Release Notes for Cisco Signaling Link Terminal with Cisco IOS Release 12.4(15)XZ

First Released: February 24, 2009
Last Revised: Decmeber 2, 2010
Cisco IOS Release 12.4(15)XZ2
OL-19160-02 First Release

These release notes for the Cisco Signaling Link Terminal support Cisco IOS Release 12.4(15)XZ. 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 4. *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

Introduction

The Cisco Signaling Link Terminal (SLT) enables service providers to reliably transport SS7 protocols across an IP network. The Cisco SLT uses the Cisco IOS SS7 Signaling Link Terminal feature set, providing reliable interoperability with the Cisco Media Gateway Controller. The Cisco SLT is responsible for terminating the Message Transfer Part (MTP) 1 and MTP 2 layers of the SS7 protocol stack. Using the Cisco Reliable User Datagram Protocol (RUDP), the Cisco SLT backhauls, or transports, upper-layer SS7 protocols across an IP network to the Cisco Media Gateway Controller (Cisco VSC3000 or Cisco SC2200).

In combination with this application-specific version of the Cisco IOS software, the Cisco SLT hardware component leverages the widely deployed Cisco 2600 series multiservice access router. The Cisco 2600 series, driven by a powerful RISC processor, provides the high performance required in complex networking infrastructures.

Note When used as a Cisco Signaling Link Terminal device integrated into a Cisco Media Gateway Controller, the Cisco 2611 has SS7 functionality only; all standard Cisco 2611 software features are disabled when running the Cisco SLT image. In that case, only the Cisco Signaling Link Terminal document and the Cisco Media Gateway Controller documentation are relevant.

When used for Signaling Link Terminal applications, the modular Cisco 2611 dual-Ethernet port router can be configured with dual serial and the multiflex interface cards. The E1 multiflex interface cards offer integrated DSUs, and the T1 multiflex interface cards offer integrated CSU/DSUs. For additional flexibility, the multiflex interface cards can also be ordered with a dual-port drop-and-insert capability. All of these interface cards are Field Replaceable Units (FRUs).

The Cisco SLT supports only the SS7 MTP 2 serial protocol. Therefore, the serial interfaces cannot be configured for other protocols such as HDLC, PPP, X.25, LAPB, and Frame Relay.

The Cisco SLT functions as a component of several solutions that are currently under development. Participants in lab trials can obtain solution documentation from their Cisco representative.

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 SLT series

Table 1 Memory Recommendations for the Cisco 2611 and Cisco 2651 with Cisco SLT

Platform	Image Name	Image	Flash Memory (MB)	DRAM (MB)
SLT	c2600-ipss7-mz	Cisco SLT Series IOS SS7 Signaling Link Termination	16	64

Hardware Supported

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

- Cisco 2611
- Cisco 2651

For Cisco SLT documentation, see:

http://www.cisco.com/en/US/docs/voice_ip_comm/pgw/itp_l/itpl.html

Determining the Software Version

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

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. Individual publication links are listed at http://www.cisco.com/warp/public/707/cisco-sa-20090325-ctcp.shtml.

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. Individual publication links are listed at http://www.cisco.com/warp/public/707/cisco-sa-20090325-ctcp.shtml.

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

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

Workaround Enter the description without any quotes via the CLI.

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 12.4T*
- *Cisco IOS Software Releases 12.4 Special and Early Deployments*
- *Caveats for Cisco IOS Release 12.4T*

Platform-Specific Documents

For Cisco SLT documentation, see:

http://www.cisco.com/en/US/docs/voice_ip_comm/pgw/itp_l/itpl.html

For Cisco 2600 Series Multiservice Platforms documentation, see:

http://www.cisco.com/en/US/products/hw/routers/ps259/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.