Release Notes for Cisco 2800 Series Integrated Services Routers with Cisco IOS Release 12.4(15)XZ

First Released: April 14, 2008
Last Revised: March 25, 2009
Cisco IOS Release 12.4(15)XZ2
OL-16638-02 Second Release

These release notes describe new features and significant software components for the Cisco 2800 series integrated services routers (ISRs) that support the Cisco IOS Release 12.4(15)XZ releases. These release notes are updated as needed. Use these release notes with the *Cross-Platform Release Notes for Cisco IOS Release 12.4T and About Cisco IOS Release Notes.*

For a list of the software caveats that apply to the Release 12.4(15)XZ releases, see the "Caveats" section on page 10. *See also Caveats for Cisco IOS Release 12.4(15)T.* The online caveats document is updated for every maintenance release.

Contents

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

© 2008-2009 Cisco Systems, Inc. All rights reserved.

System Requirements

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

Memory Requirements

Table 1 describes the memory requirements for the Cisco IOS feature sets supported by Cisco IOS Release 12.4(15)XZ on the Cisco 2800 series integrated services routers (ISRs).

Table 1 Required Memory for the Cisco 2800 series Integrated Services Routers (ISRs) with Cisco IOS Release 12.4(15)XZ

Platform	Image Name	Feature Set	Image	Flash Memory (MB)	DRAM (MB)
Cisco 2811 Cisco 2821 Cisco 2851	Cisco 2800 Advanced Enterprise Services	Enterprise Services	adventerprisek9-mz	64	256
	Cisco 2800 AISK9-AESK9 Feature Set Factory Upgrade For Bundles	AISK9-AESK9 Feature Set Factory Upgrade For Bundles		64	256
	Cisco 2800 ASK9-AESK9 Feature Set Factory Upgrade For Bundles	ASK9-AESK9 Feature Set Factory Upgrade For Bundles		64	256
	Cisco 2800 INT Voice/Video, IPIPGW, TDMIP GW AES	INT Voice/Video, IPIPGW, TDMIP GW AES	adventerprisek9_ivs-mz	64	256
	Cisco 2800 INT Voice/Video GK, IPIPGW, TDMIP GW AES, LI	INT Voice/Video GK, IPIPGW, TDMIP GW AES, LI	adventerprisek9_ivs_li-mz	64	256
	Cisco 2800 Advanced Enterprise Services With SNA Switching	Advanced Enterprise Services With SNA Switching	adventerprisek9_sna-mz	64	256
	Cisco 2800 Advanced IP Services	Advanced IP Services	advipservicesk9-mz	64	256
Cisco 2811 Cisco 2821 Cisco 2851	Cisco 2800 SPSK9-AISK9 Feat Set Factory Upgrade For Bundles	SPSK9-AISK9 Feat Set Factory Upgrade For Bundles		64	256
	Cisco 2800 ASK9-AISK9 Feature Set Factory Upgrade For Bundles	ASK9-AISK9 Feature Set Factory Upgrade For Bundles		64	256
	Cisco 2800 AISK9-AISK9 Feature Set Factory Upgrade For Bundles	AISK9-AISK9 Feature Set Factory Upgrade For Bundles		64	256
	Cisco 2800 Advanced Security	Advanced Security	advsecurityk9-mz	64	256
	Cisco 2800 ASK9-ASK9 Feature Set Factory Upgrade For Bundles	ASK9-ASK9 Feature Set Factory Upgrade For Bundles		64	256
	Cisco 2800 Enterprise Base w/o Crypto	Enterprise Base without Crypto	entbase-mz	64	256
	Cisco 2800 Enterprise Base	Enterprise Base	entbasek9-mz	64	256
	Cisco 2800 Enterprise Services w/o Crypto	Enterprise Services without Crypto	entservices-mz	64	256

Table 1 Required Memory for the Cisco 2800 series Integrated Services Routers (ISRs) with Cisco IOS Release 12.4(15)XZ (continued)

Platform	Image Name	Feature Set	Image	Flash Memory (MB)	DRAM (MB)
Cisco 2811 Cisco 2821 Cisco 2851	Cisco 2800 Enterprise Services	Enterprise Services	entservicesk9-mz	64	256
	Cisco 2800 SPSK9-ESK9 Feature Set Factory Upgrade For Bundles	SPSK9-ESK9 Feature Set Factory Upgrade For Bundles		64	256
Cisco 2811 Cisco 2821 Cisco 2851	Cisco 2800 IP Base without crypto	IP Base without Crypto	ipbase-mz	64	256
	Cisco 2800 IP Base	IP Base	ipbasek9-mz	64	256
	Cisco 2800 IP Voice without crypto	IP Voice without Crypto	ipvoice-mz	64	256
	Cisco 2800 INT Voice/Video, IPIP GW, TDMIP GW	INT Voice/Video, IPIP GW, TDMIP GW	ipvoice_ivs-mz	64	256
	Cisco 2800 IP Voice	IP Voice	ipvoicek9-mz	64	256
	Cisco 2800 SP Services	SP Services	spservicesk9-mz	64	256
	Cisco 2800 SPSK9-SPSK9 Feature Set Factory Upgrade For Bundles	SPSK9-SPSK9 Feature Set Factory Upgrade For Bundles		64	256

Table 1 Required Memory for the Cisco 2800 series Integrated Services Routers (ISRs) with Cisco IOS Release 12.4(15)XZ (continued)

Platform	Image Name	Feature Set	Image	Flash Memory (MB)	DRAM (MB)
Cisco 2801	Cisco 2801 IOS Advanced Enterprise Services	Advanced Enterprise Services	adventerprisek9-mz	64	192
	Cisco 2801 IOS AISK9-AESK9 Feature Set Factory Upgrade For Bundles	AISK9-AESK9 Feature Set Factory Upgrade For Bundles		64	256
	Cisco 2801 IOS ASK9-AESK9 Feature Set Factory Upgrade For Bundles	ASK9-AESK9 Feature Set Factory Upgrade For Bundle		64	192
	Cisco 2801 IOS SPSK9-AESK9 Feat set factory upgrade for bundles	SPSK9-AESK9 Feat set factory upgrade for bundles		64	192
	Cisco 2801 IOS INT Voice/Video, IPIPGW, TDMIP GW AES	INT Voice/Video, IPIPGW, TDMIP GW AES	adventerprisek9_ivs-mz	64	192
	Cisco 2801 IOS Advanced Enterprise Services SNA Switching	Advanced Enterprise Services SNA Switching	adventerprisek9_sna-mz	64	128
	Cisco 2801 IOS Advanced IP Services	Advanced IP Services	advipservicesk9-mz	64	128
	Cisco 2801 IOS SPSK9-AISK9 Feature Set Factory Upgrade For Bundles	SPSK9-AISK9 Feature Set Factory Upgrade For Bundles		64	192
	Cisco 2801 IOS ASK9-AISK9 Feature Set Factory Upgrade For Bundles	ASK9-AISK9 Feature Set Factory Upgrade For Bundles		64	192

Table 1 Required Memory for the Cisco 2800 series Integrated Services Routers (ISRs) with Cisco IOS Release 12.4(15)XZ (continued)

Platform	Image Name	Feature Set	Image	Flash Memory (MB)	DRAM (MB)
Cisco 2801	Cisco 2801 IOS AISK9-AISK9 Feature Set Factory Upgrade For Bundles	AISK9-AISK9 Feature Set Factory Upgrade For Bundles	advipservicesk9-mz	64	128
	Cisco 2801 IOS Advanced Security	Advanced Security	advsecurityk9-mz	64	128
	Cisco 2801 IOS ASK9-ASK9 Feature Set Factory Upgrade For Bundles	ASK9-ASK9 Feature Set Factory Upgrade For Bundles		64	192
	Cisco 2801 IOS Enterprise Base w/o Crypto	Enterprise Base w/o Crypto	entbase-mz	64	128
	Cisco 2801 IOS Enterprise Base	Enterprise Base	entbasek9-mz	64	128
	Cisco 2801 IOS Enterprise services w/o crypto	Enterprise services w/o crypto	entservices-mz	64	192
	Cisco 2801 IOS Enterprise Services	Enterprise Services	entservicesk9-mz	64	192
	Cisco 2801 IOS SPSK9-ESK9 Feat Set Factory Upgrade For Bundles	SPSK9-ESK9 Feat Set Factory Upgrade For Bundles		64	192
	Cisco 2801 IOS IP Base w/o Crypto	IP Base w/o Crypto	ipbase-mz	64	128
	Cisco 2801 IOS IP Base	IP Base	ipbasek9-mz	64	128
	Cisco 2801 IOS IP Voice w/o Crypto	IP Voice w/o Crypto	ipvoice-mz	64	192
	Cisco 2801 IOS INT Voice/Video, IPIP GW, TDMIP GW	INT Voice/Video, IPIP GW, TDMIP GW	ipvoice_ivs-mz	64	256
	Cisco 2801 IOS IP Voice	IP Voice	ipvoicek9-mz	64	192
	Cisco 2801 IOS SP Services	SP Services	spservicesk9-mz	64	192
	Cisco 2801 IOS SPSK9-SPSK9 Feature Set Factory Upgrade For Bundles	SPSK9-SPSK9 Feature Set Factory Upgrade For Bundles		64	192

Hardware Supported

Cisco IOS Release 12.4(15)XZ supports the following Cisco 2800 series routers:

- Cisco 2801
- Cisco 2811
- Cisco 2821
- Cisco 2851

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 2800 series routers, which are available at:

http://www.cisco.com/en/US/products/ps5854/tsd_products_support_series_home.html

Determining the Software Version

To determine the version of Cisco IOS software currently running on your Cisco 2800 series router, see *About Cisco IOS Release Notes* located at http://www.cisco.com/en/US/docs/ios/12_4/12_4x/12_4xy15/ReleaseNote.html.

Upgrading to a New Software Release

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

Feature Set Tables

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

New and Changed Information

This section contains the following information:

New Hardware Features in Cisco IOS Release 12.4(15)XZ2

There are no new hardware features in this release.

New Software Features in Cisco IOS Release 12.4(15)XZ2

There are no new software features in this release.

New Hardware Features in Cisco IOS Release 12.4(15)XZ1

There are no new hardware features in this release.

New Software Features in Cisco IOS Release 12.4(15)XZ1

There are no new software features in this release.

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

There are no new hardware features in this release.

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

The new software features are:

Configurable SIP Listening Port

This features provides users the ability to configure the port where SIP messages are listened to.

For more information, see:

http://cisco.com/en/US/docs/ios/voice/cube/configuration/guide/vb-gw-sipsip.html

SIP Video Support for Telepresence Calls

This feature allows the Cisco Unified Border Element to generate SIP INVITES that include SDP lines for both voice and voice media paths. This allows the Border Element to provide back-to-back user agent functionality for both voice and video calls. For more information, see:

http://cisco.com/en/US/docs/ios/voice/cube/configuration/guide/vb-gw-sipsip.html

Gatekeeper Enhancement: Support for extended InterZone Clear Token

Provides additional security to the gatekeeper by ensuring that ARQ and RRQ are not spoofed. For more information, see:

http://cisco.com/en/US/docs/ios/voice/cubegk/configuration/guide/ve_book/ve_book.html

Configurable SIP Parameter Modification

Allows users to change the standard SIP messages sent from the Cisco SIP stack for better interworking with different SIP entities. For more information, see:

http://cisco.com/en/US/docs/ios/voice/cube/configuration/guide/vb-gw-sipsip.html

Configurable Bandwidth Parameters for SIP Calls

This features provides the ability to manually configure the bandwidth that is signaled in the outbound SIP invite. For more information, see:

http://cisco.com/en/US/docs/ios/voice/cube/configuration/guide/vb-gw-sipsip.html

SIP - Ability to Send a SIP Registration Message on a Border Element

This feature provides a new command configured under the SIP-UA that allows the Border Element to send a REGISTRATION command to a SIP REGISTRAR. For more information, see:

http://cisco.com/en/US/docs/ios/voice/cube/configuration/guide/vb-gw-sipsip.html

SIP Delayed Offer to Early Offer for Video Calls

This feature allows a SIP delayed offer video call to be translated into a SIP early offer video call when traversing the Cisco Unified Border Element. For more information, see:

http://cisco.com/en/US/docs/ios/voice/cube/configuration/guide/vb-gw-sipsip.html

SIP - Support for SIP Video Calls with Flow Around Media

This feature allows a SIP video call media flow around the Cisco Unified Border element. Previous support was for call scenarios where the media flowed through the Border Element. For more information, see:

http://cisco.com/en/US/docs/ios/voice/cube/configuration/guide/vb-gw-sipsip.html

SIP - Support for SESSION REFRESH with reINVITEs

This feature expands the ability of the Cisco Unified BE to control the session refresh parameters and ensure the session does not time out. For more information, see:

http://cisco.com/en/US/docs/ios/voice/cube/configuration/guide/vb-gw-sipsip.html

New Features in Release 12.4T

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

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 - Release 12.4(15)XZ2

There are no open caveats in this release.

Resolved Caveats - Release 12.4(15)XZ2

- CSCsv04836

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

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

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

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

CSCsr16693

A series of TCP packets may cause a denial of service (DoS) condition on Cisco IOS devices that are configured as Easy VPN servers with the Cisco Tunneling Control Protocol (cTCP) encapsulation feature. Cisco has released free software updates that address this vulnerability. No workarounds are available; however, the IPSec NAT traversal (NAT-T) feature can be used as an alternative.

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

Note: The March 25, 2009, Cisco IOS Security Advisory bundled publication includes eight Security Advisories. All of the advisories address vulnerabilities in Cisco IOS Software. Each advisory lists the releases that correct the vulnerability or vulnerabilities in the advisory. The following table lists releases that correct all Cisco IOS Software vulnerabilities that have been published in Cisco Security Advisories on March 25, 2009, or earlier.

http://www.cisco.com/en/US/products/products_security_advisories_listing.html

CSCsu21828

A series of TCP packets may cause a denial of service (DoS) condition on Cisco IOS devices that are configured as Easy VPN servers with the Cisco Tunneling Control Protocol (cTCP) encapsulation feature. Cisco has released free software updates that address this vulnerability. No workarounds are available; however, the IPSec NAT traversal (NAT-T) feature can be used as an alternative.

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

Note: The March 25, 2009, Cisco IOS Security Advisory bundled publication includes eight Security Advisories. All of the advisories address vulnerabilities in Cisco IOS Software. Each advisory lists the releases that correct the vulnerability or vulnerabilities in the advisory. The following table lists releases that correct all Cisco IOS Software vulnerabilities that have been published in Cisco Security Advisories on March 25, 2009, or earlier.

http://www.cisco.com/en/US/products/products_security_advisories_listing.html

CSCsv38166

The server side of the Secure Copy (SCP) implementation in Cisco IOS software contains a vulnerability that could allow authenticated users with an attached command-line interface (CLI) view to transfer files to and from a Cisco IOS device that is configured to be an SCP server, regardless of what users are authorized to do, per the CLI view configuration. This vulnerability could allow valid users to retrieve or write to any file on the device's file system, including the device's saved configuration and Cisco IOS image files, even if the CLI view attached to the user does not allow it. This configuration file may include passwords or other sensitive information.

The Cisco IOS SCP server is an optional service that is disabled by default. CLI views are a fundamental component of the Cisco IOS Role-Based CLI Access feature, which is also disabled by default. Devices that are not specifically configured to enable the Cisco IOS SCP server, or that are configured to use it but do not use role-based CLI access, are not affected by this vulnerability.

This vulnerability does not apply to the Cisco IOS SCP client feature.

Cisco has released free software updates that address this vulnerability.

There are no workarounds available for this vulnerability apart from disabling either the SCP server or the CLI view feature if these services are not required by administrators.

This advisory is posted at the following link:

http://www.cisco.com/warp/public/707/cisco-sa-20090325-scp.shtml.

CSCsu11522

A vulnerability exists in the Session Initiation Protocol (SIP) implementation in Cisco IOS software that can be exploited remotely to cause a reload of the Cisco IOS device.

Cisco has released free software updates that address this vulnerability. There are no workarounds available to mitigate the vulnerability apart from disabling SIP, if the Cisco IOS device does not need to run SIP for VoIP services. However, mitigation techniques are available to help limit exposure to the vulnerability.

This advisory is posted at the following link:

http://www.cisco.com/warp/public/707/cisco-sa-20090325-sip.shtml.

CSCsr29468

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

Cisco has released free software updates that address this vulnerability.

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

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

CSCsq09424 Few headers are duplicated when configured in passthru-hdr list and pass.

Symptom In a CUBE, when headers may be passed through from the incoming side of a call to the outgoing side, there are certain headers which may be added multiple times.

Conditions When Max-Forwards, Server, Allow, or Allow-Events headers are passed through in an INVITE, INVITE response, CANCEL, or ACK, multiple instances of the header may occur.

Workaround None.

Further Problem Description: This problem occurs because a header is being passed through a CUBE from the OGW to the TGW in an IP-IP call. This results in outgoing SIP messages which are syntactically invalid, and may result in failures depending on the SIP implementation on the receiving end.

CSCsr78883 Router console displays messages "Data corruption Data Inconsistency.

Symptom There will be traceback on configuring **mls qos cos pass-through dscp** in supporting interface mode.

Conditions Configuring **mls qos cos pass-through dscp** in the interface that supports the functionality.

Workaround Currently, the CLI is not supported in the most network modules, and thus, invisible to the users. If the CLI is supported, configure it as **mls qos cos override | cos-value.**

Further Problem Description: Due the buffer overflow, there will be traceback when configuring the QoS in the supporting interface. Currently, the CLI is not supported in the most network modules, and thus, invisible to the users.

CSCsr06874 2800 periodically crash on CMM_CRS functions.

Symptom Periodical crashes on 2800 with CME features.

Conditions When **callmonitor scan** is configured.

Workaround Turned off **callmonitor scan.**

CSCsq50366 Last digit getting truncated when prefix is set to its max value of 32.

Symptom Last digit getting truncated when prefix is configured with a length of 32 under the dial-peer.

Conditions When the prefix is configured with a length of 32 under the dial-peer only 31 digits are being sent across and the calls fails as there is no matching dial-peer at the other end. When the prefix is configured for 31 digits, then all the digits are sent correctly and the call is successful.

This is seen in the following call scenario:

1. Configure E1R2 ds0 groups between callgen and UUT:
2. Callgen calls into the UUT using ds0-group1.
3. The UUT has DID configured.
4. The UUT directs the call to ds0-group2 which is connected back to callgen.
5. Callgen has DID configured for the incoming call.
6. Callgen directs the call to ds0-group3 which is connected back to the UUT
7. The uut establishes a VoIP call leg back to callgen.

Workaround None.

CSCsr68545 Error %DATACORRUPTION-1-DATAINCONSISTENCY when running ipsla with rtt.

Symptom Error message occurs:

000302: Jul 24 13:00:13.575 CDT: %DATACORRUPTION-1-DATAINCONSISTENCY: copy error -Traceback= 0x410FD1A4 0x41119DB0 0x41138324 0x41DE5714

Conditions IP SLA configured with RTT.

Workaround None.

CSCsr27960 Traceback observed after configuring credential under sip-ua.

Symptom Traceback observed when configuring credentials CLI under sip-ua.

Conditions This happens when user configures credentials CLI with username length more than 32 characters.

Workaround None.

CSCso58935 Caller ID still display Barge for point-to-point call between sccp share.

Symptom Caller ID still display To Barge for point to point call between two sccp shared line phones after the other party drops out from cBarge conference.

Workaround None.

CSCsr14658 CLI Cannot handle Double quotes.

Symptom CME 4.3. IOS 12.4.15XZ SP Services. Under telephony-service the following url services was configured:

http://10.1.1.1 "My service"

Note the quotes. On the running config you see the above command without the quotes and everything works fine. When you type **wr,** then you again see the same command without the quotes. The issue is that, when you reload the router, the command is there, but it is not accepted and you have to type it again. Also, if you type **url services http://10.1.1.1 My service**, then you get an error of invalid input.

Conditions Normal operation.

Workaround Use one word and underscore instead of space.

CSCsq48167 CME DN **description** command may allow for open-ended quote delimination.

Symptom The CME **description** command under the ephone-dn potentially allows for the description string to be saved to the router configuration without a trailing quote. This leaves an open-ended delimination in the configuration for the description string, and will cause the CME GUI to fail to load with an "unterminated string constant" error.

Conditions There are two ways that the configuration can get a description with no closing quote:

1. Description is entered with quotes on both sides, and total string length is between 33 and 40 characters.

   Entering

   Router(config)#ephone-dn 1

   Router(config-ephone-dn)#description "012345678901234567890123456789123 45"

   Appears as

   ephone-dn 1

   description "01234567890123456789012345678912

2. Description is entered with quotes only on beginning of string.

   Entering

   Router(config)#ephone-dn 1

   Router(config-ephone-dn)#description "test

   Appears as

   ephone-dn 1

   description "test

Enter the description without any quotes via the CLI.

Open Caveats - Release 12.4(15)XZ1

There are no open caveats in this release.

Resolved Caveats - Release 12.4(15)XZ1

- CSCsq58779

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

  Cisco has released free software updates that address this vulnerability.

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

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

Symptom After Reload Secure Conference profile does not register with CCM

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

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

CSCsm71666 eem changes for LLP64 in mcp_dev

CSCsh23090 Police action cannot be allowed for a policy to be attached to self zone

Symptom Police action gets configured on a policy associated to self zone.

Conditions This symptom is observed only when the user tries to edit a policy associated to self zone to include police action. Associating a policy configured with police action to self zone will fail.

Workaround Do not configure police action to a policy when it is associated to self zone.

CSCsk42373 Memory leak in ctid_set_changetime function

Symptom Memory leak is observed after the device boots up. 'sh mem debug leaks chunks' will show the leak. The memory leak shows up against "SNMP SMALL CHUNK" as the memory is allowed by MakeOctetString, called from reg_invoke_ctid_get_octet_string.

CSCsl08086 Ping Traffic Dropped: Dialer based PPPoE

CSCsl26908 ASSERTION FAILED: file "../les/if_les_bri_i3081.c", line 744

Symptom Assertion message displays.

CSCsl99275 High CPU on 5400XM when doing show flash

Symptom High CPU can be seen on Cisco AS5400XM after given uptime.

Conditions Occurs after 2-3 weeks uptime. CPU usage increases because of "Background Loade" process.

Workaround Reload the access server.

CSCsm34706 CUBE sends fixed DTMF duration and ignores received H.245 User Input

Symptom CUBE sends a fixed 800 time units for every digit pressed (sent via RFC 2833) regardless of what it receives in the duration of a H.245 User Input field.

Conditions In H323-SIP networking scenario on CUBE, for DTMF conversion from h245-alphanumeric to RFC2833, regardless of the duration received in H.245 User Input field, CUBE always sends a fixed 800 ms for every digit pressed (sent via RFC 2833).

Workaround There is no workaround.

CSCsm37093 CME 4.1after security is enabled 7970 will register with US locale

Symptom After security is enabled locale in the phone 7970 cannot be changed.

Conditions User cannot leave security enabled as the user cannot configure their locale.This issue is not seen in 7960 and 7940 as they have the firmware locally stored (flash).

Workaround There is no workaround.

CSCsm64258 ephone-hunt group does NOT present calls to overlaid DNs

Symptom When an ephone hunt-group is configured with 'present-call idle-phone', the ephone hunt-group skips the DNs which are configured as overlay.

Conditions The problem is observed when the ephone hunt-group is configured with 'present-call idle-phone' and DN is configured as overlay.

Workaround Remove the 'present-call idle-phone' configuration from the ephone-hunt and do not use overlaying.

CSCsm69056 IEC error (Software Error) seen on CME & CUBE when doing Call Fwd No Ans

Symptom CME and CUBE may display the following error message when forwarding a call. "CCAPI: Internal Error (Software Error)"

Conditions The error may display if this is Call Forward No Answer.

Workaround There is no workaround.

CSCsm74560 sdatar phone does not look for network locale file for user defined languages

Symptom Wireless IP phone 7920 doesn't download the 7960-tones.xml files when user defined network locale is configured

Conditions CME writes incomplete XML tags in the phone config file, for user defined language network locale. So phone cannot generate the query for the relevant network locale file.

Workaround Along with User defined, we also need to define inbuilt network locale.

For example DE - Germany

telephony-service

network-locale DE

create cnf-files

Now rename the user defined file to 'germany_7960-tones.xml'

Replace the file under ITS directory with the new 'germany_7960-tones.xml' (Make sure the name is the system defined name)

DO NOT run 'create cnf-file' as it will again override with the system defined parameters

Reboot the 7921 wireless phone

In case if you have to issue 'create cnf-file', then ensure to repeat all the steps mentioned above again.

CSCsm88771 CME trunk optimized calls being put on hold automatically

Symptom Answering a trunk call transferred from another phone is automatically put on hold and cannot be resumed.

Conditions The call originally came in on a trunk dn and is transferred to another extension on a phone sharing that trunk. Trunk optimization takes place.

Workaround There is no workaround.

CSCsm89158 7921 does not display call park number while the call is parked

Symptom 7921 does not show the parked number when the call is parked.

Conditions UC520W-16U-4FXO-K9 and 7921(CP7921G-1.0.3.LOADS)

Workaround There is no workaround.

CSCso45208 Unable to specify ephone-hunt extensions in ascending order

Symptom Cannot set ephone-hunt list members in certain orders during configurations.

Conditions If there are multiple ephone-dn w/ different preference matches one ephone-hunt list member and the preference difference among one ephone-hunt member + number of ephone-hunt list members >10.

Workaround There is no workaround.

CSCso48788 ActiveLine not reset back to 0 when offhook timer expired

Symptom When the phone is onhold call and if you press another button to seize a new call but left offhook till timer expired (the seize call will back onhook), the button become un-usable after that.

Conditions Put call onhold and offhook another line.

Workaround Seize another button.

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

Symptom Bad Refcount with tracebacks.

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

Workaround There is no workaround.

CSCso64585 redundant CallRemoteMultiLine sccp msg to monitor park DN

Symptom Jitter or voice quality issue may occur.

Conditions If there are a lot of ephones, say there are 50, monitoring same park DN, there will be 2500 same sccp messages sent to these 50 phones respectively in few mili seconds.

Workaround There is no workaround.

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

Symptom Different SSRC in RTCP compared to RTP after transcoding.

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

Workaround There is no workaround.

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

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

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

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

CSCso74656 MG2:device-based BLF shown incorrect status for EM

CSCso75055 SysObjID Missed in SR 520 Routers

CSCso78702 7961 IP Phone acct softkey get "no park number available"

Symptom 2851 Version 12.4(15)T4 press the ACCT SoftKey and get "NO PARK NUMBER AVAILABLE".

CSCso79611 cBarge:Traceback found at x40C66334:SkinnyHWConfAPI(0x40c628c0)+0x3a74

Symptom Trace back appears while doing transfer of barge call from barge initiator to a SIP phone.

Conditions This is observed during transfer of barge call between SCCP & SIP phone.

Workaround There is no workaround.

CSCso82469 Improper message displayed when user tries to create new mail

Symptom When the user tries to create new mail and OWA displays an improper message like the "page cannot be displayed".

Workaround There is no workaround.

CSCso83726 Ignore CFA for voice hunt-groups similar to ephone-hunt

Symptom Call Forward setting are NOT ignored for members of "voice hunt group" on Cisco Unified Communications Manager Express.

Conditions When phones are member of "voice hunt group" and call forward is enabled.

Workaround There is no workaround.

CSCso83948 Tracebacks pointing to CS_ProcessRerouteFailure - No release note enclosure

CSCso88429 CME/CUBE rejects incoming SIP INVITE if Max-Forwards > 70

Symptom CME or CUBE will reject an inbound SIP INVITE if Max-Forwards is greater than 70.

Conditions The Max-Forwards header field in SIP INVITE is greater than 70.

The Max-Forwards header field must be used with any SIP method to limit the number of proxies or gateways that can forward the request to the next downstream server. This can also be useful when the client is attempting to trace a request chain that appears to be failing or looping in mid-chain. The Max-Forwards value is an integer in the range 0-255 indicating the remaining number of times this request message is allowed to be forwarded. This count is decremented by each server that forwards the request. The recommended initial value is 70. This header field should be inserted by elements that can not otherwise guarantee loop detection. For example, a B2BUA should insert a Max-Forwards header field.

Workaround There is no workaround.

CSCso89001 Reload Steeler cause LWAPP AP change BOOT to autonomous mode

Symptom When AP is in LWAPP mode and C880 reloads, C880 first comes up, console session to AP right away, you can see AP displays invalid license messages. Also show boot on AP points to an autonomous image.

Conditions The Cisco 880 router reloads. When Access Point reloads in LWAPP mode, Access Point boot may also points to autonomous image.

Workaround When AP is in LWAPP mode and show boot on AP points to autonomous image, after AP reboot, AP goes back to autonomous mode. AP needs to go through LWAPP upgrade process, namely via recovery image to finally go back to LWAPP mode.

CSCso95643 sRTP Package missing in c1861

Symptom MGCP srtp-package option is not available in c1861 platform.

Workaround This occurs only on Cisco1861.

CSCso99426 Ringing delay of approx 3 secs on some ephones of blast hunt grp

Symptom 3 sec delay experienced in some ephones as hunt group members with shared DNs/monitor DN's

Conditions This occurs if ephones have shared DN's/monitor buttons.

Workaround There is no workaround.

CSCsq01339 CME - increase support for local entries to 250

CSCsq07606 Blast:Memory leak at AFW_application ivr: rerouteNumber SSrerouteInfo_t

Symptom Memory leak at AFW_application ivr: rerouteNumber SSrerouteInfo_t

Conditions 1) Two parallel hunt groups are created & final number on one parallel hunt group is configured with call forward all to pilot number of second hunt group. 2) Call from ephone 1 to 2 and ephone 2 answers and gets connected. Now from ephone 2 do blind transfer call to pilot # of first hunt group with 32 numbers. 3) All 32 phones will ring & upon no answer, the call is forwarded to final number which is configured with call forward all to the pilot number of second hunt group. 4) All the phones in the second hunt group rings and the first phone in the list answers the call.

Workaround There is no workaround.

CSCsq10768 Intermittent Live-Record failure in CME

Symptom Random failure of Live-Record functionality in CUCME may be observed. The phone indicates a message "Live Record Failed!".

Conditions This is observed on IOS version 12.4(15)XZ.

Workaround Disconnect that active voice call, re-establish voice call between same parties and attempt Live-Record again.

CSCsq15064 RDT: crash seen with null pointer during reload on C860w (with AP)

Symptom On steelers, issues command reload and say 'yes' to reload AP, the system crash.

Conditions . This occurs only when reload command is issued with AP in reload.

Workaround Do a reset command and continue the reload process. There is no service impact as Steelers and AP are going through reload.

CSCsq15847 Watch button can't exist with normal dn and causes no ringing.

Symptom The phone may not ring if the incoming call is designated to the overlaid DN which is also configured on other button as a W or M button.

Conditions A DN is configured on both overlay button and W or M button.

Workaround There is no workaround.

CSCsq17862 CME 4.3/ TSP Caller ID not displayed in TAPI client

Symptom The Caller ID is not displayed on UCC client when using CME 4.3. When the IP phone is tied to UCC, it displays the Caller ID.

Conditions This is observed in CME 4.3.

Workaround Use CME 4.2 or earlier.

CSCsq25714 present-call should not be an option for CLI callqueue

Symptom The CLI "present-call" is available under "callqueue". It is shown outside of the ephone-hunt.

Conditions After configuring present-call under ephone-hunt, the NVRAM would show it also outside of the ephone-hunt.

Workaround There is no workaround.

CSCsq26111 Name for the line or speeddial button may be truncated by SRST

Symptom The extension number and speed dial number may not be displayed in full length on a fallback ephone.

Conditions The number is display incorrectly after an ephone falls back to the SRST.

Workaround There is no workaround.

CSCsq31077 Router crash at bootup, trace ending in cce_dp_policy_get_class_instance CSCsq33020 hall c88x machine check exception information

Symptom Router crashes if the same inspect policy is applied to more than 7 zone-apirs.

Workaround The crash happens when the same policy is applied on more than 7 different zone-pairs. So the work around is to create another copy of 'GLOBAL-POLICY'(say GLOBAL-POLICY-DUP) and apply GLOBAL-POLICY on the first 7 zone-pairs and GLOBAL-POLICY-DUP on the next 7.

CSCsq36422 URLF:need have unified deny-page format for different browsers

Symptom The display of deny-page is different with different browsers.

Conditions Deny-page in IE doesn't indicate the real reason for this URL.

Workaround There is no workaround.

CSCsq39195 Apply QE_QMC patch to Steelers data BRI

Symptom New FPGA to solve Steelers BRI lock up issue.

Conditions VLAN traffic.

Workaround There is no workaround.

CSCsq41137 max-reserved-bandwidth config is lost after reload

Symptom max-reserved-bandwidth is removed upon reload.

Workaround add the command back in manually.

CSCsq41189 Memory Leak - "Presence Process"

Symptom Memory Leak with "Presence Process", this could lead to router crash.

Workaround There is no workaround.

CSCsq42134 JPN: 7921 XML Services are displayed as squares

Symptom 7921 directories are displayed as squires in CME Userlocale: JP environment.

Conditions 7921: 1.1.1, CME: 4.2 (IOS 12.4(11)XW7), Locale File: CME-locale-jp_JP-4.1.0.1.tar

Workaround There is no workaround.

CSCsq42153 Move up CCE Firewall switching path hook next to CCE Post NAT

Symptom Firewall classification is done prior to few other features.

Conditions FW is configured on the box.

Workaround There is no workaround.

CSCsq42689 JPN: XML parse error when accessing My Phone Apps > Speed Dial Buttons

CSCsq49894 SIP TNP phone fails to ring after receiving INVITE message

CSCsq51090 DSPware 23.6.1 Release IOS Commit

CSCsq51500 TTI petitioner page fails to bring up when using ezsdd/welcome

Symptom 7970 SIP phone fails to ring and connect after receiving INVITE message.The SCCP phone involved in the scenario registers fine. The 7970 SIP phone gets registered initially, but later the dial-peer does not come up so the phone un-registers.

Conditions OODR call is being made between a SCCP phone and a SIP 7970 phone.

Workaround There is no workaround.

CSCsq52296 Overlay numbers are ignored on single button extension mobility phones

Symptom Overlay numbers are ignored.

Conditions Apply voice profile on single button phones.

Workaround There is no workaround.

CSCsq54601 SCCP&SIP Registration failure with Ezvpn and NAT

Symptom SCCP&SIP Registration failure with Ezvpn and NAT.

Conditions When SCCP Registration traffic is passing through NAT Router. This affects the Voice traffic.

Workaround There is no workaround.

CSCsq54690 dx 3G modem sw locking: remove the Generic GSM SKU id support

CSCsq56103 Service-policy is not attached with priority by removing in serial int

Symptom Causes configuration issues for serial interface.

Conditions -When a strict policy is applied on a serial interface, if the user re-configures the strict priority configuration under the same class in the same policy, it will fail.

Conditions -

Conditions When the user tries to remove the service policy from the serial interface. The HQF data structure is not cleaned up. (i.e. the class default blt and physical interface blt are not deleted.)

Workaround There is no workaround.

CSCsq62269 3270 crash if no startup configuration

Symptom If 3270 has no startup configuration, it will crash by following or terminating the auto install.

Conditions No startup configuration and c3270-adventerprisek9-mz.124-15.XZ.bin.

Workaround Execute tftpdnld -r in rommon to boot c3270-entbase-mz.124-15.XZ.bin. Say no to auto install. Save the default configuration and reboot it with c3270-adventerprisek9-mz.124-15.XZ.bin.

CSCsq64715 EM login credential could be set to stack junk in error condition

Symptom EM login username and password may be set to random values in process stack in case the actual input from the phone is in an invalid format. And if both string picked up from the stack happened to match a username/password pair in a configured user profile, EM will login the user accidentally.

Conditions This is seen as normal behavior.

Workaround There is no workaround.

CSCsq74767 CME transfers hold to different phone with overlay on Stimulus message

Symptom A call put on hold is picked up by another user in an overlay situation.

Conditions The phone that held the call, and the phone that picked up the call, are on same overlay configuration lines. The call also has to be on the last dn of the overlay set.

Workaround Transfer the call back to the original party.

CSCsq90567 TSP gets stuck at connected state when a shared dn is resumed

Symptom The TSP gets stuck in connected state.

Conditions After resuming an onhold shared DN from the associated ephone, the TAPI gets stuck.

Workaround There is no workaround but you can reboot the ephone and the TAPI.

CSCsq92958 Typical intercom ext # not added to voice-logout profile

Symptom Numbers with alphabetic characters are ignored in EM profile.

Conditions This behavior is normal.

Workaround Use numeric numbers in EM profile.

CSCsq93564 Only 8 button are available for phones with addon module 7914/7915/7916

Symptom When 7975 (7965) IP phone with add-on module (7914/7915/7916) fallback to SRST4.3, only 8 (6) lines are available during SRST fallback.

Conditions This problem occurs when phones which register on Call Manager 6.1 fallback to SRST4.3.

Workaround There is no workaround.

CSCsq94677 SRST4.3 The last channel of all DNs is invalid after 2nd fallback

Symptom The 2nd channel for a dual-line DN or the 8th channel for octo-line DN is not available for a fallback phone.

Conditions This problem occurs when a phone falls back to the SRST the 2nd time after the SRST reboots.

Workaround There is no workaround.

CSCsr02593 incoming call wrongly ring SCCP overlay because of memory corruption

Symptom An incoming call for DN 2 rings both the SCCP phone A which has the DN and another SCCP phone B without it but has an overlay line. DN 2 and overlay line aren't shared line. Incoming call for the overlay only rings the overlay but incoming call for DN 2 will ring both.

Workaround Remove the overlay button from phone B, restart it, make an incoming to DN 2, add the overlay button back, restart phone. However, the problem will happen again after reload.

CSCek78623 ISSU infra test using expect & SESUT

CSCsg56685 Handle review comments about PRR#126487

CSCsj42809 GLBP flaps after SSO (fix: RF_PROG_ACTIVE_FAST; proc priority)

CSCsj46764 ancaz VLAN Manual LB - HA Support

CSCsj55804 HSRP flaps after SSO with 100 peers and default timer

CSCsk11684 Remove unused MRIB RP proxy code

CSCsk25878 alignment error flow_exp_v9_adjust_length flow_common_send_data

Symptom An alignment error may occur. This can cause a crash on certain routers and a traceback on others.

Conditions This symptom is observed when using the v9 export protocol with Flexible Netflow.

Workaround There is no workaround.

CSCsl32593 IPv6 SLA: Need to add flow_label to in6_pktinfo for the responder

CSCsl50516 FNF possible alignment errors when wring v9 header

Symptom An alignment error may occur, which may also lead to crash.

Conditions This symptom is observed when using the v9 export protocol with Flexible Netflow. Sending FNF export packets may cause this problem to be seen.

Workaround There is no workaround.

CSCsm12905 FNF: monitor can not be removed when interface removed

CSCsm54873 EEM some time are not triggered properly

Symptom Embedded Event Manager (EEM) rules may not trigger properly when performing SIP OIR.

Conditions EEM policies that interact with the IOS CLI through the command

Conditions action command and EEM TCL policies that use the CLI library may not interact properly when triggered. Incorrect sequencing with the IOS CLI may result when the policies are triggered resulting in the IOS CLI commands not being invoked.This problem exists on all shipped versions of IOS XE.

Workaround There is no workaround.

Further Problem Description: This can impact customers that use the Embedded Event Manager with EEM applets or policies that interact with the CLI. It was seen on the ASR platform and other platforms when "sched heapchecks process" was enabled. A timing issue can cause EEM action CLI commands to not coordinate with the IOS exec properly.The SIP2 is probably related to the ASR platform. An OIR event issued to trigger the specific EEM policy. This should occur with any EEM type policy however.

SXF is not impacted by this bug.

CSCsm58164 Default publish timers are not set properly when configured.

CSCsm62598 EEM action cns_event missing from Tcl action list.

CSCsm83056 FNF - FLOW MON: '<name>' could not setup cache control plane

CSCsm84550 WI08: Unable to remove eem cli event by using 'no event cli'

Symptom Unable to remove EEM cli event by using 'no event cli'.

Conditions When using EEM CLI ED to create a EEM APPLET. This is EEM CLI ED only issue. No other EDs i.e. applets using other EDs are effected.

Workaround This is EEM 2.4 issue only.

CSCsm84550 WI08: Unable to remove eem cli event by using 'no event cli'

CSCso01595 VS2: ~ 31000 Remote registry calls with VIRTUAL_SW:79 in fh_server.proc

CSCso17255 FNF - IPv6 payload chunk has arbitrary data after the end of the payload

CSCso29011 MF:Ipv6 mtu isn't restricted by smaller L2 mtu, becomes invalid after

CSCso32575 Move issue, chkpt and rf client ids to true component system-id

CSCso39518 fh_policy_dir.proc process crash when activate 0E patch

Symptom Before applying patch with EEM policy dir subsystem in it, there is one or more EEM applets configured, after the patch is activated, trigger an EEM applet.

Unconfigure all the EEM applet config before patching, then apply all the EEM applet config after activate the patch.This would lead to (fh_policy_dir.proc)process crash, not a device crash. This bug is specific to modular IOS image.

Workaround There is no workaround.

CSCso43772 Adding matched syslog info to syslog ED

CSCso50752 Buffer size should match the msg queue size in the syslog ED

CSCso53727 Need to add new hm test in diags to test LTL memory consistency

CSCso57084 improve "Process Forced Exit" console message

CSCso70327 C2W2: process deadlock encountered during ISSU rollback

CSCso76885 call-home diagnostic message is sent for every diag HM failure

CSCso83318 EEM: Build failure in v2,3

CSCso99953 /vob/cisco.comp/ipv6_forwarding/icmp/src/ipv6_icmp.c:memory leak

Open Caveats - Release 12.4(15)XZ

CSCso39750- router crashes at socket_inherit_fd after no ccm sccp

CSCsm65870- Excessive CCE dp feature memory leak as uut stressed at 99% cpu

CSCso21397- TB@ const_mfib_lc_free after peer router crashed

CSCso66410- software reload while reconfiguring bandwidth under policy map

Resolved Caveats - Release 12.4(15)XZ

CSCsl62609

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

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

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

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

CSCso57523- Call from SIP trunk to route point fails due to MALLOC failure

Symptom No audio and memory allocation failures when an incoming call through SIP trunk is connecting to route point(AA/ICD).

Conditions This is seen on C3845 in CME interoperating with UCCX.

Workaround To use PSTN trunks for incoming calls to CME.

CSCsm15782 -CCE-FW: Class-map with 'match class-map' does not seem to match traffic

Symptom Traffic may not match a class which contains 'match class-map' statement.

Conditions The traffic is expected to match a nested class inside a class-map.

Workaround Do not do nested class-map.

CSCsm72881- Router crashes after removing ipv6-address

CSCso14297 -parser validation is wrong for usb-devices with most of the CLIs

CSCsm31048- CTM server does not compile with CTC 9.0

CSCsm17819- Need number of temp sensor return to host

CSCsq15064 RDT: crash seen with null pointer during reload on C860w (with AP)

Symptom On steelers, when you issue a reload command and say "yes" to reload AP, the system crashes.

Conditions It occurs in a rare case and happens only when reload command is issued with AP in reload.

Workaround Reset the command and continue the reload process. There is no service impact as Steelers and AP are going through reload.

Additional References

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

- Release-Specific Documents
- Platform-Specific Documents

Release-Specific Documents

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

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

Platform-Specific Documents

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

http://www.cisco.com/en/US/products/ps5854/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 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.

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.

CCDE, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0812R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2008-2009, Cisco Systems, Inc. All rights reserved.