Release Notes for Cisco IAD2801 Series Integrated Access Devices with Cisco IOS Release 12.4(11)XJ

March 26, 2008
Cisco IOS Release 12.4(11)XJ4
OL-12461-03 Fifth Release

These release notes for the Cisco IAD2801 Series Integrated Access Devices Cisco IAD2801 describe the product-related enhancements provided in the Cisco IOS Release 12.4(11)XJ2. These release notes are updated as needed.

For a list of the applicable software caveats, see the "Caveats" section on page 6. See also *Caveats for Cisco IOS Release 12.4T*, which is updated for every maintenance release.

Use these release notes with the *Cross-Platform Release Notes for Cisco IOS Release 12.4T*.

We recommend that you view the field notices for this release to see if your software or hardware platforms are affected. If you have an account on Cisco.com, you can find field notices at http://www.cisco.com/warp/customer/tech_tips/index/fn.html. If you do not have a Cisco.com login account, you can find field notices at http://www.cisco.com/warp/public/tech_tips/index/fn.html.

Contents

These release notes describe the following topics:

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

Introduction

The following Cisco IAD2801 models are supported:

- IAD2801-2BRI-A/K9- Fixed configuration router, with integrated PVDM2-8, HWIC-1ADSL, and 1 VIC2-2BRI-NT/TE-P, 2 Fast Ethernet connections, and 1 factory configurable HWIC slot
- IAD2801-4BRI-A/K9- Fixed configuration router, with integrated PVDM2-16, HWIC-1ADSL, and 2 VIC2-2BRI-NT/TE-P, 2 Fast Ethernet connections, and 1 factory configurable HWIC slot.
- IAD2801-4BRI-S/K9- Fixed configuration router, with integrated PVDM2-16, HWIC-4SHDSL , and 2 VIC2-2BRI-NT/TE-P, 2 Fast Ethernet connections, and 1 factory configurable HWIC slot

The following cards are supported in the factory configurable HWIC slot on all models:

- HWIC-4ESW
- VIC-4FXS
- HWIC-AP-AG-E or HWIC-AP-G-E

For information on new features and Cisco IOS commands supported by Cisco IOS Release 12.4(11)XJ, see the "New and Changed Information" section on page 4.

System Requirements

This section describes the system requirements for the Cisco IOS Release 12.4(11)XJ releases and includes the following sections:

Memory Requirements

Table 1 lists the memory requirements for the Cisco IOS feature sets on the Cisco IAD2801 in Cisco IOS Release 12.4(11)XJ. The Cisco IAD2801 uses a 32-MB Flash memory card.

Table 1 Cisco Release 12.4(11)XJ Memory Requirements for the Cisco IAD2801 Series IAD

Platform	Feature Set	Software Image	Recommended Flash Memory (MB)	Recommended DRAM Memory (MB)	Runs From
Cisco IAD2801	Advanced IP Services	ciad2801-advipservicesk9-mz	64	256	RAM
Cisco IAD2801	SP Services	ciad2801-spservicesk9-mz	64	256	RAM

Hardware Supported

Cisco IOS Release 12.4(11)XJ supports the Cisco IAD2801 series IADS.

For detailed descriptions of the new hardware features, see the "New and Changed Information" section on page 4.

For information about supported hardware for this platform and release, see the *Hardware/Software Compatibility Matrix* at http://www.cisco.com/cgi-bin/front.x/Support/HWSWmatrix/hwswmatrix.cgi

Determining the Software Release

To determine which version of Cisco IOS software is currently running on your Cisco IAD2801, log in to the router and enter the **show version** command. The following sample output from the **show version** command indicates the release number.

```
roIAD2801#sh version

Cisco IOS Software, IAD2801 Software (CIAD2801-ADVIPSERVICESK9-M), Version 12.4(11)XJ,
RELEASE SOFTWARE (fc1)
Synched to technology version 12.4(11)T
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Mon 08-Jan-07 21:36 by prod_rel_team
ROM: System Bootstrap, Version 12.4(13r)T, RELEASE SOFTWARE (fc1)
yourname uptime is 0 minutes
System returned to ROM by reload at 23:28:34 UTC Thu Jan 11 2007
System image file is "flash:ciad2801-advipservicesk9-mz.124-11.XJ"12.4(11)XJ"
This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.
A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html
If you require further assistance please contact us by sending email to
export@cisco.com.
Cisco IAD2801 (revision 6.0) with 237568K/24576K bytes of memory.
Processor board ID FTX1051Z280
1 DSL controller
2 FastEthernet interfaces
4 ISDN Basic Rate interfaces
1 Virtual Private Network (VPN) Module
1 DSP, 16 Voice resources
DRAM configuration is 64 bits wide with parity disabled.
191K bytes of NVRAM.62720K bytes of ATA CompactFlash (Read/Write)Configuration register is
0x2102
```

Upgrading to a New Software Release

For general information about upgrading to a new software release, see the *Software Installation and Upgrade Procedures* located at http://www.cisco.com/warp/public/130/upgrade_index.shtml.

Feature Set Tables

Cisco IOS software is packaged in feature sets consisting of software images, depending on the platform. Each feature set contains a specific set of Cisco IOS features. Cisco IOS Release 12.4(11)XJ supports the same feature sets as Releases 12.4 and 12.4(11)T, and Cisco IOS Release 12.4(11)XJ includes new features supported by the Cisco IAD2801. See *Cisco Feature Navigator* for supported features

New and Changed Information

The following sections list the new hardware products and software features supported by the Cisco IAD2801 in Cisco IOS Release 12.4(11)XJ1:

New Hardware Features in Release 12.4(11)XJ4

There are no new hardware features in this release.

New Software Features in Release 12.4(11)XJ4

There are no new software features in this release.

New Hardware Features in Release 12.4(11)XJ3

There are no new hardware features in this release.

New Software Features in Release 12.4(11)XJ3

There are no new software features in this release.

New Hardware Features in Release 12.4(11)XJ2

There are no new hardware features in this release.

New Software Features in Release 12.4(11)XJ2

There are no new sofrtware features in this release.

New Hardware Features in Release 12.4(11)XJ1

There are no new hardware features in this release.

New Software Features in Release 12.4(11)XJ1

There are no new software features in this release.

New Features in Release 12.4T

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

Limitations and Restrictions

The following limitations and restrictions apply to the Cisco IAD 2801 series

Fixed Configuration Platforms Supporting Specific Cards

The IAD2801 series are fixed configuration platforms with each slot supporting specific cards. Supported cards in each model are shown in the table below:

Model	Slot 0	Slot 1	Slot 2	Slot 3
IAD2801-2BRI-A/K9	VIC2-2BRI-NT/TE-P	HWIC-1ADSL	Not Available	LTD Option*
IAD2801-4BRI-A/K9	VIC2-2BRI-NT/TE-P	HWIC-1ADSL	VIC2-2BRI-NT/TE-P	LTD Option*
IAD2801-4BRI-S/K9	VIC2-2BRI-NT/TE-P	HWIC-4SHDSL	VIC2-2BRI-NT/TE-P	LTD Option*

* LTD OPTION (Factory installable or Field Upgradeable)

- HWIC-AP-AG-E and HWIC-AP-G-E

- HWIC-4ESW

- VIC-4FXS/DID

Unsupported Card Message

If any unsupported card is detected during the bootup, the following message appears:

"Card is not supported in slot 2. Please remove it"

This message will appear for each unsupported card detected.

If any cards are not supported and **smart-init** is enabled, another message appears during bootup:

```
Smart Init is enabled
smart init is sizing iomem
  ID             MEMORY_REQ          TYPE
                 0X003AA110 public buffer pools
                 0X00211000 public particle pools
                 0X00020000 Crypto module pools
                 0X00120000 VPM buffer pools
0X05B3           0X000034A0 Card in slot 0
0X04C8           0X00077D00 Card in slot 1
0X05B3           0X00000000 UNKNOWN Card in slot 2
0X003A           0X00000000 Card in slot 3
                 0X000021B8 Onboard USB
```

Caveats

Caveats describe unexpected behavior or defects in Cisco IOS software releases. Severity 1 caveats are the most serious caveats, severity 2 caveats are less serious, and severity 3 caveats are the least serious of these three severity levels.

Caveats in Cisco IOS Release 12.4(11)T are also in Cisco IOS Release 12.4(11)XJ1. For information on caveats in Cisco IOS Release 12.4(11)T, see the *Caveats for Cisco IOS Release 12.4(11)T* document. This document lists severity 1 and 2 caveats.

Note If you have an account with Cisco.com, you can also use the Bug Toolkit to find select caveats of any severity. To reach the Bug Toolkit, go to: http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl.

This section contains the following caveat information:

Open Caveats - Cisco IOS Release 12.4(11)XJ4

There are no open caveats in this release.

Resolved Caveats - Cisco IOS Release 12.4(11)XJ4

Miscellaneous Caveats

- CSCse56501

  A device running Cisco IOS software that has Internet Protocol version 6 (IPv6) enabled may be subject to a denial of service (DoS) attack. For the device to be affected by this vulnerability the device also has to have certain Internet Protocol version 4 (IPv4) User Datagram Protocol (UDP) services enabled. To exploit this vulnerability an offending IPv6 packet must be targeted to the device. Packets that are routed throughout the router can not trigger this vulnerability. Successful exploitation will prevent the interface from receiving any additional traffic. The only exception is Resource Reservation Protocol (RSVP) service, which if exploited, will cause the device to crash. Only the interface on which the vulnerability was exploited will be affected.

  Cisco is providing fixed software to address this issue. There are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20080326-IPv4IPv6.shtml.

- CSCsf12082

  Certain Cisco Catalyst 6500 Series and Cisco 7600 Router devices that run branches of Cisco IOS based on 12.2 can be vulnerable to a denial of service vulnerability that can prevent any traffic from entering an affected interface. For a device to be vulnerable, it must be configured for Open Shortest Path First (OSPF) Sham-Link and Multi Protocol Label Switching (MPLS) Virtual Private Networking (VPN). This vulnerability only affects Cisco Catalyst 6500 Series or Catalyst 7600 Series devices with the Supervisor Engine 32 (Sup32), Supervisor Engine 720 (Sup720) or Route Switch Processor 720 (RSP720) modules. The Supervisor 32, Supervisor 720, Supervisor 720-3B, Supervisor 720-3BXL, Route Switch Processor 720, Route Switch Processor 720-3C, and Route Switch Processor 720-3CXL are all potentially vulnerable.

  OSPF and MPLS VPNs are not enabled by default.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20080326-queue.shtml.

- CSCsk73104

  Cisco IOS contains multiple vulnerabilities in the Data-link Switching (DLSw) feature that may result in a reload or memory leaks when processing specially crafted UDP or IP Protocol 91 packets.

  Cisco has released free software updates that address these vulnerabilities. Workarounds are available to mitigate the effects of these vulnerabilities.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20080326-dlsw.shtml

- CSCsi01470

  A vulnerability in the Cisco implementation of Multicast Virtual Private Network (MVPN) is subject to exploitation that can allow a malicious user to create extra multicast states on the core routers or receive multicast traffic from other Multiprotocol Label Switching (MPLS) based Virtual Private Networks (VPN) by sending specially crafted messages.

  Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are available.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20080326-mvpn.shtml.

- CSCdv59309

  Two vulnerabilities exist in the virtual private dial-up network (VPDN) solution when Point-to-Point Tunneling Protocol (PPTP) is used in certain Cisco IOS releases prior to 12.3. PPTP is only one of the supported tunneling protocols used to tunnel PPP frames within the VPDN solution.

  The first vulnerability is a memory leak that occurs as a result of PPTP session termination. The second vulnerability may consume all interface descriptor blocks on the affected device because those devices will not reuse virtual access interfaces. If these vulnerabilities are repeatedly exploited, the memory and/or interface resources of the attacked device may be depleted.

  Cisco has made free software available to address these vulnerabilities for affected customers.

  There are no workarounds available to mitigate the effects of these vulnerabilities.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20080326-pptp.shtml

- CSCsj58566

  Two vulnerabilities exist in the virtual private dial-up network (VPDN) solution when Point-to-Point Tunneling Protocol (PPTP) is used in certain Cisco IOS releases prior to 12.3. PPTP is only one of the supported tunneling protocols used to tunnel PPP frames within the VPDN solution.

  The first vulnerability is a memory leak that occurs as a result of PPTP session termination. The second vulnerability may consume all interface descriptor blocks on the affected device because those devices will not reuse virtual access interfaces. If these vulnerabilities are repeatedly exploited, the memory and/or interface resources of the attacked device may be depleted.

  Cisco has made free software available to address these vulnerabilities for affected customers.

  There are no workarounds available to mitigate the effects of these vulnerabilities.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20080326-pptp.shtml

`CSCsg70474`

Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:

- Session Initiation Protocol (SIP)
- Media Gateway Control Protocol (MGCP)
- Signaling protocols H.323, H.254
- Real-time Transport Protocol (RTP)
- Facsimile reception

Cisco has made free software available to address these vulnerabilities for affected customers. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities mentioned 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.

This advisory is posted at
http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml

CSCsi60004

Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:

- Session Initiation Protocol (SIP)
- Media Gateway Control Protocol (MGCP)
- Signaling protocols H.323, H.254
- Real-time Transport Protocol (RTP)
- Facsimile reception

Cisco has made free software available to address these vulnerabilities for affected customers. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities mentioned 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.

This advisory is posted at
http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml

CSCsi80749

Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:

- Session Initiation Protocol (SIP)
- Media Gateway Control Protocol (MGCP)
- Signaling protocols H.323, H.254
- Real-time Transport Protocol (RTP)
- Facsimile reception

Cisco has made free software available to address these vulnerabilities for affected customers. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities mentioned 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.

This advisory is posted at
http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml

CSCsh84171 Memory corruption in IOMEM - block overrun, FPGA ISDN DMA issue

Symptom Router is crashing due to memory corruption with following message:
%SYS-3-OVERRUN: Block overrun at 3F379450 (red zone 2A2A2A2A)

Conditions This occurs on a 2800 router running 12.4T images.

Workaround There is no workaround.

CSCsi60919 HWIC-ADSL-B/ST or HWIC-1ADSL Ping Fails After External Shut/No Shut

Symptom ADSL stops receiving any more packet after external shut/no shut or ADSL line retrains several times. This is specific to HWIC-1ADSL, HWIC-1ADSLI, HWIC-ADSL-B/ST, and HWIC-ADSLI-B/ST.

Conditions It happens after external shut/no shut or ADSL line retrains 8 times.

shut/no shut the ADSL ATM interface.

Workaround There is no workaround.

CSCsg03449 Etherswitch module VLAN Trunking Protocol Vulnerabilities

Symptom
* VTP Version field DoS
* Integer Wrap in VTP revision
* Buffer Overflow in VTP VLAN name

Conditions The packets must be received on a trunk enabled port.

Further Information
On the 13th September 2006, Phenoelit Group posted an advisory containing three vulnerabilities:

* VTP Version field DoS
* Integer Wrap in VTP revision
* Buffer Overflow in VTP VLAN name

These vulnerabilities are addressed by Cisco IDs:

* CSCsd52629/CSCsd34759 -- VTP version field DoS
* CSCse40078/CSCse47765 -- Integer Wrap in VTP revision
* CSCsd34855/CSCei54611 -- Buffer Overflow in VTP VLAN name
* CSCsg03449 -- Etherswitch module VLAN Trunking Protocol Vulnerabilities Cisco's statement and further information are available on the Cisco public web site at:
http://www.cisco.com/warp/public/707/cisco-sr-20060913-vtp.shtml

CSCsi45826 When a call is made, display shows its own ephone-dn name

CSCsh89887 One way voice path with h/w conference on ephone-dn w/o preference 0

CSCsi46911 MALLOCFAIL failure on 2800,Cause: Mempool corrupt

Symptom While doing h323 to sip interop, the router is crashing due to Mempool corrupt.

Topology: PhoneA -- CME1 --- SIP --- CME2 -- PhoneB

Call flow:

1. PhoneA calls PhoneB.
2. PhoneB answers.
3. PhoneB presses transfer.
4. PhoneB presses NewCall.
5. PhoneB dials PhoneA.
6. We see PhoneB drop out of the call with no error indications or tones.
7. We see PhoneA display one call on hold and the other call incoming.
8. Hang up PhoneA.
9. PhoneA rings briefly when you put it on hook.

Workaround There is no workaround.

CSCsi65535 codec configured under ephone is used by all monitored phone.

Symptom The “codec” configuration under a “ephone” which monitors a line (“ephone-dn”) with the “m” button configuration command affects the codec of calls involving that “ephone-dn” as if the line was shared in the regular manner (using the “:” button configuration command).

Conditions Please see the “Symptom” description above. Please remember that the “codec” configuration under “ephone” is for phones registering over a WAN to the CME router. It directs CME to attempt to use the G.729 codec to save some bandwidth over that WAN segment, in some (non-VoIP) call scenarios. It doesn't restrict the codec of any call in any way. There is no well defined “negotiation” mechanism that makes use of this codec configuration as in H.323/H.245 codec negotiation for example.

Workaround There is no workaround.

CSCsi79331 Overlay DN gets stuck to BUSY when using loopbacked TCL script invocation

Symptom Ephone dn gets stuck in a busy state.

Conditions Callers will get ringback but no phone will actually ring.

Workaround Remove the DN, then add it back in. Also have to add all the buttons for that DN back on the ephones.

CSCsi58842 CME: 7960+7914 display select line when conference IP phone

Symptom

1. A caller call a person “A”.
2. Person “A” answer the call.
3. Person “A” is monitored by the person “B”.
4. The person “B” see on his phone that the person “A” has received a call. Also person “B” calls person “A” using the monitor button.
5. Person “A” answers the call, putting the first caller on hold.
6. Person “A” uses the conference softkey “Confirm”.
7. The message “Select Line” appears without any effect.

Workaround There is no workaround.

CSCsi14143 Some phone types not working with trunk monitor lines

Symptom The 7920, 7921, and 7985's line icon change does not change in response to a seized trunk line.

Conditions A 7920, 7921, or 7985's line is configured under CME with 'trunk <xxx> monitor-port x/x/x' and the corresponding trunk is seized.

Workaround There is no workaround.

CSCsi04538 Router crash with memory corruption when configure cert-upgrade auth mod

Symptom A router that is configured as a Cisco Unified Call Manager Express (CUCME) router may crash because of a memory corruption.

Conditions This symptom is observed when voice calls are made involving a transcoder.

Workaround There is no workaround.

CSCsg38919 Traceback and DSP timeout found after T1/E1 CAS call is established

CSCek74685 Wrong caller ID showed on XEE after Consult Transfer

Symptom When SIP phone calls through SIP trunk to (XOR) phone and transfer to another (XTO) phone, the XTO phone shows the XOR caller id.

CSCsf02356 <calling-number local> is broken for hairpin call forwarding

Symptom Calling party information is shown wrongly for a forwarded call when using 'calling-number local'.

Conditions On CME 4.0 configured with 'calling-number local', a forwarded call rings the forward target and displays calling party name, number and redirection information. When 'calling-number local' is configured, the call setup to the forwarding target should just contain the forwarder's name and number as calling party information.

Workaround There is no workaround.

CSCsi41401 Spurious memory access at ephone_delete_tftp_binding_by_url

Symptom Spurious memory access seen on startup or after creating cnf files.

Conditions CME secure phone config.

Workaround There is no workaround.

CSCsi29899 Fast busy in CME 4.1 if two conferences completed at same time

Symptom Creator of conference gets a fast busy when trying to complete conference. Other parties of potential conferenced are connected to parties of separate conference

Conditions User must have CME 4.1 using hardware resources for conferencing. Two users must try to complete separate conferences at same time

Workaround There is no workaround.

CSCsg96319 reverse ssh eliminated telnet authentication on VTY

Symptom Anyone can have unprivileged Telnet access to a system without being authenticated, when a reverse SSH session is established with valid authentication credentials. This only affects reverse SSH sessions where a connection is made with the **ssh -l userid**:*number ip-address* command.

Conditions This symptom has been seen only when Reverse SSH Enhancement is used. This enhancement is documented at the following URL: http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec_rev_ssh_enhanmt_external_docbase_0900e4b1805b0676_4container_external_docbase_0900e4b1807b42a5.html

Workaround Configure reverse SSH with the **ip ssh port** *portno* **rotary** *rotarygroup* command.

This configuration is explained at the following URL:

http://www.cisco.com/en/US/tech/tk583/tk617/technologies_q_and_a_item09186a0080267e0f.shtml#newq1

CSCsi56172 CME 4.1 IP phone dropped when trying to complete hardware conference

Symptom IP phone trying to create an ad-hoc conference is dropped when pressing “Conf” softkey the second time.

Conditions Must be using hardware conferencing in CME 4.1. The IP phone must receive a call first on on overlaid button. This initial call must come in on any DN besides the first DN configured in the “button” command in ephone config.

CSCsg37315 IOS FW on VPN tunnels fail on 12.4(11)T on 87x and 18xx platforms

Symptom If CBAC is configured in conjunction with VPN tunnels, TCP connections through the firewall might fail. CBAC ignores the SYN/ACK packets coming from IPsec tunnel and then drops all outbound TCP packets except initial SYN, generating message “Invalid Segment tcp”. Outbound TCP connections to the Internet (not over IPSec tunnel) are not affected and work fine with CBAC.

Conditions VPN tunnels must be configured on the router in conjunction with CBAC

Workaround Disable hardware encryption on the router with the command: **no crypto engine accelerator**

CSCsi93064 Only One line is available in CME GUI for 7921 instead of SIX

Symptom When a 7921 IP Phone is in "registered" status, CME GUI displays only one line instead of six lines.

Conditions There is no workaround

Workaround Use the CLI to configure additional lines.

CSCsi07340 no call waiting notification for monitored line

CSCsh24266 L2TP connection fails on PPP phase due to invalid UDP port#

Symptom L2TP connection fails on PPP phase because the LNS replies PPP frame within L2TP frame including invalid UDP destination port number, to LAC.

Conditions
- This problem only occurs on PPP phase after L2TP setup.
- On L2TP tunnel/session setup phase, LNS uses correct UDP port number.
- source port number which LNS generates is not affected.
- If you use Cisco router as LAC, this problem will not occur.

Workaround There is no workaround.

CSCsi78162 SNASw %DATACORRUPTION-1-DATAINCONSISTENCY messages

CSCsf96318 QSIG (ISO) Call back fails between 3745 and 1760

CSCsi13312 Authentication fails and unable to login to a factory fresh router

Symptom Authentication with Security Device Manager (SDM) 2.3.3 fails, preventing you from logging into the router through HTTPS, HTTP, SSH, Telnet, console, or any management application.

Conditions This symptom is observed on a Cisco router that is "fresh out of the box" and affects the following routers:

Cisco 800 series
Cisco 1700 series
Cisco 1800 series
Cisco 2700 series

Cisco 2800 series
Cisco 3700 series
Cisco 3800 series

Workaround For extensive information and a workaround, see the following Field Notice: http://www.cisco.com/en/US/support/tsd_products_field_notice_summary.html

`CSCsi39520 CME: SIP MWI relay does not send notify msg after MWI on from Unity`

`CSCsi94745 ISDN call is dropped in due to STATUS message from PBX`

Symptom Call is dropped from GW in response to STATUS message from PBX.

Conditions Then CONNECT message has Channel ID i.e., some PBX complain and send STATUS message.

Workaround There is no workaround.

`CSCse91298 Sharedline and Overlay Phone Calling the Sharedline Cause Port Hung`

Symptom STCAPP port get hung in various state.

Conditions When a sharedline member calls the sharedline DN phone number, the other sharedline member which also overlay DNs on the same line will get port hung in various state.

Workaround Reload

`CSCsi76991 incoming sip call transferred local; audio not heard on ip phone`

Symptom After the call transfer on alert, audio is not heard on ip phone

Conditions G729 call from Service Provider Network through SIP trunk to IP phone A on CME, transferred local on alert (blind transfer) to ip phone B; CME is configured to hairpin the calls

Workaround There is no workaround.

Further Problem Description: During the call transfer, service provider network send slightly different media capabilities on the 200 OK with SDP; capabilities are agreed from CME; but this new capabilities seem to make the issue;

CSCsg40567 Memory leak found with malformed tls/ssl packets in http core process

Symptom Malformed SSL packets may cause a router to leak multiple memory blocks.

Conditions This symptom is observed on a Cisco router that has the ip http secure server command enabled.

Workaround Disable the ip http secure server command.

CSCsi67763 memory leak under simpleudpfuzz attack for port 500

Symptom The U.S. Computer Emergency Response Team (US-CERT) has reported a network evasion technique using full-width and half-width unicode characters that affects several Cisco products. The US-CERT advisory is available at the following link: http://www.kb.cert.org/vuls/id/739224.

By encoding attacks using a full-width or half-width unicode character set, an attacker can exploit this vulnerability to evade detection by an Intrusion Prevention System (IPS) or firewall. This may allow the attacker to covertly scan and attack systems normally protected by an IPS or firewall.

Cisco response is posted at the following link:

http://www.cisco.com/warp/public/707/cisco-sr-20070514-unicode.shtm

CSCsh86912 HWIC-4SHDSL: Implement CO mode support and line probing (PMMS) config

Symptom Need to add a CLI to configure a HWIC-4SHDSL as CO and a CLI to configure the noise margin settings for auto mode.

Workaround This is an enhancement.

Further Problem Description:

```
Router(config)#controller shdSL 0/3/0
Router(config-controller)#termination ?
 co   termination co (network)
 cpe  termination cpe (customer)

Router(config-controller-dsl-group)#shd rate auto pmmsmargin ?
 current  PMMS Current SNR Margin
 worst    PMMS Worst SNR Margin
```

CSCsi11217 HWIC-4SHDSL has issue on IMA interface w/Lucent SHDSL-IMA card

Symptom Some links in IMA group are shown as down though they are active at IMA level.

Conditions With Lucent as DSLAM, when IMA group is made inactive and then active again, some links are shown as down and not counted as active.

Workaround Doing a shutdown/no shutdown from the CLI at the dsl group recovers from the issue.

CSCsj23569 codec selection issue on incoming SIP trunk

Symptom Incoming call on a SIP trunk with G729 as preferred codec sets up but there is no ringback and dtmf is not working.

Conditions

```
incoming SDP 18 0 8 101
!
voice class codec 729
codec preference 1 g729br8
codec preference 2 g729r8
codec preference 3 g711ulaw
!
```

Workaround Do not use voice-call codec.

CSCsj03494 I/O Memory corruption crash with IP communicator and 7961 IP Phones

Symptom A 2811 series router may crash due to I/O memory corruption.

Conditions Router running CME 4.1 with 12.4.11.XJ3 image and using IP communicator and/or IP phones

Workaround Stop using IP phones or IP communicator.

CSCsj18014 Caller ID string received with extra characters

Symptom Caller ID is received with extra characters.

Conditions Whatever name is sent by the source will be received by the destination.

Workaround There is no workaround.

Open Caveats - Cisco IOS Release 12.4(11)XJ3

There are no open caveats for this release.

Resolved Caveats - Cisco IOS Release 12.4(11)XJ3

There are no resolved caveats for this release.

Open Caveats - Cisco IOS Release 12.4(11)XJ2

CSCsi09530 CME SIP phone failed to register because of authenticate register

Symptom If “authenticate register” is configured under “voice register global”, CME SIP failed to registered.

Conditions “authenticate register” is configured under “voice register global”, when CME is acting as a RIGISTRAR

Workaround Disable “authenticate register” under “voice register global”

Further Problem Description: In registrar Functionality, CME challenges an inbound Register request with 401 response If “authenticate register” is configured under “voice register global”. The Registering Endpoint then Sends a Register Request with Credentials. GW Stack is not processing this Request and is dropping it.

Resolved Caveats - Cisco IOS Release 12.4(11)XJ2

CSCsf08998

Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:

- Session Initiation Protocol (SIP)
- Media Gateway Control Protocol (MGCP)
- Signaling protocols H.323, H.254
- Real-time Transport Protocol (RTP)
- Facsimile reception

Cisco has made free software available to address these vulnerabilities for affected customers. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities mentioned 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.

This advisory is posted at
http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml

CSCsh23992 IAD2801 BRI voice port ISDN status does not come up

Csg51259 CME: DTMF stops working after consult transfer to called party’s mailbox

CSCsg51244 CME: CME does not send 3xx messages for transfer --> forward scenarios

CSCsg46411 CME: CME does not send a REFER over SIP trunk for calls involving AA

CSCsg30101 CME: dtmf-relay force rtp-nte CLI does not work

CSCsf32028 CME: Host portion of Refer-To: header must be an Address of Record

CSCsg59037 85x/87x cannot upgrade rommon from IOS

Symptom Cisco 851 and 871 routers have no way to remotely upgrade the ROMMON firmware image.

Conditions Cisco IOS versions for the Cisco 851 and 871 routers did not provide a mechanism to remotely upgrade the ROMMON firmware image.

Workaround Cisco IOS Release 12.4(11)T1 for the Cisco 851 and 871 router introduces the command upgrade rom-monitor file which allows the ROMMON firmware image to be remotely upgraded. Please consult this link for more information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124tcr/tcf_r/cf_13ht.htm#wp1032550

CSCsf26561 CME: User portion of Diversion header is incorrect when calling through AA

Conditions Tests on Cbeyond's Live setup have revealed that PSTN to AA --> tx to SCCP phone--> CFWD to CUE/PSTN has an issue. The 302 Moved Temporarily from CME to BroadSoft has a Diversion header whose user portion is the private extension #, not the expanded DID # due to which the subsequent call fails.

Workaround Unless removing the dialplan-pattern, no work around present.

CSCsg46362 contact header incorrect in 302 message using sip-srst redirect mode

Symptom The contact header ip address is incorrect in the 302 message sent by sip srst in redirect mode. As the result basic call fails in this mode.B2b mode is working okay.

Workaround Use b2b mode

CSCsg17289 DNS-SRV issues for SIP registrations

CSCsg39750 Spurious mem access/traceback while resetting sip phone with presence

CSCsg18902 Blind transfer is not working on SIP trunk

Symptom Blind transfer failed on SCCP endpoint over SIP trunk

Conditions When session-target is configured but outbound-proxy is not configured.

Workaround None

CSCse89321 Dtmf path not getting confirmed in sip media forking call

CSCsg94873 One way audio for PSTN to AA and calls xferred to SIP phone with G.729

CSCsh25511 A router may crash with CPU Vector 300

Symptom A router may crash with CPU vector 300

Conditions IOS running qos and cce

Workaround none

Further Problem Description:

CSCsh45544 Placed call list in 7970 phone always shows unknown number

CSCsh37177 %SDP-3-SDP_PTR_ERROR traceback error when redirecting call to AA

CSCsg31719 Digits are not relayed correctly when call is not connected.

Symptom When onhook dialing or speed dial is performed from CME to an analog port where dialtone is slightly delayed some digits are dropped.

Conditions This is not seen when the digits are delayed, or when the user waits to hear dialtone then dials.

Workaround Dial digit by digit

CSCsh14247 Call transfer fails when initiated from SIP Phone

CSCsg49416 Refer is not sent by CME when Cfwd all is set from TNP phone

CSCsh19990 Traceback= 0x438662AC 0x40BF2BEC with Call Park/Pick Up operation

CSCsh37345 DSL Operating-mode ‘auto tone low’ enables ETSI mode only

Symptom The DSL line fails to train with “dsl operating-mode auto tone low” command if the DSLAM does not support ETSI mode.

Conditions In the command **dsl operating-mode auto tone low**, the “**dsl operating-mode auto**” is used to enable all the supported modes on a DSL line and the “**tone low**” is used to disable DT-UR2 so that the DSL line can use the carrier tones 29 through 48. Instead, this command does not disable DT-UR2 and enables only ETSI mode. With this,

a. If the DSL configuration on the DSLAM does not support ETSI mode, then the DSL line fails to train up.

b. If the DSLAM supports ADSL2+, ADSL2, ETSI modes, then it trains in ETSI mode, where it's supposed to train in ADSL2+, since the ADSL2+ has higher priority than ETSI mode.

Workaround Avoid using “**dsl operating-mode auto**” command. To select a desirable mode along with disabling DT-UR2, the commands like “**dsl operating-mode adsl2+ tone low**” or “**dsl operating-mode adsl2 tone low**” can be used.

`CSCsh11146 Memory leak at AFW_SS_SIP_PrepareTransferSetup`

Symptom Memory leak occurred in transfer scenarios.

Workaround There are no workarounds.

`CSCek67638 include presence feature in c2801 security package`

Symptom The 2801 security image does not have presence feature.

`CSCsh59469 DTMF is distorted when played from SCCP controlled ATA on CME`

Symptom DTMF generated by a SCCP controlled ATA registered to CallManager Express may be choppy, broken, or overlapping when multiple digits are pressed, one after another.

Example topology:

```
IVR---fxs---ATA---sccp---CME---pri---PSTN
```

A user in the PSTN calls the IVR. The digits are not reliably detected by the IVR when pressed by the PSTN user because of the overlapping / choppy output.

Conditions This is seen on a SCCP controlled ATA registered to CallManager Express.

Workaround Use H323 software on the ATA.

`CSCsh55262 Update CME GUI version and new Cisco logo`

`CSCsg95736 MAC address is missing for radio interface`

Symptom IOS image is not reading the mac address for radio interface.

Workaround The problem is not seen if the dot11 interface is in up state.

CSCsh53808 Transcoder fails after several H.323 transcoded calls to CUE

CSCsg31559 Spurious memory access at strncmp, skinny_hwconf_check_adhoc_register

CSCsh14101 503 Service Unavailable should be sent to CAC rejected calls

CSCsh60218 VG224 continues to ring when first of two ringing shared calls hangs up

CSCsh48646 FAC fails for the first time after enabling in certain conditions

CSCsh78605 Need CLI to enable/disable SIP Line incoming dial-peer matching

Symptom For an inbound call across a SIP Trunk, IOS might match an dynamically configured dial-peer instead of the user-defined dial-peer configured with “incoming called-number“.

Conditions This problem was observed when IOS SIP Gateway was also configured as a SIP SRST.

Workaround Use IOS 12.4(6)T6.

CSCsh39749 Few objects of hdsl2ShdslSpanStatusTable giving wrong values with ARCHER

Symptom MIB value for LineRate (hdsl2ShdslStatusMaxAttainableLineRate) queried through SNMP GET/GETNEXT returns incorrect values. Also hdsl2ShdslInvVendorID displays data in wrong format.

Conditions No Specific conditions.

Workaround For hdsl2ShdslStatusMaxAttainableLineRate, multiply the value with 1000 and for **hdsl2ShdslInvVendorID**, convert the displayed values into ASCII characters.

CSCsh63545 ARCHER IMA MIB modifications

Symptom SNMP walk on imaLinkIntervalTable returns no entries. SNMP get does not work for **imaGroupTable**.

Conditions No specific condition.

Workaround No workaround for **imaLinkIntervalTable**. Do a SNMP Walk on **imaGroupTable** to view the individual table entry values.

CSCsh46622 HDSL2-SHDSL-LINE-MIB:Few tables not populated for ARCHER with CRUSHER on

Symptom When HWIC-4SHDSL and WIC-1SHDSL-V2 are present in a router, HDSL2-SHDSL-LINE-MIB entries for HWIC-4SHDSL are not getting displayed.

Conditions This problem happens if WIC-1SHDSL-V2 comes up before HWIC-4SHDSL.

1. Shutdown both HWIC-4SHDSL and WIC-1SHDSL-V2.
2. Reload the router. Do a “no shutdown” on HWIC-4SHDSL controller first and then do a “no shut” for WIC-1SHDSL-V2 controller.
3. Then save the config.

CSCsh41397 SNMP getone gives NO_SUCH_INSTANCE_EXCEPTION error for HWIC-4SHDSL

Symptom SNMP GET operation on HDSL2-SHDSL-LINE-MIB objects returns no such instance for HWIC-4SHDSL.

Conditions No specific conditions. The failure always happens when a SNMP get is done.

Workaround Workaround is to do SNMP Walk for the entire table.

CSCsh68584 CME MWI notify message not compliant to RFC 3842

Symptom MWI lights on 7970 does not glow

Conditions 7970 when configured as SIP phone for CME.

Workaround There are no workarounds

CSCsh68560 CME: sip to sccp to sccp attend transfer fails

Symptom One way audio.

Conditions The problem is observed when you have XEE SIP line or trunk, XOR and XTO sccp on same CME, consultation transfer.

Workaround No apparent workaround, except that the problem is intermittent.

`CSCsh22682 vlan information disappears after router reload`

Symptom Devices in data VLAN on MVAP configured port with portfast loose connectivity

Conditions Device is connected to MVAP configured port with portfast enabled. Router has been reloaded.

Workaround Remove and add data VLAN from VLAN database. Sometimes this does not seem to work

12.4(9)T and earlier releases do not see this problem

Do not use portfast on MVAP port

Further Problem Description: After the router has been reloaded we see an incomplete **arp** entry. Removing and adding VLAN data fixes this issue for a while. This issue si also resolved If the MVAP port does not have portfast enabled.

`CSCsg76281 CME 4.1:PSTN-to-AA, tx to sccp1, then tx to sccp2, cfwd all to CUE fails`

`CSCsg18481 Consult Transfer failed with Call forward busy`

Symptom Consult transfer failed when XTO has call-forward busy

Conditions XEE is SCCP endpoint and XOR is SIP phone

Workaround There are no workarounds

`CSCsh58082 SIP: A router may reload due to SIP traffic`

Symptom Cisco devices running an affected version of Internetwork Operating System (IOS) which supports Session Initiation Protocol (SIP) are affected by a vulnerability that may lead to a reload of the device when receiving a specific series of packets destined to port 5060. This issue is compounded by a related bug which allows traffic to TCP 5060 and UDP port 5060 on devices not configured for SIP. There are no known instances of intentional exploitation of this issue. However, Cisco has observed data streams that appear to be unintentionally triggering the vulnerability.

Workaround Workarounds exist to mitigate the effects of this problem on devices which do not require SIP. This advisory is posted at: http://www.cisco.com/warp/public/707/cisco-sa-20070131-sip.shtml.

CSCec12299 Corruption of ext communities when receiving over ipv4 EBGP session

Symptom EIGRP-specific Extended Community 0x8800 is corrupted and shown as 0x0:0:0.

Conditions This symptom is observed when EIGRP-specific Extended Community 0x8800 is received via an IPv4 EBGP session on a CE router. This occurs typically in the following inter-autonomous system scenario:

ASBR/PE-1 <----> VRF-to-VRF <----> ASBR/PE-2

Workaround Use a configuration such as the following to remove extended communities from the CE router:

```
router bgp 1
 address-family ipv4 vrf one
 neighbor 1.0.0.1 remote-as 100
 neighbor 1.0.0.1 activate
 neighbor 1.0.0.1 route-map FILTER in
 exit-address-family
!
ip extcommunity-list 100 permit _RT.*_
!
!
route-map FILTER permit 10
 set extcomm-list 100 delete
!
```

CSCsh95740 CME tftp bindings corrupt/erroneous with perphone cnf

Symptom On 12.4(11)XJ, performing a 'show tele tftp-bindings' may show corrupted or incorrect output.

Conditions The CME system was reloaded with 'cnf-file perphone' configured under telephony-service.

Workaround There is no workaround.

CSCek68607 CallerID not updated with AA CFB call to sip phone over SIP trunk

CSCsh90148 SIP UPDATE message sending should be controllable via CME on SIP trunk

Symptom UPDATE messages being sent on the SIP trunk cause calls to fail under certain conditions

Conditions Calls are over a SIP trunk from CME 4.1 to service provider SIP proxy

Workaround There are no workarounds

CSCsh45568 Alignment errors in classify_packet

Symptom Alignment errors may be seen on a Cisco router due to NBAR. High CPU may be seen as well.

Workaround No known workaround at this time.

CSCsf25671 Client with L2TPv2 on Virtual-PPP fails to get ip add from LNSs ip pool

Symptom L2TPv2 VPDN sessions are terminated by the client shortly after IPCP negotiation completion

```
00:00:23.859: Vp1 IPCP: State is Open
00:00:23.859: Vp1 IPCP: Install negotiated IP interface address #.#.#.#
00:00:23.859:  IP-ADDR: ip_new_address(), old 0.0.0.0/0, new #.#.#.#/# on
Virtual-PPP1
00:00:23.859: ACLIB [Vp1, 22]: ac_ppp_voluntary_restore_link_vectors() -
Restoring previously saved link
00:00:23.859: ACLIB [Vp1, 22]: SW AC interface UNPROVISIONED for PPP interface
Vp1
00:00:23.859: ACLIB: Unbinding SWSB subblock
00:00:23.859: ACLIB [Vp1, 22]: Deleting AC sublock structure.
00:00:23.859: ACLIB: ac_ppp_restart_session() - restarting LCP.
00:00:23.859: Xconnect[ac:Vp1(PPP)]: provisioning fwder with fwd_type=1,
sss_role=2
00:00:23.859: ACLIB: Setting new AC state to Ac-Provisioning, old state was

Ac-Idle
00:00:23.859: ACLquest
00:00:23.859:  IP-ADDR: invoke_ip_address_change() to 0.0.0.0/0, secondary

off, sense off, on Virtual-PPP1
00:00:23.859:  IP-ADDR: invoke_ip_address_change() to #.#.#.#/#, secondary

off, sense on, on Virtual-PPP1
00:00:23.859:  IP-ADDR: ipaddr_table_insert() #.#.#.#, in global table on

Virtual-PPP1IB [Vp1, 22]: AC attached subblock to Virtual-PPP1
00:00:23.859: ACLIB ive <Circuit Provisioned> msg
00:00:23.863: ACMGR [Vp1, 22]: provision event, FSP down state no chg, action

is ignore[Vp1, 22]: AC provisioned. Bringing down existin
00:00:23.863: XC L2TP: Received L2TUN API message <Unprovision>
00:00:23.863: XC L2TP: uid:116[#.#.#.#/#] Event <L2TUN Session Unprovision>,
```

```
state Established -> Established
00:00:23.863: XC L2TP: Sending L2TUN message <Disconnect>
00:00:23.863: XC L2TP: uid:116[#.#.#.#/#] L2TUN socket teardown:
00:00:23.863: XC L2TP: uid:116[#.#.#.#/#]   "xconnect destroyed"
00:00:23.863: XC L2TP: uid:116[#.#.#.#/#] PW-MGMT: PW peer #.#.#.#, vcid #
00:00:23.863: XC L2TP: uid:116[#.#.#.#/#] PW-MGMT: Reason [Unprovisioned]g

PPP session on interface Vp1
00:00:23.859: ACLIB [Vp1, 22]: ac_ppp_voluntary_set_link_vectors() changing

vectors for Vp1
00:00:23.859: ACLIB [Vp1, 22]: SW AC intf PROVISIONED for PPP interface Vp1
00:00:23.859: Xconnect[unkn:#.#.#.#:#]: provisioning fwder with fwd_type=2,

sss_role=1
00:00:23.859: XC L2TP: XConnect provision re
00:00:23.859: Vp1 IPCP: Install route to #.#.#.#
00:00:23.863: L2TP:(Tnl#:Sn#)L2X s/w switching session unboun #.#.#.# vcid #,

Unprovisioned, VC state UP
00:00:23.863: XC L2TP: uid:116[#.#.#.#/#] Tell MIB that PW peer #.#.#.#, vcid

1 is UP
00:00:23.863: L2TUN APP: uid:116handle/176170Destroying app session
00:00:23.863: XC L2TP: Received L2TUN API message <Provision>
00:00:23.863: XC L2TP: uid:121[#.#.#.#/#] PW-MGMT: PW peer #.#.#.#, vcid 1
00:00:23.863: XC L2TP: uid:121[#.#.#.#/#] PW-MGMT: Reason [Provisioned]d
00:00:23.863: L2TP   #:#:#   : Received a SSM L2TP segment down event
00:00:23.863: ACMGR [Vp1, 22]: Receive <Circuit Unprovisioned> msg
00:00:23.863: ACMGR [Vp1, 22]: unprovision event, SIP state chg both up to

end, action is peer service disconnect
00:00:23.863: ACMGR [Vp1, 22]: Sent a sip service disconnect
```

Conditions Client-initiated xconnect L2TPv2 sessions

Workaround The problem was not observed in 12.4(9)T2

CSCse78963 Adopt new `default summer-time rules from EPA BADCODE BUG`

Symptom Starting in calendar year 2007, daylight savings summer-time rules may cause Cisco IOS to generate timestamps (such as in syslog messages) that are off by one hour.

Conditions The Cisco IOS configuration command: clock summer-time zone recurring uses United States standards for daylight savings time rules by default. The Energy Policy Act of 2005 (H.R.6.ENR), Section 110 changes the start date from the first Sunday of April to the second Sunday of March, and it changes the end date from the last Sunday of October to the first Sunday of November.

Workaround A workaround is possible by using the clock summer-time configuration command to manually configure the proper start date and end date for daylight savings time. After the summer-time period for calendar year 2006 is over, one can for example configure: clock summer-time PDT recurring 2 Sun Mar 2:00 1 Sun Nov 2:00 (this example is for the US/Pacific time zone)

`CSCsi06347 CLI for MOH should be displayed under voice-port`

Symptom CLI for MOH is hidden

Conditions Happens when signal loopstart live-feed is configured under voice-port.

Workaround There are no workarounds.

CSCsh98465 INFO request not generated on hookflash

Symptom INFO request messages is generated properly on hookflash

Conditions This feature is broken in 12.4(11)XJ based image

Workaround Currently there is no workaround.

CSCse24889 Malformed SSH version 2 packets may cause processor memory depletion

Symptom Malformed SSH version 2 packets may cause a memory leak, causing the platform to operate under a degraded condition. Under rare circumstances, the platform may reload to recover itself.

Conditions This symptom is observed on a Cisco platform that is configured for SSH version 2 after it has received malformed SSHv2 packets.

Workaround As an interim solution until the affected platform can be upgraded to a Cisco IOS software image that contains the fix for caveat

CSCse24889, configure SSH version 1 from the global configuration mode, as in the following example:

```
config t
ip ssh version 1
end
```

Alternate Workaround: Permit only known trusted hosts and/or networks to connect to the router by creating a vty access list, as in the following example:

```
10.1.1.0/24 is a trusted network that
is permitted access to the router, all
other access is denied

access-list 99 permit 10.1.1.0 0.0.0.255
access-list 99 deny any

line vty 0 4
access-class 99 in
end
```

Further Problem Description: For information about configuring vty access lists, see the *Controlling Access to a Virtual Terminal Line* document.

For information about SSH, see the *Configuring Secure Shell on Routers and Switches Running Cisco IOS* document:

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

CSCse98165 Mid-call invite not sent to OGW with nat symmetric check-media-src

Symptom IPIP gateway does not send an to the Originating gateway when a mid-call invite is received from the terminating gateway The following is configured on the IPIP gateway

sip-ua

nat symmetric check-media-src

Workaround There are no workarounds.

CSCsh74276 Counter for Lost packet not cumulative during a call

Symptom Packet loss counter varies randomly.

Conditions Sequence number goes wild.

Workaround There are no workarounds.

CSCek70160 UDP packet corrupted in SIP->H323 IPIPGW during T38 mode

Symptom In fax1 -- OGW --sip--- IPIPGW -- h323 -- TGW --fax2 scenario, T38 fax fails.

Conditions When "dtmf-relay rtp-nte digit-drop" is configured on IPIPGW and T38 is sent from fax1 to fax2.

Workaround There are no workarounds

CSCsh67943 7301 fails on a T38 when configured as IPIPGW doing SIP - H323

Symptom In fax1 -- OGW --sip--- IPIPGW -- h323 -- TGW --fax2 scenario, T38 fax fails.

Conditions When TGW is using v123-21 image, IPIPGW using 12.4(9)T image, T38 fails.

Workaround There are no workarounds.

CSCsi09696 CME SIP missed quotation for aop parameter

CSCsi18104 SIP: 400 Bad Request for AA's REFER, and AA's transfer failed

Symptom Seeing “400 Bad Request” response for AA’s “REFER” request, and AA’s semi-attended transfer failed against XJ1 image.

Conditions This happens when AA/CUE is configured to use **dtmf-relay sub-notify**.

Workaround **xfer** works if AA/CUE uses **dtmf-relay sip-notify**.

CSCek56688 Change after-hours login timer to 1 min

Symptom The minimum after-hours login timer is 5 mins. It is too long. Customer wants to be able to deactivate the login in 1 min.

Conditions The problem is observed when after-hours call blocking is enabled.

Workaround There are no workarounds.

CSCsg31867 Router crashes on large ping pkts with IPSEC/NAT configured

Symptom A Cisco IOS router may experience a unexpected reload.

Conditions This problem occurs in IOS version 12.4(11)T and later when the router is configured with IPSec and NAT, and when it needs to fragment a large packet to be encrypted over the IPSec tunnel.

Workaround There is no known workaround at this time.

CSCsh33057 SPEs in stuck state after stress

Symptom SPEs may hang after voice calls have been processed. When you enter the clear SPE command for the affected SPEs, the platform may reload unexpectedly.

Conditions These symptoms are observed on a Cisco AS5400 and Cisco AS5850.

Workaround There is no workaround to prevent the SPEs from hanging. When the SPEs hang, reload the platform to recover the SPEs.

CSCsg46624 Router crashes on applying service policy on the atm subinterface

Symptom Router crash

Conditions When a policy map is applied on the mohican point to point subinterface.

Workaround There are no workarounds.

CSCsh16540 Router Crashes when encapsulation dot1Q <VC id is enabled

Symptom A router crashes when you enter the encapsulation **dot1q vlan-id** command.

Conditions This symptom is observed on a Cisco 7200 series that runs Cisco IOS interim Release 12.4(12.7) and that is configured for MPLS. However, the symptom is platform-independent.

Workaround There is no workaround.

CSCsh83836 C1700 Router crashes @ fpm_db_add_acl

CSCsg80097 Calling name in Facility sent via CCM Sip trunk does not appear on SIP CME

CSCsh11157 Memory leak at DestCaptureCallForward

CSCsg40247 T38 Fax Relay calls are going as Cisco Fax Relay

CSCsi15229 No memory available if qos and acl on router

Symptom One or more of the following symptoms may occur. CPU HOGS, crashes, high cpu, and/or memory allocation failures.

Conditions This problem is triggered when making configuration changes to an access list that is currently in use by a service policy.

Workaround Disable the service policy before make changes to its components.

CSCsg14313 Traceback seen while making conference/transcoder co_exist calls

CSCsg57002 SIP timer tree corruption is causing SIP gateway crash under load

Symptom The SIP Gateway will crash when handling calls involving DTMF relay.

Conditions Following is the scenario that is causing the crash: sip-notify and sip-kpml are configured as DTMF relay mechanisms on both Cisco IOS Gateway and CCM. When a call is coming in from CCM onto the GW, because of a bug (CSCse72749), GW negotiates the DTMF mechanism as sip-notify whereas CCM negotiates the DTMF relay mechanism as sip-kpml. Subsequently, CCM sends subscribe request for KPML. GW accepts the KPML subscription and starts the respective KPML timers. Now when the call is terminated, Cisco IOS GW is cleaning up the data structures without stopping the KPML timers since the negotiated DTMF relay on Cisco IOS GW is sip-notify.

Workaround There are two workarounds:

1. Migrate to a Cisco IOS version which has CSCse72749 fix integrated.

2. Enable either sip-notify or sip-kpml on the Cisco IOS GW (do not enable both).

CSCsg34501 Traceback from voice_reg_supports_utf8 is seen

CSCsb79829 call dropped when incoming invite with alert-info header

CSCsg92387 Calling name in Notify message does not appear on SIP-CME Phone

CSCsh17599 One way audio with Adhoc conference by CCM and 1 participant hangs up

CSCsg36224 DSPs not released when conference DN no. is directly dialed

CSCsh32714 Spurious memory access traceback at sipSPI_ipip_copy_channelInfo_to_sdp

CSCsh57237 router crashes immediately after enabling service policy

Symptom Router crashes

Conditions Crash happens immediately or after a few seconds of applying service policy on the gigabit ethernet and atm pvc. The only commands executed after applying the service policy are write memory and show run.

Workaround There are no workarounds.

CSCsi24620 Enable support for StationUnicodeCapableMsk feature bit

Symptom UTF8 localized characters can not display on new generation phones, ex 7970, 7961 and etc.

Conditions When using phone load later than 8.0.x.

Workaround There are no workarounds.

Further Problem Description: If the locale on CME requires UTF8 encoding the character will not display correctly with 8.0.x and newer phone loads.

CSCsh11907 Router crashes @ fair_queue_classify_wred

Symptom Router crashes after show policy-map command

Workaround There is no workaround.

CSCsg03849 Spurious accesses traceback seen @ **AFW_Leg_CheckConsultSetup**

Open Caveats - Cisco IOS Release 12.4(11)XJ1

There are no open caveats in this release.

Resolved Caveats - Cisco IOS Release 12.4(11)XJ1

CSCsh23992: The ISDN status does not come up for Cisco IAD2801 BRI voice port

Symptom : The ISDN status of the voice port VIC2-2BRI-NT/TE-P on the IAD2801 router is always in deactivated state and disallows the link to come up. The interface does not take the **isdn layer1-emulate network** command (on the network side). Because the link does not come up, the user is unable to make any calls through the BRI ports.

Workaround : Configure VIC2-2BRI-NT/TE card on c2801 with the c2801-adventerprisek9-mz.12172006.

Cisco IOS Software Documentation Set

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

Additional References

Use these release notes with the documents listed in the following sections:

- Obtaining Documentation, Obtaining Support, and Security Guidelines
- Platform-Specific Documents

Release-Specific Documents

The following documents are specific to Release 12.4 and apply to Release 12.4(11)XJ. They are located on Cisco.com:

- *Cross-Platform Release Notes for Cisco IOS Release 12.4(11)T*, follow this path:
- *Caveats for Cisco IOS Release 12.4* and *Caveats for Cisco IOS Release 12.4(11)T*

Note If you have an account with Cisco.com, you can also use the Bug Toolkit to find selected caveats of any severity. To reach the Bug Toolkit, log in to Cisco.com, and go to: http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl.

Platform-Specific Documents

Hardware installation guides, configuration and command reference guides, and additional documents specific to the Cisco 2800 series routers are available on Cisco.com at the following location:

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/2800/index.htm

Cisco Feature Navigator

Cisco Feature Navigator is a web-based tool that enables you to quickly determine which Cisco IOS software images support a particular set of features and which features are supported in a particular Cisco IOS image. Feature Navigator is available 24 hours a day, 7 days a week.

To use Feature Navigator, you must have a JavaScript-enabled web browser such as Netscape 3.0 or later, or Internet Explorer 4.0 or later. Internet Explorer 4.0 always has JavaScript enabled. To enable JavaScript for Netscape 3.x or Netscape 4.x, follow the instructions provided with the web browser. For JavaScript support and enabling instructions for other browsers, check with the browser vendor.

Feature Navigator is updated when major Cisco IOS software releases and technology releases occur. You can access Feature Navigator at the following URL:

http://www.cisco.com/go/cfn Use these release notes with appropriate documents for your Cisco configuration.

Open Source License Acknowledgements

The following notices pertain to this software license.

OpenSSL/Open SSL Project

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

License Issues

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License:

Copyright © 1998-2007 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”.
4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:

   “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”.

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT “AS IS”' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License:

Copyright © 1995-1998 Eric Young (eay@cryptsoft.com). All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

   "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)".

   The word 'cryptographic' can be left out if the routines from the library being used are not cryptography-related.
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)".

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License].

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly What's New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain online documentation, troubleshooting tips, and sample configurations from online tools by using the Cisco Technical Assistance Center (TAC) Web Site. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC Web Site.

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