wireless interface, though multicast routing is enabled and otherwise is configured normally. Wireless hosts cannot pass multicast traffic between each other, and multicast traffic from the wired network will not be transmitted out the wireless interface.

Workaround There is no workaround.

CSCsj55923 hwic-fe silently drops input packets > 1000bytes @ >4kpps

Symptom HWIC-1FE is silently dropping ~2% input packets

Conditions HWIC-1FE in a CISCO2821 chassis running 12.4(11)XV The dropped packet are >1000b and >4kpps

Workaround There is no workaround.

Further Problem Description:

silent drops because the packets are seen by the driver (as per sh controller | i Unicast) and the software level interface (as per sh interface) does not account the same number of input packets and doesn't show any drops nor errors.

CSCsk44535 Tracebacks are seen for H323(SS)---SIP(DM) on IPIPGW2

Symptom Tracebacks are seen for H323(SS)---SIP(DM) on IPIPGW2

Conditions Traceback occurred in the following topology: Callgen1----OGW(H323 SS)-----(H323 SS)IPIPGW1(SIP DM)-----(SIP DM)IPIPGW2(H323 SS)---- (H323 SS)TGW----Callgen1

Workaround There is no workaround.

Further Problem Description:

Tracebacks are seen on IPIPGW2 If Call is made from OGW to TGW. Verified by making a call from TGW to OGW and found similar Tracebacks on IPIPGW1.

CSCsj66265 Assertion failed: at bgp_tcp_read_notify()

Symptom Router halts with an assertion error.

Conditions The failure usually occurs while closing connections.

Workaround There is no workaround.

CSCsj25356 SIP DO_EO: Memory leak in IPIP channels during stress test

CSCsk83813 sip call will pick up the wrong codec type from voice class codec

Symptom When this problem occurs, the tone remote control functionality does not work and voice becomes distorted due to the codec mismatch.

Conditions A SIP call consistently uses the incorrect codec type from the "voice class codec" configuration. It should use the value that is configured for "codec preference 1," but instead it uses the value that is configured for the "codec preference 2" setting. This issue occurs when the following configuration is used:

```
voice class codec 1
      codec preference 1 g729r8
      codec preference 2 g711ulaw

dial-peer voice 9191916 pots
 description #1/1:16#0# INUSE 163
 destination-pattern 19900001429191916
 port 1/1:16

dial-peer voice 555 voip
 rtp payload-type lmr-tone 107
 rtp payload-type nte-tone 108
 voice-class codec 1
 session protocol sipv2
 incoming called-number.
 dtmf-relay rtp-nte
 no vad

Using 2811
Cisco IOS versions: 12.4(17.4)PI1b and 12.4(17.4)PI1a
```

Workaround There is no workaround.

CSCsl12443 CME: TNP phones may experience one way audio

Symptom IP phone with FXO trunk config may experience intermittent one way audio.

Conditions Debug ephone detail will show the following error:

```
OpenReceiveChannelAck status orcError on socket
```

Workaround Reboot the phone.

CSCsk93064 Banaras-QSIG: Calls failed

CSCsl04993 uc520 devices does not get reload via SNMP

Symptom Cisco Unified Communications Series Integrated Services routers are not reloaded through SNMP.

Conditions Cisco Unified Communications Series Integrated Services routers (ISRs) are not reloaded using SNMP when you restore the device configuration. Cisco Monitor Manager sends a device-reload request to the device after configuration file is restored; however, Cisco Unified Communications 500 Series ISRs do not accept this request through SNMP.

Workaround To work around this problem, reload the device manually after restoring the configuration file.

CSCsk74181 SIP DO-DO - Basic Fax call fails

Symptom Fax call fails for a SIP DO-DO call.

Conditions When the CUBE receives a ReINVITE with fax params, it does not forward the same. Instead it sends a BYE and the call gets disconnected.

Workaround There is no workaround.

CSCsk66907 %SYS-3-CPUHOG: due to Skinny MOH Server process

Symptom CPU Hog due to Skinny MOH Server causing phones to unregister:

```
%SYS-3-CPUHOG: Task is running for (xxx)msecs, more than (xxx)msecs
(xxxxxx),process = Skinny MOH Server.
```

Conditions Occurs if Music on Hold (MOH) is being streamed from flash in IOS 12.4(11)XW3.

Workaround Use the live feed option by plugging in a CD player or iPOD or any such device to the MOH port on the UC500. Disable MOH from flash that implies tone on hold (or beep on hold).

CSCsk17498 Per Port Storm-Control is broken

CSCsk52683 System crashed when wireless client is trying to associate with AP

Symptom System crashes when there are clients trying to associate with AP

Conditions When AAA authentication fails with mis-configuration in the system or the wireless clients given wrong password to try to associate.

Workaround Make sure the AAA config is setup correctly and client password is configured correctly.

CSCsk86210 Tracebacks seen while testing After hours callblock feature

Symptom When making override after-hour call, intermittently gets traceback for buffer overflow.

CSCsk89542 CRAZYHAWK: crazyhawk_tx_start NULL/FAILED msgs with traffic stress

CSCsk82709 CABLE_MODEM_HWIC-3-FAILURE_DETECT: after CM firmware upgrade/reboot

Symptom After an upgrade of the cable modem firmware, or a reset of the cable modem daughter card, a message could be displayed about failure of cable modem card.

```
%CABLE_MODEM_HWIC-3-FAILURE_DETECT: The Cable
Modem Daughtercard has failed on interface Cable-Modem0/0/0.
```

Conditions This could happen after a cable modem firmware upgrade or reset from IOS. The message is misleading because it is not really a failure of the cable modem card but a reset.

Workaround There is no workaround.

CSCsk16153 Modem won't be disconnected on exit

Symptom Modem connection is still active on exit.

Conditions This is seen after "exiting" from the modem session.

Workaround There is no workaround.

CSCsk65748 If POE 48V fails to come up, we need to retry 3 times

CSCsk28946 CRAZYHAWK: no ip cef crashes UUT due to corrupted magic value

CSCsk54492 CRAZYHAWK:potential issue working with Detox

CSCsj66492 SPUD: cable-modem QOS not working

Symptom When a service policy is configured under the cable modem interface and matching traffic passed through it, the policy-map counters do not go up.

Conditions when a service policy is configured - something like below:

```
nterface cable-modem 0/0/0
   service-flow primary upstream
       service-policy output
and matching traffic passed, the service policy should take affect for primary service
flow packets. However, it does not.
```

Workaround There is no workaround.

CSCsk41133 TCP Interception not working on HWIC 1GE and NM-1GE interface

Additional References

Use this release note with the documents and websites in this release note and the documents listed in the following sections:

- Release-Specific Documents
- Platform-Specific Documents

Release-Specific Documents

The following documents are specific to Release 12.4 and apply to Release 12.4(15)XY.

- *Cross-Platform Release Notes for Cisco IOS Release 12.4)T*
- *Cisco IOS Software Releases 12.4 Special and Early Deployments*
- *Caveats for Cisco IOS Release 12.4(15)T*

Platform-Specific Documents

Hardware installation guides, configuration and command reference guides, and additional documents specific to the Cisco 3800 series routers are available at:

http://www.cisco.com/en/US/products/ps5855/tsd_products_support_series_home.html

Documentation Modules

Each module in the Cisco IOS documentation set consists of one or more configuration guides and one or more corresponding command references. Chapters in a configuration guide describe protocols, configuration tasks, and Cisco IOS software functionality, and contain comprehensive configuration examples. Chapters in a command reference provide complete command syntax information. Use each configuration guide with its corresponding command reference. *Cisco IOS Software Documentation* is available in html or pdf form.

Select your release and click the command references, configuration guides, or any other Cisco IOS documentation you need

Notices

See the "Notices" section in *About Cisco IOS Release Notes* located at: http://www.cisco.com/en/US/docs/ios/12_4/12_4x/12_4xy15/ReleaseNote.html.

Use this document in conjunction with the documents listed in the "Additional References" section.