Release Notes for Cisco 1800 Series Routers with Cisco IOS Release 15.0(1)XA

First Released: October 27, 2009
Last Revised: December 28, 2010
Cisco IOS Release 15.0(1)XA5
OL-20856-06 Sixth Release

These release notes describe new features and significant software components for the Cisco 1800 series routers that support Cisco IOS Release 15.0(1)XA releases. These release notes are updated as needed. Use these release notes with *About Cisco IOS Release Notes*.

For a list of the software caveats that apply to the Release 15.0(1)XA releases, see the "Caveats" section on page 8 and the online *Caveats for Cisco IOS Release 15.0M* document. The caveats document is updated for every 15.0M 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 Cisco IOS Release 15.0(1)XA5 and includes the following sections:

Memory Requirements

Table 1 lists the memory requirements for the Cisco IOS feature sets that are supported by Cisco IOS Release 15.0(1)XA on the Cisco 1800 series routers.

Table 1 Memory Requirements for the Cisco 1800 Series Routers

Platform	Image Name	Image	Flash (MB)	RAM (MB)
Cisco 1801, Cisco 1802	Cisco 180x Series IOS Advanced Enterprise Services	c180x-adventerprisek9-mz	32	128
	Cisco 180x Series IOS Advanced IP Services	c180x-advipservicesk9-mz		
	Cisco 180x Series IOS IP Broadband	c180x-broadband-mz		

Table 1 Memory Requirements for the Cisco 1800 Series Routers (continued)

Platform	Image Name	Image	Flash (MB)	RAM (MB)
Cisco 1841	Cisco 1841 IOS BB-AESK9 Feature Set Factory Upgrade For Bundles	c1841-adventerprisek9-mz	64	256
	Cisco 1841 IOS Advanced Enterprise Services			
	Cisco 1841 IOS AISK9-AESK9 Feature Set Factory Upgrade For Bundles			
	Cisco 1841 IOS ASK9-AESK9 Feature Set Factory Upgrade For Bundles			
	Cisco 1841 IOS BB-AESK9 Feature Set Factory Upgrade For Bundles			
	Cisco 1841 IOS Advanced IP Services	c1841-advipservicesk9-mz		
	Cisco 1841 IOS ASK9-AISK9 Feature Set Factory Upgrade For Bundles			
	Cisco 1841 IOS BB-AISK9 Feature Set Factory Upgrade For Bundles			
	Cisco 1841 IOS AISK9-AISK9 Feature Set Factory Upgrade For Bundles			
	Cisco 1841 IOS BB-ASK9 Feature Set Factory Upgrade For Bundles	c1841-advsecurityk9-mz		
	Cisco 1841 IOS Advanced Security			
	Cisco 1841 IOS BB-ASK9 Feature Set Factory Upgrade For Bundles			
	Cisco 1841 IOS ASK9-ASK9 Feature Set Factory Upgrade For Bundles			
	Cisco 1841 IOS Broadband	c1841-broadband-mz	64	192

Table 1 Memory Requirements for the Cisco 1800 Series Routers (continued)

Platform	Image Name	Image	Flash (MB)	RAM (MB)
Cisco 1841	Cisco 1841 IOS BB-BB Feature Set Factory Upgrade For Bundles	c1841-broadband-mz	64	192
	Cisco 1841 IOS Enterprise Base Without Crypto	c1841-entbase-mz		
	Cisco 1841 IOS Enterprise Base	c1841-entbasek9-mz		
	Cisco 1841 IOS Enterprise Services Without Crypto	c1841-entservices-mz	64	256
	Cisco 1841 IOS Enterprise Services	c1841-entservicesk9-mz		
	Cisco 1841 IOS IP Base Without Crypto	c1841-ipbase-mz	64	192
	Cisco 1841 IOS IP Base	c1841-ipbasek9-mz		
	Cisco 1841 IOS BB-SPSK9 Feature Set Factory Upgrade For Bundles	c1841-spservicesk9-mz	64	256
	Cisco 1841 IOS SP Services			
	Cisco 1841 IOS BB-SPSK9 Feature Set Factory Upgrade For Bundles			
	Cisco 1841 IOS SPSK9-SPSK9 Feature Set Factory Upgrade For Bundles			

Hardware Supported

Cisco IOS Release 15.0(1)XA supports the following routers:

- Cisco 1801
- Cisco 1802
- Cisco 1841
- Cisco 1861

For detailed descriptions of new hardware features and which features are supported on each router, see the "New and Changed Information" section on page 5. 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 1800 series routers, which are at

http://www.cisco.com/en/US/products/ps5853/tsd_products_support_series_home.html.

Determining the Software Version

To determine the version of Cisco IOS software currently running on your Cisco 1800 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

New Hardware Features in Cisco IOS Release 15.0(1)XA5

There are no new hardware features in this release.

New Software Features in Cisco IOS Release 15.0(1)XA5

There are no new software features in this release.

New Hardware Features in Cisco IOS Release 15.0(1)XA4

There are no new hardware features in this release.

New Software Features in Cisco IOS Release 15.0(1)XA4

There are no new software features in this release.

New Hardware Features in Cisco IOS Release 15.0(1)XA3

There are no new hardware features in this release.

New Software Features in Cisco IOS Release 15.0(1)XA3

There are no new software features in this release.

New Hardware Features in Cisco IOS Release 15.0(1)XA2

There are no new hardware features in this release.

New Software Features in Cisco IOS Release 15.0(1)XA2

There are no new software features in this release.

New Hardware Features in Cisco IOS Release 15.0(1)XA1

There are no new hardware features in this release.

New Software Features in Cisco IOS Release 15.0(1)XA1

BRIDGE-MIB for Layer 2 Ethernet Switching

Simple Management Network Protocol (SNMP) development and use is centered around the Management Information Base (MIB). An SNMP MIB is an abstract data base, i.e., a conceptual specification for information that a management application may read and modify in a certain form. This does not imply that the information is kept in the managed system in that same form. The SNMP agent translates between the internal data structures and formats of the managed system and the external data structures and formats defined for the MIB.

The Layer 2 Ethernet Switching Interface BRIDGE-MIB is supported in the Cisco 1861 platform from the release 15.0 (1) XA. The BRIDGE-MIB enables the user to know the Media Access Control (MAC) addresses and spanning tree information of the Ethernet switch modules. The user can query the MIB agent using the SNMP protocol and get the details of Ethernet switch modules such as MAC addresses of each interfaces and spanning protocol information.

The Bridge-MIB uses the following approaches to get the L2 layers BRIDGE-MIB information:

- Community string based approach
- Context based approach

In the community string based approach, one community string is created for each VLAN. Based on the query, the respective vlan MIB is displayed.

To get the BRIDGE-MIB details, use the **snmp-server community public RW** command in the Configuration mode.

```
Router(config)#snmp-server community public RW
```

Use the following syntax to query the SNMP BRIDGE-MIB details.

```
snmpwalk -v2c <ip address of the ISR, …>  public .1.3.6.1.2.1.17
snmpwalk -v2c <ip address of the ISR, …>  public@2 .1.3.6.1.2.1.17
snmpwalk -v2c <ip address of the ISR, …>  public@3 .1.3.6.1.2.1.17
```

Note When you create a vlan ‘x’, the logical entity public@x is added. If you query with public community, the L3 MIB is displayed. When you query with public@x, the L2 MIB for vlan ‘x’ is displayed.

In the context based approach, the SNMP context mapping commands are used to display the values for L2 interfaces information. Each VLAN is mapped to a context. When the user queries with a context, the MIB displays the data for that specific VLAN, which is mapped to the context. In this approach, each vlan is manually mapped to a context.

To get the BRIDGE-MIB details, use the following commands in the Configuration mode.

```
Router(config)#Routersnmp-server group public v2c context bridge-group
Router(config)#snmp-server community public RW
Router(config)#snmp-server community private RW
Router(config)#snmp-server context bridge-group
Router(config)#snmp mib community-map public context bridge-group
```

Use the following syntax to query the SNMP BRIDGE-MIB details.

```
snmpwalk -v2c <ip address of the ISR, …>  public@1 .1.3.6.1.2.1.17 ?L2-MIB
snmpwalk -v2c <ip address of the ISR, …>  private .1.3.6.1.2.1.17?L3-MIB
```

Note When you query with the public community, the L2 MIB is displayed. Use private group for L3 MIB.

For more details to configure and retrieve the BRIDGE-MIB details, see the Technical Notes at

http://www.cisco.com/en/US/tech/tk648/tk362/technologies_tech_note09186a0080094a9b.shtml#brgmib

New Hardware Features in Cisco IOS Release 15.0(1)XA

There are no new hardware features in this release.

New Software Features in Cisco IOS Release 15.0(1)XA

Transporting 802.1q Tags over ATM PVCs for ADSL2+

This feature allows 802.1q tags to be transported over Asynchronous Transfer Mode (ATM) permanent virtual circuits (PVC) used in ADSL2+ uplinks. This feature offers the following benefits:

- It allows Customer Premise Equipment (CPE) to carry traffic with a provider-specific 802.1q-tag.
- It supports the deployment of voice, video, and data services at customer premises. This service combination offers a real-time channel dedicated to Voice over IP (VoIP) traffic, and a second channel that delivers best-effort Internet service. In the current release, all traffic is marked with an 802.1p marking of 0, best-effort. This is implemented using VLAN-based service differentiation.

New Features in Release 15.0

For information regarding the features supported in Cisco IOS Release 15.0, see the *Release Notes* and *Feature Guides* links at

http://www.cisco.com/en/US/products/ps10591/tsd_products_support_series_home.html

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 section contains the following caveat information:

Open Caveats - Cisco IOS Release 15.0(1)XA5

There are no open caveats in this release.

Resolved Caveats - Cisco IOS Release 15.0(1)XA5

Note This will be the last rebuild of the Cisco IOS XA release. No further DDTS will be committed to this branch. The migration path for this release is 15.1T or a later release.

`CSCth03022 Crafted SIP packets may cause device to reload.`

Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software and Cisco IOS XE Software that could allow an unauthenticated, remote attacker to cause a reload of an affected device or trigger memory leaks that may result in system instabilities. Affected devices would need to be configured to process SIP messages for these vulnerabilities to be exploitable.

Cisco has released free software updates that address these vulnerabilities. There are no workarounds for devices that must run SIP; however, mitigations are available to limit exposure to the vulnerabilities.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20110928-sip.shtml.

`CSCti33534 "no ipv6 address autoconfig" may cause crash after router advert flood.`

Symptom After launching a flood of random IPv6 router advertisements when an interface is configured with "ipv6 address autoconf", removing the IPv6 configuration on the interface with "no ipv6 address autoconf" may cause a reload. Other system instabilities are also possible during and after the flood of random IPv6 router advertisements.

Conditions Cisco IOS is configured with "ipv6 address autoconf".

Workaround Not using IPv6 auto-configuration may be used as a workaround.

Note Cisco IOS checks for the hop limit field in incoming Neighbour Discovery messages and packets received with a hop limit not equal to 255 are discarded. This means that the flood of ND messages has to come from a host that is directly connected to the Cisco IOS device.

`CSCtg64478 IOS-NAT drops SIP INVITE packet.`

Symptom Router drops valid packets, causing SIP call to fail.

Conditions This is only for SIP traffic using SDP.

Workaround There is no workaround.

CSCsw64971 NAT-Entry deletion fails in SNAT backup router for H.323 RAS traffic.

Symptom NAT-Entry deletion fails in SNAT backup router for H.323 RAS traffic. We can also see crashes on the Standby router if the Active interface is brought up.

Conditions This can occur when using SNAT with HSRP and has been seen on numerous images.

Workaround There is no workaround.

CSCsx49358 Ping fails between the 6CE-6PE over the MPLS cloud.

Symptom A Cisco router may face ping failure between provider and customer networks.

Conditions This can occur on routers running Cisco IOS Release 12.4(23.15)T3.

Workaround There is no workaround.

CSCte91259 Dynamic DNS may crash router.

Symptom A Cisco router may unexpectedly reload due to a bus error after displaying an "%IDMGR-3-INVALID_ID" error.

Conditions The crash will be seen only if the router is using DHCP Client Dynamic DNS update.

Workaround There is no workaround.

CSCtg41606 RRI configuration drops egress traffic due to incomplete adjacency.

Symptom With Reverse Route Injection (RRI) configured with the **reverse-route** command, if the crypto map is applied to a multi-access interface (for example, ethernet), then egress traffic may fail when the router cannot populate an ARP entry for the crypto peer address.

Conditions The symptom could occur when the upstream device does not support proxy arping.

Workaround Use the **reverse-route remote-peer <next-hop-ip>** command instead of the **reverse-route** command.

CSCtc73759 H323 gatekeeper crashing upon receipt of specific traffic.

Symptom The H.323 gatekeeper implementation in Cisco IOS Software is crashing after receiving specific traffic.

Conditions This issue occurs after receiving specific content on the TCP/H.245 session or the H.323 gatekeeper RAS device either on Cisco IOS releases 12.4(20)T1-ES5 or 12.4(20)T4.

Workaround There is no workaround. Refer to the advisory posted at http://www.cisco.com/warp/public/707/cisco-sa-20100922-h323.shtml.

CSCtg41733 Memory Leak on SIP UDP REGISTER Call Paths During Fuzzing.

Symptom Certain crafted packets may cause a memory leak in the device in very rare circumstances.

Conditions This symptom is observed on a Cisco IOS router configured for SIP processing.

Workaround Disable SIP if it is not needed.

CSCtb73450 L2TPv3: SCCRQ packets causes tunnel to reset after digest failure.

Symptom Start-Control-Connection-Request (SCCRQ) packets may cause tunnel to reset after digest failure.

Conditions This issue is observed when the SCCRQ packets are sent with an incorrect hash.

Workaround Disable SIP if it is not needed.

CSCtg64478 IOS-NAT drops SIP INVITE packet.

Symptom Router drops valid packets, causing SIP call to fail.

Conditions This is only for SIP traffic using SDP.

Workaround There is no workaround.

CSCsd34855 VTP update with a VLAN name >100 characters causes buffer overflow.

Symptom The VTP feature in certain versions of Cisco IOS software is vulnerable to a locally exploitable buffer overflow condition and potential execution of arbitrary code. If a VTP summary advertisement is received with a Type-Length-Value (TLV) containing a VLAN name greater than 100 characters, the receiving switch will reset with an Unassigned Exception error.

Conditions The packets must be received on a trunk enabled port, with a matching domain name and a matching VTP domain password (if configured). On the September 13, 2006, The Phenoelit Group posted an advisory containing three vulnerabilities: VTP Version field DoS, Integer Wrap in VTP revision, and Buffer Overflow in VTP VLAN name. These vulnerabilities are addressed by the following Cisco IDs: CSCsd52629/CSCsd34759-VTP version field DoS, CSCse40078/CSCse47765-Integer Wrap in VTP revision, and CSCsd34855/CSCei54611-Buffer Overflow in VTP VLAN name. Cisco statement and further information are available on the Cisco public website at http://www.cisco.com/warp/public/707/cisco-sr-20060913-vtp.shtml.

Workaround There is no workaround.

CSCtf91428 NAT H.323: router crashes in IP Input [in LL_Get]

The Cisco IOS Software Network Address Translation functionality contains three denial of service (DoS) vulnerabilities. The first vulnerability is in the translation of Session Initiation Protocol (SIP) packets, the second vulnerability in the translation of H.323 packets, and the third vulnerability is in the translation of H.225.0 call signaling for H.323 packets.

Cisco has released free software updates that address these vulnerabilities.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20100922-nat.shtml.

Note: The September 22, 2010, Cisco IOS Software Security Advisory bundled publication includes six Cisco Security Advisories. Five of the advisories address vulnerabilities in Cisco IOS Software, and one advisory addresses vulnerabilities in Cisco Unified Communications Manager. Each advisory lists the releases that correct the vulnerability or vulnerabilities detailed in the advisory. The table at the following URL lists releases that correct all Cisco IOS Software vulnerabilities that have been published on September 22, 2010 or earlier:

http://www.cisco.com/warp/public/707/cisco-sa-20100922-bundle.shtml

Individual publication links are in *Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication* at the following link:

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep10.html

CSCtf17624 NAT SIP: Crash at ipnat_clear_sd

The Cisco IOS Software Network Address Translation functionality contains three denial of service (DoS) vulnerabilities. The first vulnerability is in the translation of Session Initiation Protocol (SIP) packets, the second vulnerability in the translation of H.323 packets, and the third vulnerability is in the translation of H.225.0 call signaling for H.323 packets.

Cisco has released free software updates that address these vulnerabilities.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20100922-nat.shtml.

Note: The September 22, 2010, Cisco IOS Software Security Advisory bundled publication includes six Cisco Security Advisories. Five of the advisories address vulnerabilities in Cisco IOS Software, and one advisory addresses vulnerabilities in Cisco Unified Communications Manager. Each advisory lists the releases that correct the vulnerability or vulnerabilities detailed in the advisory. The table at the following URL lists releases that correct all Cisco IOS Software vulnerabilities that have been published on September 22, 2010 or earlier:

http://www.cisco.com/warp/public/707/cisco-sa-20100922-bundle.shtml

Individual publication links are in *Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication* at the following link:

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep10.html

`CSCte14603 IGMPv3 DoS Vulnerability`

A vulnerability in the Internet Group Management Protocol (IGMP) version 3 implementation of Cisco IOS Software and Cisco IOS XE Software allows a remote unauthenticated attacker to cause a reload of an affected device. Repeated attempts to exploit this vulnerability could result in a sustained denial of service (DoS) condition. Cisco has released free software updates that address this vulnerability.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20100922-igmp.shtml.

Note: The September 22, 2010, Cisco IOS Software Security Advisory bundled publication includes six Cisco Security Advisories. Five of the advisories address vulnerabilities in Cisco IOS Software, and one advisory addresses vulnerabilities in Cisco Unified Communications Manager. Each advisory lists the releases that correct the vulnerability or vulnerabilities detailed in the advisory. The table at the following URL lists releases that correct all Cisco IOS Software vulnerabilities that have been published on September 22, 2010, or earlier:

http://www.cisco.com/warp/public/707/cisco-sa-20100922-bundle.shtml

Individual publication links are in "Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication" at the following link:

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep10.html

Open Caveats - Cisco IOS Release 15.0(1)XA4

There are no open caveats in this release.

Resolved Caveats - Cisco IOS Release 15.0(1)XA4

`CSCtd33567`

The H.323 implementation in Cisco IOS Software contains two vulnerabilities that may be exploited remotely to cause a denial of service (DoS) condition on a device that is running a vulnerable version of Cisco IOS Software.

Cisco has released free software updates that address these vulnerabilities. There are no workarounds to mitigate these vulnerabilities other than disabling H.323 on the vulnerable device.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20100922-h323.shtml.

Note: The September 22, 2010, Cisco IOS Software Security Advisory bundled publication includes six Cisco Security Advisories. Five of the advisories address vulnerabilities in Cisco IOS Software, and one advisory addresses vulnerabilities in Cisco Unified Communications Manager. Each advisory lists the releases that correct the vulnerability or vulnerabilities detailed in the advisory. The table at the following URL lists releases that correct all Cisco IOS Software vulnerabilities that have been published on September 22, 2010, or earlier:

http://www.cisco.com/warp/public/707/cisco-sa-20100922-bundle.shtml

Individual publication links are in "Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication" at the following link:

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep10.html

CSCtd86472

The Cisco IOS Software Network Address Translation functionality contains three denial of service (DoS) vulnerabilities. The first vulnerability is in the translation of Session Initiation Protocol (SIP) packets, the second vulnerability in the translation of H.323 packets and the third vulnerability is in the translation of H.225.0 call signaling for H.323 packets.

Cisco has released free software updates that address these vulnerabilities.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20100922-nat.shtml.

Note: The September 22, 2010, Cisco IOS Software Security Advisory bundled publication includes six Cisco Security Advisories. Five of the advisories address vulnerabilities in Cisco IOS Software, and one advisory addresses vulnerabilities in Cisco Unified Communications Manager. Each advisory lists the releases that correct the vulnerability or vulnerabilities detailed in the advisory. The table at the following URL lists releases that correct all Cisco IOS Software vulnerabilities that have been published on September 22, 2010, or earlier:

http://www.cisco.com/warp/public/707/cisco-sa-20100922-bundle.shtml

Individual publication links are in "Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication" at the following link:

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep10.html

CSCtf72678

Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software that could allow an unauthenticated, remote attacker to cause a reload of an affected device when SIP operation is enabled.

Cisco has released free software updates that address these vulnerabilities. There are no workarounds for devices that must run SIP; however, mitigations are available to limit exposure to the vulnerabilities.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20100922-sip.shtml.

Note: The September 22, 2010, Cisco IOS Software Security Advisory bundled publication includes six Cisco Security Advisories. Five of the advisories address vulnerabilities in Cisco IOS Software, and one advisory addresses vulnerabilities in Cisco Unified Communications Manager. Each advisory lists the releases that correct the vulnerability or vulnerabilities detailed in the advisory. The table at the following URL lists releases that correct all Cisco IOS Software vulnerabilities that have been published on September 22, 2010, or earlier:

http://www.cisco.com/warp/public/707/cisco-sa-20100922-bundle.shtml

Individual publication links are in "Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication" at the following link:

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep10.html

Cisco Unified Communications Manager (CUCM) is affected by the vulnerabilities described in this advisory. Two separate Cisco Security Advisories have been published to disclose the vulnerabilities that affect the Cisco Unified Communications Manager at the following locations:

http://www.cisco.com/warp/public/707/cisco-sa-20090826-cucm.shtml

http://www.cisco.com/warp/public/707/cisco-sa-20100922-cucmsip.shtml

`CSCtb44167 Router reloads while testing Eapfast authentication with RadiusAccountng.`

Symptom A Cisco router may reload when running EAP-FAST authentication with RADIUS Accounting.

Conditions This symptom is observed on a Cisco 1841 integrated services router that is running Cisco IOS Release 12.4T.

Workaround There is no workaround.

`CSCtf57481 FXS port controlled by STCAPP is stuck after a few calls.`

Symptom No powering ring observed for the new incoming call on STCAPP control analog phone.

Conditions Configure STCAPP control analog phone with button **C** (overlay-callwaiitng). After the STCAPP ephone park a call (FAC Park), if the XEE goes onhook before the parked call answered, there will be no power ring heard on the next incoming call to this STCAPP control analog phone.

Workaround Use button **O** (overlay) for the STCAPP ephone or shut/no-shut the STCAPP fxs port.

`CSCtg04747 Octopoda: support making an outgoing call on a queuing dn.`

Symptom Dial Via Office (DVO) failed to work using UCX-SI SDK.

Conditions When outgoing call is done using queuing-dn.

Workaround There is no workaround.

CSCtg36728 CTI makeCall request with prompt option crashes router when locale is enabled.

Symptom Router crashes or spurious memory access can be seen.

Conditions The symptom is observed if non-default locale is enabled and a UCME receives a make call request from UCXSI with the "prompt" option.

Workaround There is no workaround.

Open Caveats - Cisco IOS Release 15.0(1)XA3

There are no open caveats in this release.

Resolved Caveats - Cisco IOS Release 15.0(1)XA3

CSCtd66433 GW failed to send an UNREGISTER message.

Symptom GW failed to send REGISTER message when unconfigured from dial-peer.

Conditions GW failed to send REGISTER message when unconfigured from dial-peer

Workaround There is no workaround.

Open Caveats - Cisco IOS Release 15.0(1)XA2

There are no open caveats in this release.

Resolved Caveats - Cisco IOS Release 15.0(1)XA2

CSCta19962

The H.323 implementation in Cisco IOS Software contains two vulnerabilities that may be exploited remotely to cause a denial of service (DoS) condition on a device that is running a vulnerable version of Cisco IOS Software.

Cisco has released free software updates that address these vulnerabilities. There are no workarounds to mitigate these vulnerabilities other than disabling H.323 on the vulnerable device if H.323 is not required.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20100324-h323.shtml.

CSCtb93855

The H.323 implementation in Cisco IOS Software contains two vulnerabilities that may be exploited remotely to cause a denial of service (DoS) condition on a device that is running a vulnerable version of Cisco IOS Software.

Cisco has released free software updates that address these vulnerabilities. There are no workarounds to mitigate these vulnerabilities other than disabling H.323 on the vulnerable device if H.323 is not required.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20100324-h323.shtml

CSCte53732 UC520 ran into rommon mode and locked up the console port access.

Symptom A Cisco UC520 crashes with memory corruption and frozen console access.

Conditions This symptom is observed when upgrading from Cisco IOS Release 15.0(1) image XA to XA1 with the default configuration applied.

Workaround Power-cycle the router. This symptom will not occur after the image has been upgraded.

CSCtd17417 Router crash when configured as mobile router with IP phone attached.

Symptom Router crash when configured as mobile router with IP phone attached.

Conditions Mobile IP with IP phone attached.

Workaround There is no workaround.

CSCte08121 SRST8.0: 7937 with sccp version 17 would not register to SRST.

Symptom IP phones running firmware that uses sccp version 17 cannot register to SRST/CME-SRST or can register but will not obtain any lines.

Conditions SRST router running 15.0(1)XA. This is the first image with sccp version 17 support for SRST.

Workaround Download the IP phone firmware to a version that does not use sccp version 17.

For 79x1/5/2 phones and 7970s, this is 8.4 firmware.

For 7937 phones, get a load prior to 1.4(1).

CSCte73286 SCCP lines cannot fallback to SRST properly.

Symptom The line buttons may be missing after phone falls back to the SRST.

Conditions If there are more than 42 buttons configured on the phone, some line buttons may be missing after the phone fails over to the SRST.

Workaround Downgrade the phoneload to sccp v16 or lower.

CSCtf12048 UC560 fan broken detection for environment monitoring.

Symptom The IOS messages could be observed.

%ENVM-3-FAN_SLOW: System detected Sluggish Fan Condition.
%SMHM-2-SHUTDOWN: Shutdown service module due to a fan failed condition.

Conditions The symptom could happen under normal condition.

Workaround There is no workaround.

CSCtd66592 860 build fails with undefined reference to 'l2_bmib_add_vlan_entity_entry'.

CSCtb66273 EZVPN+DVTI: Ping through EZVPN tunnel fails with Split-tunneling.

Symptom EzVPN traffic is getting dropped at the DVTI interface on the server.

Conditions The symptom is observed with an EzVPN DVTI server configured with split tunneling.

Workaround Remove the split tunnel configuration.

CSCtd78882 Stuck port possible with trunk group with max-retry and unplugged port.

Symptom FXO ports can get stuck in offhook state.

Conditions The symptom is observed when FXO ports are members of a huntgroup where the first member port is disconnected or down. The trunkgroup has max-retry configured and rapid calls are connected and disconnected using the trunkgroup.

Workaround Unconfigure max-retry. Under each port, configure timeouts power-denial 0" so that disconnected ports are moved to offhook state and will not be hunted.

CSCte54658 CISCO-ISDN-MIB shows invalid output on Uc520.

Symptom CISCO-ISDN-MIB should be supported on UC520 from the MIB locator tool. Customer is using "demandNbrCallDetails" to monitor the status of Free BRI channels using ISDN MIB.

Conditions When trying to run an snmpwalk for an active call on UC520 on the following OIDs:

1.3.6.1.4.1.9.9.26.1.1.1.1.3 - Channel ID
Always get the output as 0.

The output is different compared to the value received from the same configuration on 2800 and 3800.

Workaround There is no workaround.

CSCtd53835 UC500 crashed after configuring SPA525 with SPA500S.

Symptom Router crashes.

Conditions When configuring SPA525 phone with SPA500S side car, followed by restart command.

Workaround Use reset instead of restart.

CSCte39270 CME does not support TsRemoteHold on sccp v16.

CSCte84849 69xx phones display toast message "From XXXX" instead of Caller ID.

Symptom 69xx phones display toast message "From : XXXX" when it receives an incoming call for 6 seconds and then it displays the caller ID of the person.

Conditions Observed for 8.5.3 and 8.5.4 phone firmwares.

Workaround Not seen for phone firmware 8.5.1.66.22.

CSCte65327 Caller ID does not work in Gilera2 image.

Symptom The Update method would have two call-info headers in certain call scenarios. This would cause the caller ID information to be "unknown" when the two headers were present.

Conditions Under certain call scenarios, the Update method would have two call-info headers, one for normal remotecc info and one for security status.

Workaround There is no workaround but it is not service effecting. Caller ID would be unavailable in certain instances.

CSCtc51573 CME GPickup/Pickup does not work with Voice Hunt-group.

Symptom CME group pickup or pickup features do not work properly.

Conditions The symptom is observed in Cisco IOS Release 12.4(24)T1 when a call is placed to the voice-hunt group.

Workaround There is no workaround.

CSCtd92892 myphoneapp of snr config should not be modified by monitor phone.

Symptom A monitor phone can change the monitored dn SNR number via myphoneapp application.

Conditions Using myphoneapp on a monitoring phone can change the SNR target of a monitored dn.

Workaround There is no workaround.

CSCtb73337 AnyConnect 2.4 does not work with IOS if cert not trusted/name mismatch.

Symptom AnyConnect Client version 2.4 does not work with IOS headend when a certificate is used that is not trusted or there is mismatch in the hostname entered in the URL to that to the CN (common name) or SAN (subject alternative name) in the IOS router certificate.

AnyConnect 2.4 fails to connect with IOS headend due certificate verify fail error.

This only pertains to the 2.4 version of AnyConnect and previous versions are not affected.

Conditions

- AnyConnect 2.4 is used.
- Untrusted router ssl certificate or CN or SAN does not match with that of the URL (fqdn) entered.

Workaround Any of the following workarounds may be used:

- Make sure that the router cert is trusted (import into cert store) and then match the CN/SAN on cert to that of the URL. If there is no DNS entry, then you can use a Local DNS entry by updating the host file for the hostname in certificate.
- Downgrade AnyConnect to a previous version 2.3.

CSCtf07474 TCP over IPsec session is failed after EZVPN session up and disconnected.

Symptom TCP sessions fail to establish between two IOS routers over an IPSEC VPN tunnel after an EZVPN client session has been established and torn down to the two routers. Logs show %FW-6-DROP_PKT: Dropping TCP session 192.168.0.0:58553 192.168.255.255:23 due to invalid segment with IP ident 35331 tcpflags 0x5010 seq.no 2978402186 ack 1370657297.

The TCP sessions could be a telnet or H.323 sessions that terminate and originate between the two routers.

Conditions

- Two IOS routers setup with IPSEC point to point VPN.
- IOS release is 15.0(1)XA or higher.
- Both routers are setup as EZVPN servers.
- An EZVPN session has been established to one of the routers and has been disconnected.

Workaround

- Always keep an EZVPN client session up to the router.
- Remove and readd "IP inspect" CLI on WAN interface after EZVPN session has been disconnected.

CSCtf26271 UC500: 525G2 does not register with CME.

Symptom SPA525G2 phone would not register.

Conditions Plug in the SPA525G2 phone to the UC500.

Workaround There is no workaround.

CSCtf40571 Missing line button when sccp version 17 phones fallback to SRST.

Symptom No line or speed dial buttons are shown on the fallback skinny phone.

Conditions Skinny phone falls back to the SRST.

Workaround Attach side cars to the phone.

Open Caveats - Cisco IOS Release 15.0(1)XA1

There are no open caveats in this release.

Resolved Caveats - Cisco IOS Release 15.0(1)XA1

CSCsv33322 remove_snmp_index_entry seen on first OIR removal in NM-1A-T3/E3.

CSCsw32679 IKE SAs between COOP KeyServers are not getting deleted

Symptom IKE does not get cleared, even if the GDOI Group is removed from the COOP Key servers.

Conditions Removed the GDOI Group from both the COOP Keyservers.

Workaround Issue **clear crypto isa**

CSCsx49309 FTP pauses 80 seconds in respond to "copy /verify ftp: flash:" op prompt.

Symptom When using the **copy ftp** command to update IOS software issued on a router, it takes approximately 80 seconds before the file transfer begins.

Conditions This is seen on a 2800 or 3800 series router, but is not seen on routers in other series, such as 2600 or 7200.

Workaround Use a different protocol to transfer the file, such as TFTP, RCP, or HTTP.

CSCsy54137 Some calls are shown active after WAN link flaps between gateway and CCM.

Symptom Some calls are shown as active after a WAN link outage between the gateway and Call Manager.

Conditions This symptom is observed if a WAN outage happens when more than 40 calls are in progress. Some random calls are then shown to be active when using the command **show call active voice compact** with Cisco IOS Release 12.4(24)T2.

Workaround There is no workaround.

CSCta11698 skinny-nat is not doing deep packet inspection after issuing the command **clear ip nat trans.**

CSCta24984 FWP - NULL should not be accepted as a name for class-maps and policy-maps.

Symptom NULL is accepted as a name for class-maps and policy-maps. No error message is displayed.

Conditions Create a class-map or policy-map with "" or " " or any other similar combination as the name.

Workaround There is no workaround.

CSCta61523 Initial code commit for SWI 501 modem support.

CSCta65909 Failed to get media source address for a stream in a DO call.

Symptom Failed to get media source address for a stream in a DO call.

Conditions Failed to get media source address for a stream in a DO call with rsvp.

Workaround There is no workaround.

CSCta69407 DSP is not told to "turn off" digits with mgcp dtmf-relay nte-gw / nte-ca.

Symptom When using mgcp dtmf-relay type nte-gw, a sniffer trace will reveal that digits are sent both in-band (within the audio stream) and out-of-band (dtmf-relay). Because of this, double digits can be seen in Unity and MeetingPlace.

Conditions GW with PRI/CAS backhaul via MGCP to CUCM and mgcp dtmf-relay configured to use nte-gw.

Workaround Use mgcp dtmf-relay type out-of-band.

CSCta79031 Pub key cache for peers is not cleared after cert map change.

Symptom If a certificate map is changed or added to the trustpoint, the pub key cache for the peers is not cleared. This makes it possible for a client which was connected in the past to reconnect again even if its certificate was banned by the certificate map.

Workaround Updated the 'Configuring Authorization and Revocation of Certificates in a PKI' module with notes to indicate that if a certificate map is changed or added to the trustpoint, the public key cache for the peers is not cleared. The link to the latest document is: http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_cfg_auth_rev_cert.html#wp1107650

CSCta81752 Keepalive does not get applied, debugs show as feature applied.

CSCta84002 Path confirmation failure while making transcoding call.

CSCta98556 Clientless WebVPN incorrectly redirected access to web portal.

Symptom Incorrect redirection is seen while using IOS WebVPN.

Conditions Only seen with IE8.

Workaround IE6 can be used as a workaround.

Further Problem Description: Customer has two server (A, B) protected behind the IOS WebVPN . Some pages on server A automatically does a silent login to server B and gets the information required to generate reports. When using IE8 this login information does not gets properly propagated to the backend server B which results in redirection request to the login page from server B.

CSCtb00695 Default shaper Bc and Be is 25ms on LE platforms.

CSCtb10100 Same bridge-group is accepted on main interface & and its lw-vlan.

CSCtb11302 Precedence Call waiting tone not generated when caller id is enabled.

CSCtb15175 8792 can only receive up to 4.5 Mbps instead of 7 Mbps.

CSCtb28877 Crashes when debug tftp packet is enabled.

Symptom Crash occurs on router configured as tftp-server when IPV6 addresses are used for tftp copy and tftp packet/event debugs have been enabled on the server router.

Conditions

- A router is configured as tftp server and IPV6 addresses are configured on both the server and client interfaces and the IPV6 addresses are used for the tftp copy.
- **debug tftp packets/events** is configured on the tftp server router.

Unconfigure **debug tftp packets/events.**

CSCtb34358 IP tunnel source interfaces are mixed up after reload.

Symptom Tunnel sources get mixed up when tunnel interfaces are configured with serial subinterfaces as sources and the router is reloaded.

Conditions The symptom occurs only after a reload or when a saved configuration is applied to the running configuration.

Workaround There is no workaround.

CSCtb39686 Caller ID check failed after Call Blast scenario.

Symptom Wrong Caller ID is displayed after Call Blast done.

Conditions Phone A does a call blast by calling pilot number xxxxx. All the phones start ringing till time out 60 seconds then call lands on the final phone B. Phone B answers the call and gets connected, then it checks for called number at Phone A. The final phone's number should be displayed. But the pilot number is displayed.

Workaround There is no workaround.

CSCtb40985 IP SLA memory leak with invalid source address.

Symptom The memory occupied by the IP SLAs Sync Pro may gradually increase.

Conditions The issue occurs when ICMP path jitter operation is configured on the router with invalid source address. Platform is sup720-3B with 12.2(33)SXI1 image.

Workaround Configure the SLA operation with the right source address.

CSCtb42748 No ringback on Incoming SIP to AA to SNR line with different codecs.

Symptom No ringback on Incoming SIP to AA to SNR line with different codecs.

Conditions

- The incoming call is from SIP trunk.
- The outgoing call to mobile has different codec than the incoming call leg.
- The mobile phone on the sip trunk needs to send back the 183 progress message while rining.
- User is not able to hear the ringback tone after ringing the moblie phone.

Workaround There is no workaround.

CSCtb43226 12.4 IOS MGCP generates 510 remote description error.

Symptom Voice call is rejected, because gateway replies 510 error for MDCX message.

Conditions Interworking with 3rd party IAD device, which doesn't support NSE codec, will mess up SDP format.

Workaround Disable t38 and modem passthrough, so gateway doesn't generate NSE in SDP.

CSCtb44681 Fix static_route single source diffs between eagle_cnh and mcp_dev.

CSCtb46181 Incorrect updation of Winscale options.

Symptom Application set window scale factor does not get used by the accepted connection, instead the scale factor set by the global command **ip tcp window XXXX** is used.

Conditions **ip tcp window XXXX** configured to a higher than 65535 value. Connection has window scale enabled on both sides.

Workaround There is no workaround.

CSCtb47950 I/O memory depleted after 20 minutes of CME SIP TRUNK calls.

Conditions The router runs into low-mem condition due to mem-fragmentation in certain voip-perf testing. It has a known work-around and is not a problem as such unless similar level of bursty traffic with the peculiar size of request is generated (as used in testing).

CSCtb48731 Port MEP remains inactive after interface is no shut from shut.

CSCtb48984 Adjust webvpn.html page and add support for iphone and ipod.

Symptom SSLVPN Login Page is not properly displayed on mobile devices. Also, there is no support for iPhone and iPod safari browsers.

Conditions The symptom is observed on an access page using Windows Mobile, or on an iPhone or iPod.

Workaround Page is displayed but quality is poor.

CSCtb49885 Caller ID check failed for Call Foward with supp.services disabled.

Symptom The called name is not displayed on the caller sccp phone when the call is forwarded to non-sccp endpoint (ie. sip trunk or sip phone). The called number is displayed correctly.

Workaround There is no workaround.

CSCtb51993 NAS got crashed while establishing pppoe session @ tw_timer_stop.

Symptom A router crashes upon bringing up PPPoE sessions.

Conditions The symptom is observed when AAA proposes a pool name but the pool is not defined on the NAS as well as the radius.

Workaround Define the pool on the NAS or as a dynamic pool on the radius.

CSCtb56878 Memory Leak at dom_data_strdup.

Symptom When we load an FPM tcdf file on the router, a memory leak is seen. However, this is a one time operation and has minimal impact.

Conditions Whenever we load an FPM tcdf file, the XML parser parses the file which causes a memory leak. This happens in all the advanced images where FPM is used. This memory leak is not seen until we load a tcdf file. This issue is specific to the PI11 codebase.

Workaround There is no workaround.

CSCtb57404 SNR Module sets wrong leg mode for SIP-SIP Call.

Symptom When using the UCME Single Number Reach feature, it is not possible to hold/resume a call from the mobile device once the SNR ephone has entered auto-hold state.

Conditions

- Phone A calls SNR phone B
- SNR mobile phone C rings after timeout timer pops
- Answer the call from phone C
- SNR phone B will be in auto-hold after delay timer pops
- Press hold on phone C and it will not be possible to hold/resume the call

Workaround There is no workaround.

CSCtb59171 BGP IPv6 is not working with ipbasek9.

Symptom IPv6 BGP does not work with ipbasek9.

Conditions ipbasek9 is the only package enabled.

Workaround There is no workaround.

CSCtb60300 Router crash @ ipnat_sbc_add_static_cfg.

Symptom Router crashes when SBC proxy address is configured if the address is IPADDR_ZERO.

Conditions Only for SBC proxy address configuration and only if either of the addresses is zero.

Workaround There is no workaround.

CSCtb66305 shared-dn ephone unregister affects another ephone BLF subsciption.

Symptom cme on c3825-advipservicesk9-mz.124-24.T1.bin.

Conditions When one ephone runs UNREGISTER_ABNORMAL, the other ephone with shared DN will stop sending BLF presence subscription. For example:

```
ephone 34 button 1:5 2:4
ephone 61 blf-speed-dial 1 ... button 1:5 2:4
```

When ephone 34 unregisters, ephone 61 stops sending presence subscription.

Workaround There is no workaround.

CSCtb67831 Typo error "numberic" found in the command forward-to-voicemail.

CSCtb70102 Wrong application is invoked by the SRST gateway for calling from stcapp phone.

Symptom When SRST and STCAPP are configured and running on the same router, SCCCP-controlled analog phones may be unable to make an outgoing call.

Conditions This symptom is observed when, upon WAN link failure, the phones register to an SRST gateway.

Workaround There is no workaround.

Further Problem Description: This symptom occurs due to STCAPP automatically adding a *station-id* parameter under the **voice-port** command in order to save DN information for registration to SRST.

CSCtb71835 Queue-limit configured in ms is not shown.

Symptom Queue-limit configured in ms is not displayed in **show policy-map int** output.

Conditions This happens in a scenario where queue-limit is configured in ms in class-default.

Workaround There is no workaround.

CSCtb71889 DNS query response is dropped on a NAT-PT router.

Symptom DNS A answers from IPv4 DNS server (which is supposed to be forwarded to IPv6 side as AAAA-answer) is dropped on NAT-PT routers.

Conditions This symptom is observed when DNS NAT-ALG is enabled.

Workaround There is no workaround.

CSCtb73115 Memory chunk leaked at NAT String Chu while configuring ip nat pool.

Symptom Chunk memory leaked while configuring the ip nat pool.

Conditions While configuring the pool with subnet mask smaller than required length for the start and end ip address.

Workaround There is no workaround.

CSCtb73219 Unable to clear the arp sub-interface entry.

CSCtb73967 Router crashed while doing udp-echo operation in ip sla.

Symptom Using the command **default dest-ipaddr** for udp-echo, udp-jitter, and tcp-connect causes a device to crash.

Conditions The symptom is observed with the command **default dest-ipaddr**.

Workaround Do not use the command **default dest-ipaddr**. This sets the address to 0.0.0.0, which is not valid.

CSCtb74251 On hook dialing did not work on 7911 SCCP phone.

Symptom

- Shutdown cucm service.SCCP Phone 7911 registered with SRST
- Keep the phone on hook
- Press "New Call" softkey, nothing happens.

CSCtb88409 Router crashes when configuring object id under config-event-objlist.

Symptom A Cisco router may crash when configuring the object id in config-event-objlist subconfiguration mode.

Conditions This symptom is observed when entering the **cns config notify** command.

Workaround There is no workaround.

CSCtc14760 Router reloads during stress test.

CSCtc16399 NIOS watchdog timeout after power cycle MC5727 modem.

Symptom NIOS watchdog timer times out.

Conditions This symptom is observed when an MC5727 modem is power-cycled.

Workaround Reload the router.

CSCtc30869 L2 STP MIB and VlanMem MIB support for 1861 platform.

CSCtc52622 shdsl and cellular may overwrite cdb queue entries on fxd.

CSCtc52748 queueing-dn cannot be configured as a member of ephone hunt group

CSCtc53062 blf is not blocked if DND is set using CSTA message setDND.

Symptom Application sends CSTA setDND message to CME, CME does not update/block the blf monitor sessions.

Conditions Happens when the DND is set from CSTA message.

Workaround Once the phone state changes, it will reflect the real state to the blf sessions.

CSCtc75277 Call Transfer + Call Forward Scenario not working.

Symptom The CME does not process the incoming sip 302 message.

Conditions Call forward scenario where incoming sip 302 messsage is received.

Workaround Configure : voice service voip no notify redirect ip2ip.

CSCtc78721 Support Bridge-MIB and VLAN-Membership-MIB for 880&890 platforms.

CSCtc86342 IOS GW shows invalid syntax error for INVITE with multiple VIA headers.

Symptom Inbound SIP calls on IOS SIP GW / CME fails with 500 Internal Server Error.

Conditions Inbound SIP INVITE has multiple VIA headers. Voice source group is configured on IOS SIP GW/CME with access-list. The IOS version is 15.0(1)XA or 12.4(24)SB.

Workaround Use earlier IOS such as 12.4(20)T2. Remove voice source-group configuration

CSCtd07228 CME ephone call flows broken with Abacus SCCP version 4.

CSCtd11131 Fix compilation errors for the unix simulator in t_base_1.

CSCtd21596 Forbidden Header 'Call-Info' found in ACK.

Symptom The ACK to 200 OK packet sent by the CME (configured with firewall) contains 'Call-Info' Header, which is a forbidden header field when 15.1(0.2)PI12e is loaded on the CME.

Conditions Happens when the CME is loaded with 15.1(0.2)PI12e.

Workaround Call will flow through. Only if firewall is enabled, the ACK packets with Call-Info header will be dropped.

`CSCtd23424 Add specific vendorCon to support trunk dn monitor and m button.`

Symptom User can not press the button configured as trunk-dn monitor to pick up the parked call. Or user cannot press the button configured as M button to speed-dial.

Conditions Pressing the monitor button, no OP.

Workaround There is no workaround.

`CSCtd26113 Unable to configure` **`call-forward system redirecting-expanded`**`.`

Symptom Not able to configure **call-forward system redirecting-expanded**.

Conditions Not able to configure **call-forward system redirecting-expanded** on a 2800 router.

Workaround There is no workaround.

`CSCtd26844 Cisco 500 phone registration fails when ephone tag is 56 or greater.`

Symptom After a license upgrade from 48 to 64 user license on a UC520, the Cisco 500 series phone registration fails with the following errors in debug ephone register output:

```
Error: Device Id 80000 Configured Device Id -1 StationSPCPRegisterTokenReject sent
on socket 4
```

Conditions Problem is seen when registering any 500 series phone to a CME on UC520 platforms. The problem only occurs when the ephone tag value for this phone registration is 56 or higher.

Workaround Use an ephone tag that is of lower numerical value. Ephone 55 or lower will work.

`CSCtd42552 When CME fails to respond to "newcall", STCAPP hangs.`

Symptom When shared line has 2 calls, and these 2 calls disconnect at the same time, the port might hang.

Workaround There is no workaround.

CSCtd47693 Add support for SPCPPlatformInfoGet msg handling (requested by UCC.

CSCtd53835 UC500 crashed after configuring SPA525 with SPA500S.

CSCtd66592 860 build fails with undefined ref. to 'l2_bmib_add_vlan_entity_entry'.

Symptom Build failure is happening for 860 platform images.

CSCtd78882 Stuck port possible with trunk group with max-retry and unplugged port.

Symptom FXO ports can get stuck in offhook state.

Conditions FXO ports are members of a huntgroup where the first member port is disconnected or down. The trunkgroup has **max-retry** configured and rapid calls are connected and disconnected using the trunkgroup.

Unconfigure **max-retry**. Under each port, configure "timeouts power-denial 0" so that disconnected ports are moved to offhook state and will not be hunted.

Open Caveats - Cisco IOS Release 15.0(1)XA

There are no open cavetas in this release.

Resolved Caveats - Cisco IOS Release 15.0(1)XA

CSCsj16203 CPU profiling may not be reliable in c800 during nested interrupt.

Symptom CPU profiling under interrupts is not reliable.

Conditions Symptom is present on all PowerQUICC platforms (Cisco 800, 1700, and 2600 Series Routers).

Workaround There is no workaround.

CSCso05336 Crash due to corrupted magic value in in-use chunk when accessing irc.

Symptom A Cisco 1811 router reloads when trying to connect to irc.freenode.net during the first 36 hours following a reload.

Conditions The symptom is observed only in the first 36 hours following a reload.

Workaround Do not connect to irc.freenode.net in the first 36 hours following a reload.

CSCsr09625 missing voice dsp crash-dump.

Symptom The **voice dsp crash-dump** CLI is missing on all platforms except AS5400.

Conditions This happens when the CLI's parser chain was moved, hence missing them on the platforms. Need to ensure the parser chain is implemented as platform independent.

Workaround There is no workaround.

CSCsr81161 sip consult xfer results in 1-way audio with supp service refer disabled.

Symptom Consult transfer with third party sip endpoints results in one way audio when the third party endpoint has delayed response to resume request which includes change in rtp stream parameters (i.e. port number).

Conditions sip supplementary services refer is disabled.

Workaround There is no workaround.

CSCsv01339 Unable to ping some devices on subnet.

CSCsv20058 Duplicate H245-alphanumeric at digit_end on rfc2833 to h245-alpha.

Symptom Upon digit_end on the RFC-2833 side, the IPIP GW misinterprets this and sends out h245-alphanumeric, which is duplicate. Typically, the IPIP GW should ignore all the tone packets after the digit_begin is detected until the digit_end.

Conditions RTP-NTE to H245-Alphanumeric conversion is triggering this event.

Workaround There is no workaround.

CSCsw49855 Ping stops working during speed/duplex testing.

Symptom IP connectivity fails for the interface following extended pings from FastEthernet interface. The **show interface** command will indicate that the output queue is wedged:

```
Output queue: 40/40 (size/max)
```

No more packets are switched out of the interface until the interface is cleared with the **clear interface fast<#>** command.

Conditions This is seen on a Cisco 881 running IOS versions 12.4(20)T1 and T2. No indication at this time that this is specific to these images. The problem is observed when the FastEthernet interface in question is set to 10/half or 100/half.

Workaround Once the problem has occurred, clear the interface with the command **clear interface fast<#>**. This problem has not yet been seen on an interface in full duplex mode.

CSCsx20984 Router reloads with bus error and no stack trace.

Symptom Router reloads with a bus error and no tracebacks.

Workaround There is no workaround.

CSCsx30643 TDM ERL always reports +6.0 dB for VWIC2 T1/E1 voice-ports using HWECAN.

Symptom When querying for low-level DSP statistics for an active voice call the TDM ERL level reported is always identically +6.0 dB and never fluctuates:

Conditions This behavior is observed on Cisco IOS Voice GateWays installed with digital voice-ports configured on the VWIC2-1MFT-T1/E1 or VWIC2-2MFT-T1/E1 cards, and enabled with the EC-MFT-32 or EC-MFT-64 HardWare Echo CANcellation (HWECAN) daughter cards. The installed IOS version is any 12.4 or 12.4T release which supports the VWIC2 and EC-MFT hardware.

Workaround There is no known workaround available. If real-time visibility into the measured TDM ERL is desired, it is necessary to configure the digital voice-ports to use the SoftWare ECAN (SWECAN) by setting **echo-cancel enable type software**. A **shutdown/no shutdown** of the voice-ports is recommended to ensure the new setting takes effect.

CSCsx49309 FTP pauses 80 seconds in response to **copy /verify ftp: flash:** op prompt.

Symptom When using the **copy ftp://** command to update IOS software issued on a router, it is seen that it takes approximately 80 seconds before the file transfer begins.

Conditions This is seen on a 2800 or 3800 series router, but is not seen on routers in other series, such as 2600 or 7200.

Workaround Use a different protocol to transfer the file, such as TFTP, RCP, or HTTP.

CSCsx67255 ISDN call failure with cause 47 after DSP allocation failure on channel.

Symptom An outgoing call from an IP phone to PSTN through ISDN PRI fails on a channel due to a DSP allocation failure (not enough DSPs to support the call). Subsequent calls through that same channel continue to fail with "resource unavailable" cause value equal to 47 even after DSP resources have been made available to handle the call.

Conditions The symptom occurs on a router running Cisco IOS Release 12.4(15)T8 or higher. The call must first fail with a legitimate DSP allocation error. Any call made through the same channel as the failed call will also fail.

DSP allocation failures on gateway can be checked through the use of the exec command **show voice dsp group all**. The last line of the show command output includes a counter for "DSP resource allocation failure".

This issue can also be seen in some cases upon bootup. When a gateway is reloaded, system resources will come up with a slightly different timing. If, for example, a PRI interface comes up before the DSP resources have fully initialized, there may be a similar failure.

Workaround The workarounds are as follows:

- Reload the router to clear the channel. If a reload cannot be done, busy out the channel with the failed calls using the **isdn busy b_channel** command under the serial interface.
- If the issue is due to oversubscription of the DSP resources, change the configuration to meet the DSP resources available on the gateway. Further information can be found with the DSP Calculator at http://www.cisco.com/cgi-bin/Support/DSP/cisco_prodsel.pl.
- If the issue is related to timing issues upon reload, shutdown the voice-port in question before reloading the gateway. When the gateway comes back up, take the voice-port out of shutdown.

CSCsx75353 High CPU Utilization seen on 2821 after upgrade to 12.4(15)T5.

Symptom High CPU usage is observed on a Cisco 2821 router. An increase of almost 10 percent in CPU utilization is observed with every voice call.

Conditions This symptom is observed when an AIM compression card is present on the motherboard (specifically AIM-COMPR2-V2).

Workaround Remove the AIM compression card from the motherboard.

CSCsy05003 Oneway audio with MTP on cube and **progress_ind alert enable 8** configured.

Symptom CUCM --[h323]-- CUBE --[SIP]-- SIP provider

Outbound calls to the SIP provider have one-way audio. The internal IP phone can hear the remote party, but the remote party cannot hear the internal IP phone.

Conditions Fast start and MTP required is configured for the H323 gateway in CUCM -IOS hardware or software MTP is used on CUBE, **progress_ind alert enable 8** is configured on the outgoing SIP dial-peer on CUBE.

Workaround Remove **progress_ind alert enable 8** on the outgoing SIP dial-peer. Use CUCM SW MTP or any MTP that is not co-located on CUBE

`CSCsy18996 TNP phones displaying "Acct" instead of "Transfer recall" in 12.4(24)T.`

Symptom After a transfer recall, phones registered to CME will display "Acct" instead of "Transfer recall".

Conditions TNP phones with firmware 8.4.2 or 8.4.3.

Workaround There is no workaround.

`CSCsy20149 Voice-port goes to transient unregister under SRST mode.`

Symptom STCAPP voice-port becomes transiently unregistered for approximately one minute in SRST mode.

Conditions Some STCAPP voice-port is pending to switchover to SRST while active, and then when that port goes on hook and starts to switchover to SRST, the timing triggers the transiently unregistered issue on a certain port.

Workaround Wait for about a minute, and the port will automatically recover back to registered.

`CSCsy24266 SIP overrides diversion header from APP RDN number from OR to LRD.`

Symptom A call from a night hunt forwarded to BACD dial by an extension to an ephone (call forwarding no answer) to voicemail goes to the night hunt number and not the last redirected number.

Conditions The symptom is observed with Cisco IOS Release 12.4(22)T.

Workaround There is no workaround.

CSCsy31552 ADSL WIC/ATM interface stops forwarding traffic & reports output drops.

Symptom A Cisco 1841 router equipped with xDSL WIC will suddenly stop forwarding packets. The packets will appear as output drops on the ATM interface statistics. Under the PVC level, there are no drops. The DSL line is not flapping but the ATM interface(s) report output drops.

Conditions The symptom is observed when using a Cisco 1800 and 2800 series router equipped with the same ADSL-WIC module. The ATM interface(s) need to be bridge-group configured. The bridge-group is in forwarding mode.

Workaround Reload the router.

CSCsy32246 Call waiting tone not heard when caller-id is enabled for sip dsapp fxs.

Symptom The call-waiting tone will not be generated and the caller ID will not be displayed for the second call to a phone connected to a FXS port.

Conditions SIP Server -[sip]- Gateway (fxs) -- Analog phone

This is seen to occur when the Device Service Application (DSAPP) is enabled on the gateway to provide supplementary features for the phone connected to the FXS port using SIP. Configuring either **caller-id enable** or **caller-id enable type 2** on the FXS voice port will trigger this issue.

Workaround Configuring **caller-id enable type 1** under the voice port will provide call-waiting tone. However, caller-id will not be provided for the second call.

CSCsy37164 WINKUP minimum timer fails to expire on c3800 platforms on outbound calls.

Symptom A c3800 platform may intermittently fail to expire the CAS WINKUP minimum timer. This timer dictates how long a T1 CAS, wink-start endpoint must remain offhook before completing a wink. Failure to expire the timer will cause the c3800 to incorrectly classify a valid wink as invalid, failing outbound calls.

Conditions This can happen when there is a brief period of increased CPU usage while a call is in the process of connecting. In other words, a small spike in CPU usage can cause the time to fail to expire, thereby causing a wink failure.

Workaround Disable any periodic processes which may cause momentary spikes in CPU usage, such as SNMP polling, EEM scripts, or other automated processes. This may or may not help depending on the cause of the CPU spikes.

CSCsy61980 Problem with call list on CME.

Symptom Phone A (xxx) calls Phone B (yyy), Phone C (zzz) picks up the call through call pickup. A two way conversation is then established between Phone A (xxx) and Phone C (zzz). Then the call is disconnected.

When Phone A is checked, in Placed Calls, there is "Phone C yyy" instead of "Phone B yyy".

Conditions It happens with IP phones 7942/61/62 and latest version of firmwares 8.4.1-8.4.3. With 8.3.4 version of firmware, there is no issue. Also, there is no issue with latest version of firmware if the phones are registered to CME instead of Cisco Unified CM.

Workaround There is no workaround.

CSCsy88059 Second call gets dropped when the first call is put on hold.

Symptom Calls drop when answering the second call on Octo lines with the ‘Hold’ softkey.

Conditions If the calls come in a PRI or FXO interface, and a user on an active call on the octoline puts the call on hold while there is an incoming call, it will automatically answer the incoming call. Approximately 13 seconds later the second call is dropped.

Workaround When the second call comes in, use the ‘Answer’ softkey instead of putting the first call on hold. If the user requires to put a call on hold while a new call is coming in, they must wait until the incoming call stops ringing.

CSCsz00326 Memory fragmentation on VXML gateway.

Symptom Memory fragmentation, no call accepted, no output for **show run.**

Workaround Reload the router.

CSCsz03260 Unexpected callflow may cause exception on IOS H320 Gateway.

Symptom A gateway may take an exception when receiving an inbound H320 call when the call is placed via ISDN overlap sending.

Conditions The symptom is observed with Cisco IOS Release 12.4(22)T1.

Workaround There is no workaround.

CSCsz14947 12.4(20)T2 doesn't process SIP "REPLACES" header properly.

Symptom 12.4(20)T2 ignores SIP "REPLACES" header in mid-call INVITE from proxy and processes/routes call as if it were a new INVITE.

Conditions Call Resume performed on SIP side, proxy sends mid-call INVITE with REPLACES header to ISR running 12.4(20)T2.

Workaround There is no workaround.

CSCsz17030 Failure on 12.4(22)T, video port negotiated as port 0.

Symptom A video call for a 3G H.324 call fails to properly negotiate media.

Conditions In debug ccsip all debugs, this message can be seen:
/SIP/Info/sipSPIUpdateSrcSdpVariablePartVideo: Unsupported Video m-line: Setting stream 2 portnum to zero

Also, in the media sent to the endpoint, the video port is set to 0 as the debug state.

Workaround There is no workaround.

CSCsz23481 **dsp allocation signaling dspid** command not available on 2801.

Symptom The **dsp allocation signaling dspid** command under voice-card on 2801 platform is not available.

Conditions This issue is on 2801 platform alone.

Workaround There is no workaround.

CSCsz23528 IO MEM autosizing must take Dovetail increased IOMEM usage into account.

Symptom After upgrading to 12.4(24)T images or newer, the amount of free IO MEM reported by **show memory** command output is much lower (4MB less) than with previous versions. The amount of IO MEM allocated upon boot up of the router has not changed with respect to previous versions.

This change in memory consumption is expected due to the integration of new features.

Conditions This defect is seen on 12.4(24)T on ISR platforms (28xx, 38xx series).

Workaround The amount of IO MEM can be increased manually by performing the following in configuration mode:

```
router(config)# memory-size io <5-50> percentage of DRAM to use for I/O memory: 5,
10, 15, 20, 25, 30, 40, 50
```

For most configurations, 5% should be enough.

`CSCsz27002 OnHookMessage is not handled with the specified line and ref.`

Symptom Call is terminated after aborting the transfer attempt.

Conditions This problem is observed if **transfer-digit-collect** is not configured or configured as **new**, the default.

Workaround Configure **transfer-digit-collect orig**.

`CSCsz30353 Interrupt error occurred when IPSEC connection is up.`

Symptom `%GT64010-3-DMA: Interrupt error` observed when IPSEC connection is up on DMVPN spoke.

Conditions c2431 platform with HW crypto engine.

Workaround There is no workaround.

`CSCsz34920 NME-502 causing router to reboot.`

Symptom Router continuously reboots.

Conditions This symptom is observed when an NME-502 is installed on the router.

Workaround Replace or remove the NME-502.

`CSCsz35376 NM-2W VWIC2 reports multiple master clocks driving NM-2W PLL.`

Symptom The command **show controllers t1** on a 3845/2xNM-2W/4 x VWIC2-2MFT-T1/E1 combo may report clock sources driving the NM-2W's PLL are different from the clock sources being reported from the NM-2W FPGA LCS register.

Conditions Observed on 3845/2xNM-2W/4 x VWIC2-2MFT-T1/E1 combo running 124-19b, 124-24.6b, and 124-24.6.T with NM-2W populated with 2 x VWIC2-2MFT-T1/E1 with all 4 DS1s defaulting to **clock source line** and the NM-2W not participating in the system backplane clock.

Workaround Configure **clock source line independent** on all 4 DS1s.

CSCsz45855 Cisco Unified Border Element not responding to reINVITES received while call transfer is in progress.

Symptom Cisco Unified Border Element ignores reINVITEs from Cisco Customer Voice Portal (CVP).

Conditions While call transfer is in progress and Cisco Unified Border Element is waiting for NOTIFY (with 200 or any final response code), after receiving NOTIFY (with 100), it receives INVITE.

Workaround There is no workaround.

CSCsz45898 SIP Cisco Unified Border Element does not forward 200ok for session refresh.

Symptom SIP Provider -[sip]- CUBE -[sip]- CUCM

CiscoUnified Border Element does not respond to the second reINVITE to refresh the session causing the session refresher to timeout and drop the call.

Conditions Media flow around configured on CUBE, CUBE running any IOS beginning with 12.4(22)T - INVITE method to refresh the session.

Workaround Configure media flow through on CUBE. If that's not an option, downgrade to any IOS before 12.4(22)T when media flow around is configured. E.g. 12.4(20)T, 12.4(15)T, etc.

CSCsz51722 SIP profile rules are not getting applied on OOD OPTIONS message.

Symptom SIP profile rules are not getting applied on OOD OPTIONS message irrespective of SIP profile being applied globally or at dial-peer level.

Conditions This issue is seen on Cisco UBE.

Workaround There is no workaround.

CSCsz52576 vlan.dat file lost after second power cycle - VTP Domain Name disappears.

Symptom The vlan.dat file gets deleted after the second reload of the router, and the VLAN definition and names are lost (not the interfaces and IP addresses). It has been observed that when the vlan.dat is lost, in **sh vtp status**, the VTP Domain Name is blank (and was properly configured before).

Conditions This behavior is observed in a Cisco 3270 router that is running Cisco IOS Release 12.4(24)T. It is also observed with Cisco 1800 ISR with switch modules in Cisco IOS Release 12.4(22)T.

Workaround There is no workaround. Customer needs to reconfigure them again after reboot. This problem is not observed in Cisco IOS Release 12.4(15)T.

Further Problem Description: When a customer is running an image that does not store the VTP and VLAN information in the start-up configuration or the normal output of show running-config, the vlan.dat file gets overridden to the default vlan.dat approximately 2 minutes after reboot. The current VLANs and VTP information remains operational until the router is rebooted.

A reboot causes the VLANs and VTP information to disappear because the start-up configuration does not contain any VLAN or VTP information, nor does the vlan.dat file in flash.

The operating VTP information appears in the output of show running-config all (which shows non-default and default values), indicating that the router considers the VTP information to be at default values even when there is a VTP domain name configured. This allows the VLANs and VTP to remain operational until the router is rebooted.

`CSCsz54468 Crashinfo caused by MRCP CLI command, the version is MRCPv2.`

Symptom Crashinfo on VXML Gateway.

Conditions Running **show mrcp client session active detail** or **show mrcp client session active** and using MRCP v2.

Workaround Do not run these commands.

`CSCsz55969 HWIC-1DSU-T1 module does not show the 15 min performance statistics.`

Symptom HWIC-1DSU-T1 does not show the 15 min performance statistics.

Conditions The problem is specific to HWIC-1DSU-T1. WIC-1DSU-T1-V2 on the same box is not affected

Workaround There is no workaround.

`CSCsz65335 RTSP not releasing socket when socket connect attempt fails.`

Symptom VXML gateway is unable to open an RTSP connection to media server after media server is taken down and then brought back up.

Conditions The problem is observed when the media server is no longer reachable from the VXML gateway. When this occurs the VXML gateway attempts to open an RTSP socket connection to the media server. The socket connection attempt is not successful but the VXML gateway does not release the socket. With each connection attempt the socket is incremented until the max of 2047 is reached. Once the max is reached, the VXML gateway will no longer attempt to open a socket to the media server until a reload occurs.

Workaround Reload the VXML gateway.

CSCsz72535 Memory leak during IZCT testing - mem leak in gk_circuit_info_do_in_acf().

Symptom While conducting a stress test with 13500 endpoint and calls between 1000 to 2000 during 17 hours, the test memory utilization was growing to 24%. After the test, the memory fallback is 20%, it does not revert to 4%.

Workaround There is no workaround.

CSCsz74629 Delay in propagation of interface link down state.

Symptom There is a delay in the propagation of interface link down state. Link failure is detected with a huge delay once the other end of the link gets disconnected.

Conditions This symptom is observed on a Cisco 1861 router that is running Cisco IOS Release 12.4(24)T.

Workaround The default keepalive period is 10 seconds and the periodic function which updates the link state change runs on the order of keepalive time, hence it takes long time to detect the link down state. If keepalive is set to 1 or 2 seconds, the time taken to detect link down is normal.

CSCsz84392 UC500 does not report FRU information for certain VIC modules.

Symptom When certain VIC modules are installed in a UC500, the UC500 will not correctly report the Product (FRU) Number in the **show diag** output. If the UC500 is being managed using the command line, this problem is cosmetic in nature, but if it is being managed by CCA, then the VIC module will not be detected.

Conditions So far, the problem has been observed with older VIC2-2BRI-NT/TE modules, with newer versions being apparently unaffected. However, it is possible the problem may be present on other VIC modules as well. All versions of UC500 software are affected.

Workaround The problem may be able to be worked around in some cases by replacing the VIC module with a more recently manufactured unit.

CSCsz88671 Onhook GPickup * doesn't work.

Symptom If GPickup and '*' is pressed when the phone is on hook, the GPickup won't pickup the ringing call from the pickup-group to which the seized DN belongs. The seized DN depends on how the auto-line is configured on the phone.

Conditions This problem only occurs if the onhook phone sends the StationKeypadButtonMessage for the '*'.

Workaround Go offhook before pressing GPickup and enter '*' or enter "*#" to work around the problem.

CSCsz92704 Voice GWs not supporting DSPfarm services should provide warning message.

Symptom IOS Voice GateWay (VGW) platform families like the IAD2430, VG224, VG202, and VG204 are fixed form-factor VGWs which have C5510 DSPs soldered onto the mainboard. As such they are not expandable to install extra DSP resources and are meant primarily as TDM-IP devices. Nonetheless in most IOS releases it is possible to configure **dsp services dspfarm** under the **voice-card 0** CLI in the running-config as well as to set **dspfarm profile N <conference|transcode>** even though transcoding and conferencing services are not supported on these platforms. There aren't enough DSPs available to make these DSP services viable in addition to accommodating regular TDM-IP VoIP calls. Attempts at sustaining a conference or transcoding call fail, users get confused and open up TAC Service Requests.

Conditions This behavior is observed on fixed form-factor IOS Voice GateWay platform families like the Cisco IAD2430, VG224, VG202, and VG204, installed with any release of IOS.

Workaround Not applicable. DSP transcoding and conferencing features are not supported on the aforementioned VGW platforms.

CSCsz96106 Unable to configure ds1 option on snmp-server host - Ambiguous command.

Symptom Unable to configure ds1 option on snmp-server host command, ambiguous command error.

Example:

```
Router(config)#snmp-server host 10.10.10.10 tests ds1 % Ambiguous command: "snmp-server
host 10.10.10.10 tests ds1"
```

Conditions 1841 router running 12.4(24)T but probably affects all other platforms and previous versions.

Workaround There is no workaround.

CSCta02224 Calls on FXO port disconnect after hold and resumed via line button.

Symptom A call is placed on hold from an IP phone. If the user resumes the call by lifting the handset, and then pressing the line button, the call will disconnect within 60 seconds. The precise time that it takes for the call to disconnect may vary (5-60 seconds).

Call comes in via FXO port, -User answers by lifting handset -User press 'hold' button and places handset onhook -User lifts handset, then press the line button -Call drops after a few seconds.

Conditions CME versions 7 and 7.1 IOS version 12.4(20)T and 12.4(24.6)T9 7960 phone load 8.0(5.0).

Workaround If the call is resumed by pressing the line button or resumed before lifting the handset, the call will not disconnect.

CSCta07241 1841 and 2801 do not print memory dumps to crashinfo.

Symptom Crashinfo context is missing useful troubleshooting information.

Conditions This is seen in any memory corruption crashinfos for the 1841 and 2801.

Workaround There is no workaround.

CSCta07484 Crash on a router due to array index out of boundary.

Symptom A crash may occur on a CME when doing a web query on an ephone.

Conditions The symptom is observed when doing a web query on an ephone and maximum SIP phones are not configured on the CME under **voice register global**.

Workaround Configure maximum supported SIP phones under **voice register global**.

CSCta11416 H320 one-way video when H.239 enabled on endpoint.

Symptom Video endpoint -[h323]- H320 GW -[ISDN]- Video Endpoint

A call through a H.320 gateway results in two-way audio and one-way video.

Conditions This is seen when the H.239 capability is enabled on the Video endpoint.

Workaround Disable H.239 capability.

CSCta14536 Router crash pointing to SYS-6-STACKLOW on IPIPGW.

Symptom A Cisco IOS VoIP gateway configured for IPIPGW (CUBE) functionality may crash.

Conditions A gateway configured for IPIPGW functionality with the command **allow-connections** under **voice service voip** under rare conditions will crash while processing VoIP calls.

This has been found to occur in some scenarios where a single voip call loops (meaning the call is from the IPIPGW back to the same IPIPGW) through the IPIPGW.

When this occurs, the following error message may be noticed:

%SYS-6-STACKLOW: Stack for process IP Input running low, 0/12000

Workaround The workaround is to track down the source of the call looping and correct the problem there.

The other possible workaround is to introduce another termination point in the RTP packet flow beside the IPIPGW. For example, if interworking with Cisco Unified Communications Manager (Callmanager) a MTP resource may be used to prevent this loop as long as the MTP resource is not the CUBE gateway.

CSCta16495 IOS should warn if no DSP resources exist for voice-port at bootup.

Symptom When the router boots up, voice ports that require DSPs like FXO and FXS cards do not show up in the running configuration. The card shows up in **show diag, show inventory**, and **show version** but the "voice-port 0/0/0" does not show up in the configuration.

Conditions This happens when there are no available DSPs for the voice ports to use on bootup. The system should print a command similar to: **%VOICE-PORT-INIT: Voice-port 0/0/0 was not initialized due to a lack of DSP resources**.

This indicates that analog voice ports did not have enough DSPs to initialize. **show voice dsp group all** should be used to validate there are enough DSPs. The DSP calculator (http://www.cisco.com/cgi-bin/Support/DSP/cisco_prodsel.pl) should be used to ensure the router has sufficient PVDM modules**.**

Workaround This bug addresses adding the bootup command: **%VOICE-PORT-INIT: Voice-port 0/0/0 was not initialized due to a lack of DSP resources**.

CSCta24037 CME crashed for BACD incoming call while transferring to MOC over SIP trunk.

Symptom A Cisco router may reload due to a bus error and show the following messages:

```
%ALIGN-1-FATAL: Illegal access to a low address 10:09:03 PDT Tue Sep 1 2009
addr=0x0, pc=0x4159DB10z , ra=0xFFFFB4DFz , sp=0x4F059900
```

```
%ALIGN-1-FATAL: Illegal access to a low address 10:09:03 PDT Tue Sep 1 2009
addr=0x0, pc=0x4159DB10z , ra=0xFFFFB4DFz , sp=0x4F059900
```

```
TLB (store) exception, CPU signal 10, PC = 0x415A2630
```

Conditions The symptom is observed on a Cisco 2851 router that is running Cisco IOS Release 12.4(24)T1.

Workaround There is no workaround.

CSCta31622 IOS crashes on CPU hog when mini-logger is enabled.

Symptom Gateway automatically reloads when minilogger is enabled and DSP crash occurs.

Workaround There is no workaround.

CSCta34276 Should allow fixed-no-timestamps mode for clear channel in voip.

Symptom While the CLI is configured for H.323 fixed playout mode without timestamps, the DSP is configured for fixed playout mode with timestamps.

Conditions T1/E1 --- 3845 ---ip--- 3845 --- T1/E1 CLI: playout-delay mode fixed no-timestamps

Workaround There is no workaround.

CSCta40055 Placed calls directory on CUCME shows local user name if overlapping extensions exist.

Symptom When using overlapping dial-plans between 2 CUCME sites, the "Placed Calls" directory of the originating phone will display the correct called number, but the incorrect called name. CUCME correlates the called number with the local username, even though a unique prefix was prepended, and dialed, to the main extension.

Workaround There is no workaround.

CSCta40916 TOH played for incoming H323 call before media negotiation occurs.

Symptom CME: IP phone when answered hears hold tone before getting proper media from the far end. Sometimes the call stays up; other times it drops with cause temp failure.

Conditions CME receiving/sending H323 slow start call over IP.

Workaround Use H.323 fast start.

Further Problem Description: Issue appears to be more visible in cause of slow WAN links (ex: Satellite links)

CSCta54469 During consult transfer, if call on hold disconnects the second leg drops.

Symptom During consult transfer, if call on hold disconnects before user can dial the consult leg, the consult leg will drop. The disconnect times vary from 60-90 seconds

Conditions Phone A calls Phone B. Phone B hits the transfer button to do a consult transfer which places Phone A on hold. Phone A hangs up before Phone B can dial. Phone B dials Phone C. Call from phone B to Phone C is dropped after about 1 minute.

Debugs show the CME forcing the DN back into an onhook state.

Workaround Configuring transfer-digit-collect orig-call will abort the transfer attempt when the first leg disconnects.

CSCta63555 CME crashes after submitting SNR number change menu from EM phone.

Symptom A router crashes if running with Cisco IOS Release 12.4(24)T or later.

Conditions The symptom is observed if the SNR number change menu is selected from an extension mobility phone. The router crashes after submitting the change.

Workaround Configure an SNR under the user-profile or logout-profile with which the extension mobility phone is provisioned.

CSCta69407 DSP isn't told to "turn off" digits with mgcp dtmf-relay nte-gw / nte-ca.

Symptom When using mgcp dtmf-relay type nte-gw, a sniffer trace will reveal that digits are sent both in-band (within the audio stream) and out-of-band (dtmf-relay). Because of this, double digits can be seen in Unity and MeetingPlace.

Conditions GW with PRI/CAS backhaul via MGCP to CUCM and mgcp dtmf-relay configured to use nte-gw.

Workaround Use mgcp dtmf-relay type out-of-band.

CSCta98556 Clientless webvpn incorrectly redirected access to web portal.

Symptom Incorrect redirection is seen while using IOS WebVPN.

Conditions Only seen with IE8.

Workaround IE6 can be used as a workaround

Further Problem Description: Customer has two servers (A,B) protected behind the IOS WebVPN. Some pages on server A automatically does a silent login to server B and gets the information required to generate reports. When using IE8 this login information does not get properly propagated to the backend server B which results in redirection request to the login page from server B.

CSCtb42748 No Ringback on Incoming SIP to AA to SNR line with different codecs.

Symptom No Ringback on Incoming SIP to AA to SNR line with different codecs.

Conditions

- The incoming call is from SIP trunk.
- The outgoing call to mobile has different codec than the incoming call leg.
- The mobile phone on the sip trunk needs to send back the 183 progress message while ringing.
- User is not able to hear the ringback tone after ringing the mobile phone.

Workaround There is no workaround.

CSCtb43226 12.4 IOS MGCP generates 510 remote description error.

Symptom Voice call is rejected, because gateway replies 510 error for MDCX message.

Conditions Interworking with third party IAD device, which doesn't support NSE codec, will mess up SDP format.

Workaround Disable t38 and modem passthrough so gateway doesn't generate NSE in SDP.

CSCtb66305 Shared-dn ephone unregister affects another ephone BLF subscription.

Symptom cme on c3825-advipservicesk9-mz.124-24.T1.bin

one ephone UNREGISTER_ABNORMAL, the other ephone with shared DN will stop sending BLF presence subscription.

Example:

```
ephone 34 button 1:5 2:4
ephone 61 blf-speed-dial 1 ... button 1:5 2:4
```

when ephone 34 unregisters, ephone 61 stops sending presence subscription.

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, page 51
- Platform-Specific Documents, page 51

Release-Specific Documents

The following documents are specific to Release 15.0 and apply to Release 15.0(1)XA:

- *New and Changed Information*
- *Caveats for Cisco IOS Release 15.0M*

Platform-Specific Documents

Hardware installation guides, configuration and command reference guides, and additional documents specific to the Cisco 1800 series routers (fixed) are at

http://www.cisco.com/en/US/products/ps5853/tsd_products_support_series_home.html

Cisco IOS Software Documentation Set

The Cisco IOS software documentation set consists of the Cisco IOS configuration guides, Cisco IOS command references, and other supporting documents.

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.