Release Notes for Cisco 2650 and Cisco 2651 Routers for Cisco IOS Release 12.2SW

August 8, 2007
Cisco IOS Release 12.2(25)SW8
OL-5071-02

These release notes for Cisco 2650, Cisco 2651, Cisco 2650XM, and Cisco 2651XM series routers describe the enhancements provided in the Cisco IOS Release 12.2(25)SW releases. These release notes are updated as needed.

For a list of the software caveats that apply to Cisco IOS Release 12.2(25)SW, see the *"Caveats for Cisco IOS Release 12.2 SW" section on page 12* and *Caveats for Cisco IOS Release 12.2*. The caveats document is updated for every maintenance release and is located on Cisco.com and the Documentation CD-ROM.

Use these release notes with *Cross-Platform Release Notes for Cisco IOS Release 12.2* located on Cisco.com and the Documentation CD-ROM.

Cisco recommends 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.

Cisco IOS Release 12.2(25)SW8 is synchronized with Cisco IOS Release 12.2(20.4)S and contains all of the fixes that are contained in Cisco IOS Release 12.2(20.4)S. Cisco IOS Release 12.2(25)SW8 is the migration path for Cisco IOS Release 12.2(4)MB.

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 Cisco 2650 and Cisco 2651 are part of the Cisco 2600 series modular access router family. With the Cisco 2600 series, Cisco Systems extends enterprise-class and managed-services customer premise equipment (CPE) versatility, integration, and power to branch offices. The widely deployed Cisco 2600 series modular access routers are designed to enable customers to easily adopt future technologies and to scale network expansion.

The Cisco 2600 series modular architecture provides the versatility needed to adapt to changes in network technology as new services and applications become available. Driven by a powerful reduced instruction set computer (RISC) processor, the Cisco 2600 series supports the advanced quality of service (QoS), security, and network integration features required in evolving enterprise networks.

System Requirements

This section describes the system requirements for Cisco IOS Release 12.2(25)SW8 and includes the following sections:

Memory Recommendations

Table 1 Cisco IOS Release 12.2 T Memory Recommendations for Cisco 2650, Cisco 2651, Cisco 2650XM, and Cisco 2651XM Routers

Feature Set	Platform	Software Image	Recommended Flash Memory	Recommended DRAM Memory	Runs From
IP Transfer Point (M3UA/SUA)	2650-2651, 2650XM-2651XM	c2600-itpk9-mz	32 MB	128 MB	RAM
IP Transfer Point (STP/M2PA)	2650-2651, 2650XM-2651XM	c2600-itpk9-mz	32 MB	128 MB	RAM
ITP Map Gateway Base	2650-2651, 2650XM-2651XM	c2600-itpk9-mz	32 MB	128 MB	RAM

Supported Hardware

The Cisco IOS Release 12.2(25)SW releases support the following Cisco 2600 series modular access routers:

- Cisco 2650
- Cisco 2651
- Cisco 2650XM
- Cisco 2651XM

For detailed descriptions of the new hardware features, see the "New and Changed Information" section on page 5.

For additional information about supported hardware for this platform and release, refer to the Hardware/Software Compatibility Matrix at the following URL:

http://www.cisco.com/cgi-bin/front.x/Support/HWSWmatrix/hwswmatrix.cgi

Table 2 Supported Interfaces for Cisco 2600 Series Routers

Interface, Network Module, or Data Rate		Platforms Supported
LAN Interfaces	1- or 2-port Ethernet (10BASE-T)	All Cisco 2600 series
	1- or 2-port 10/100-Mbps Ethernet	Cisco 2620, Cisco 2621, Cisco 2650, Cisco 2651
T1/E1 Multiflex Voice/WAN Interface Cards	1-port T1 multiflex trunk interface (VWIC-1MFT-T1)	All Cisco 2600 series
	1-port E1 multiflex trunk interface (VWIC-1MFT-E1)	All Cisco 2600 series
	2-port T1 multiflex trunk interface (VWIC-2MFT-T1)	All Cisco 2600 series
	2-port E1 multiflex trunk interface (VWIC-2MFT-E1)	All Cisco 2600 series
	2-port T1 multiflex trunk interface with drop and insert (VWIC-2MFT-T1-DI)	All Cisco 2600 series
	2-port E1 multiflex trunk interface with drop and insert (VWIC-2MFT-E1-DI)	All Cisco 2600 series

Determining the Software Version

To determine the version of Cisco IOS software running on a Cisco 2600 series router, log in to the router and enter the **show version** EXEC command:

```
Router# show version
Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-ITP-M), Version 12.2(25)SW7, EARLY DEPLOYMENT RELEASE
SOFTWARE
```

Upgrading to a New Software Release

For general information about upgrading to a new software release, refer to *Software Installation and Upgrade Procedures* located at the following URL:

http://www.cisco.com/warp/public/130/upgrade_index.shtml

Feature Set Tables

Cisco IOS software is packaged in feature sets that consist of software images that support specific platforms. The feature sets available for a specific platform depend on which Cisco IOS software images are included in a release. Each feature set contains a specific set of Cisco IOS features.

The Cisco IOS Release 12.2(25)SW releases support the feature set that is found in the Cisco IOS Release 12.2 S IP image.

Caution Cisco IOS images with strong encryption (including, but not limited to, 168-bit Triple Data Encryption Standard [3DES] data encryption feature sets) are subject to United States government export controls and have limited distribution. Strong encryption images to be installed outside the United States are likely to require an export license. Customer orders may be denied or subject to delay because of United States government regulations. When applicable, purchaser and user must obtain local import and use authorizations for all encryption strengths. Please contact your sales representative or distributor for more information, or send an e-mail to export@cisco.com.

Table 3 lists the features and feature sets supported by the Cisco 2600 series in the Cisco IOS Release 12.2(25)SW releases. The following conventions are used:

- Yes—The feature is supported in the software image.
- No—The feature is not supported in the software image.
- In—The number in the "In" column indicates the Cisco IOS release in which the feature was introduced. For example, (1)MB1 means a feature was introduced in Cisco IOS Release 12.2(1)MB1. If a cell in this column is empty, the feature was included in the initial base release.

Note These release notes list features that are new to the Cisco IOS Release 12.2(25)SW releases. The parent release for these releases is Cisco IOS Release 12.2(20)S. For information about inherited features, refer to Cisco.com or Cisco Feature Navigator. For Cisco.com, go to http://www.cisco.com/univercd/home/index.htm, select the appropriate software release under **Cisco IOS Software**, and click **Release Notes**. If you have a Cisco.com login account, you can use the Cisco Feature Navigator tool at http://www.cisco.com/cgi-bin/Support/FeatureNav/FN.pl.

Table 3 Feature List by Feature Set for Cisco 2650, Cisco 2651, Cisco 2650XM, and Cisco 2651XM Routers

Features	Software Images by Feature Sets	
	In	IP Transfer Point (ITP)
Multi-Layer Routing (MLR) Generic Opcode Support	12.2(25)SW8	Yes
Insert Destination Point Code (DPC) in Called Party (CDPA) PC	12.2(25)SW8	Yes
Preventive Cyclic Redundancy (PCR) Error Corrections	12.2(25)SW7	Yes
MLR Call Tracing Facility	12.2(25)SW5	Yes
SMS MO Proxy Message Modification	12.2(25)SW5	Yes
Enhanced Gateway Screening	12.2(25)SW4	Yes

Table 3 Feature List by Feature Set for Cisco 2650, Cisco 2651, Cisco 2650XM, and Cisco 2651XM Routers (continued) (continued)

Features	Software Images by Feature Sets	
DSMR UCP Application Oriented to GSM Mobile Terminated Short Message Delivery, page 8	12.2(25)SW3	Yes
IS-41 SMS Multicast Notification, page 8	12.2(25)SW3	Yes
MLR Route on Originating IMSI for GSM MAP Version 1 and 2, page 8	12.2(25)SW3	Yes
M2PA v13, page 8	12.2(25)SW3	Yes
ITP Group Multi-Instance Support, page 8	12.2(25)SW3	Yes
GSM Short Message Routing Mobile-Originated to Mobile-Terminated	12.2(25)SW1	Yes
Extended number of Capability Point Codes from 2 to 200	12.2(25)SW1	Yes
ITP First Delivery Attempt (FDA)	12.2(25)SW	Yes
Extended Unitdata (XUDT) Messages Support	12.2(23)SW1	Yes
Secure Shell Support for IP Security	12.2(23)SW	Yes
CS7 Monitor	12.2(21)SW	Yes
Multi-Layer Routing Extension for Support of ANSI-41 Short Message Service	12.2(21)SW	Yes
IP Transfer Point Variant Conversion Feature	12.2(20)SW	Yes
Extensions to the Multi-Layer Routing Feature	12.2(19)SW	Yes
Support for SIGTRAN MTP3-User Adaptation and SCCP User Adaptation in Multiple Instances	12.2(19)SW	Yes
ITP M3UA/SUA Signaling Gateway	12.2(4)MB5	Yes
SCCP Load Balancing Enhancements	12.2(4)MB2	Yes
ITP Instance Translation	12.2(4)MB10	Yes
ITP Multi-Layer Routing	12.2(4)MB10	Yes
ITP Multiple Instances	12.2(4)MB10	Yes
ITP SCCP/GTT	12.2(4)MB1	Yes
ITP SS7 Offload	12.2(1)MB1	Yes

New and Changed Information

The following sections list the new hardware and software features supported by the Cisco 2600 series routers for the Cisco IOS Release 12.2 SW releases:

New Features in Cisco IOS Release 12.2(25)SW8

The following new software features are supported by the 2650 and Cisco 2651 for Cisco IOS Release 12.2(25)SW8.

Multi-Layer Routing (MLR) Generic Opcode Support

Cisco IOS Release 12.2(25)SW8 extends Mobile Access Part (MAP) operation support to include all GSM-MAP (3GPP TS 29.002 version 5.9.0 Release 5) operations in MLR rules.

Insert Destination Point Code (DPC) in Called Party (CDPA) PC

Cisco IOS Release 12.2(25)SW8 provides a global option to insert DPC into the CDPA PC for packets that are MLR-routed.

New Features in Cisco IOS Release 12.2(25)SW7

The following new feature is supported in Cisco IOS Release 12.2(25)SW7:

Preventive Cyclic Redundancy (PCR) Error Corrections

Cisco IOS Release 12.2(25)SW7 supports the Preventive Cyclic Redundancy (PCR) Error Corrections feature as described in Q.703 and GR-246. PCR is an alternate form of error correction for MTP2 links and is typically used on links that have a long delay (for example, satellite links).

New Features in Cisco IOS Release 12.2(25)SW6

There are no new features on the Cisco 26x00 in Cisco IOS Release 12.2(25)SW6.

New Features in Cisco IOS Release 12.2(25)SW5

The following new features are supported in Cisco IOS Release 12.2(25)SW5:

MLR Call Tracing Facility

The ITP Multi-Layer Routing (MLR) Call Tracing feature introduces enhanced message tracing and enables the mobile operator to provide improved customer service. The feature uses the Cisco Event Tracer facility, which reads informational messages from specific Cisco IOS software subsystems and logs messages from those components into system memory. The new **component cs7 mlr** command enables event tracing on MLR. Trace messages stored in memory can be displayed on the screen or saved to a file for later analysis.

The MLR Call Tracing feature provides the following capabilities:

- GSM SMS MO message tracing for a set of originating IMSIs.
- GSM SMS MO message tracing for a set of different MSISDNs that represent either the A-address or B-address of an SMS message.
- ANSI41 SMDPP message tracing for a set of different addresses that represent either the A-address or B-address of an SMS message.
- Displays trace entries on the router console using show commands.
- Indicates whether a message has been processed by MLR for a given traceable address, including the final routing result.
- Allows message trace logs to be obtained via FTP or TFTP.

SMS MO Proxy Message Modification

Cisco IOS Release 12.2(25)SW5 enables additional SMS MO Proxy feature capabilities which require SMS MO Proxy message modifications:

- The originating IMSI message, if known, must be allowed to be inserted into the proxied SMS MO dialogue under normal conditions. Conversion of the original SMS MO message from MAP version 1 or MAP version 2 to MAP version 3 may be required.
- When specified, the destination SMSC address should be modified to match the recipient SMSC.
- If the B-address is modified with DSMR Address Translation, the modified address should be included in the proxied SMS MO dialogue.

For more information about these features, see the Cisco IOS Release 12.2(25)SW5 configuration guide at the following link:

http://cisco.com/en/US/products/sw/wirelssw/ps1862/products_installation_and_configuration_guides_list.html

New Features in Cisco IOS Release 12.2(25)SW4

Enhanced Gateway Screening

Gateway Screening is a process in Signaling Transfer Point (STP) to check the contents of the incoming and outgoing message and either allow or reject the message based on the provisioned screening. If the incoming message is allowed, it shall be sent to MTP/SCCP/ISUP/XUA for further processing. If the

outgoing message is allowed, MTP / XUA shall route the message to the destination as specified in the outgoing message. Gateway Screening shall be used along with Access Lists, Global Translation Table (GTT) and Multi-Layer Routing (MLR). This feature is compliant with ITU Q.705 and Telcordia GR-82. The screening rules shall be applied based on a link set (or AS in case of XUA) and tables shall be created to configure the screening rule.

MLR Dynamic B-address Routing/Binding - When SMSC messaging platforms are connected to multiple signaling gateways (SG), messages should be distributed such that messages for a specific B-address are routed to the same SMSC. This is desirable in order to guarantee in-sequence delivery of messages, and to optimize the delivery of concurrent messages destined to the same mobile destination.

New Features in Cisco IOS Release 12.2(25)SW3

The features in this section are new in Cisco IOS Release 12.2(25)SW3.

DSMR UCP Application Oriented to GSM Mobile Terminated Short Message Delivery

This feature allows operators to distribute SMS messages generated by various service applications to their subscribers using the UCP protocol.

IS-41 SMS Multicast Notification

This feature requires notification when the ITP is loadsharing SMS messages across a bank of message centers and the ITP must duplicate the incoming SMSNOT message and send the message to each MC.

MLR Route on Originating IMSI for GSM MAP Version 1 and 2

The GSM SRI-SM procedure is used with the HLR of the A-address MSISDN in order to obtain the International Mobile Subscriber Identity (IMSI) value.

M2PA v13

Cisco IOS Release 12.3(25)SW3 supports draft version 13 of the M2PA protocol, which is configurable. Support for draft Version 2 is continued.

ITP Group Multi-Instance Support

This feature allows ITP to transport SS7 traffic over M2PA/SCTP/IP. The ITP router acts as a bridge between the SS7 and IP networks, by encapsulating SS7 Message Signaling Units into IP-based packets and forwarding them to IP-peer ITP devices, which perform the IP to SS7 bridging in the reverse direction.

New Features in Cisco IOS Release 12.2(25)SW2

There are no new hardware or software features in this release. See "Caveat Advisory - Resolved Caveats Cisco IOS Release 12.2(25)SW2" section on page 30.

New Features in Cisco IOS Release 12.2(25)SW1

Hardware Features

No new hardware products are supported in Cisco IOS Release 12.2(25)SW1.

Software Features

The following new software features are supported by the Cisco 2600 series routers for Cisco IOS Release 12.2(25)SW1.

GSM Short Message Routing Mobile-Originated to Mobile-Terminated

This feature provides the ability to deliver GSM Mobile Originated Short Messages to Mobile Terminated users. See the ITP Distributed Short Message Routing (DSMR) chapter of the *Cisco ITP Configuration Guide and Command Reference* on Cisco.com.

Extended Number of Capability Point Codes

The allowable number of capability point codecs has been extended from 2 to 200 in Cisco IOS Release 12.2(25)SW1.

New Features in Cisco IOS Release 12.2(25)SW

Hardware Features

No new hardware products are supported in Cisco IOS Release 12.2(25)SW.

Software Features

The following new software feature is supported by the Cisco 2600 series routers for Cisco IOS Release 12.2(25)SW:

ITP First Delivery Attempt (FDA)

The ITP performs a first delivery attempt of a GSM Mobile-Originated SMS message to an Application Server.

New Features in Cisco IOS Release 12.2(23)SW1

Hardware Features

No new hardware products are supported in Cisco IOS Release 12.2(23)SW1.

Software Features

The following new software feature is supported by the Cisco 2600 series routers for Cisco IOS Release 12.2(23)SW1:

Extended Unitdata (XUDT) Messages Support

Additional support for extended unitdata (XUDT) messages on the Signaling System 7 (SS7) network is provided by the **cs7 sua-allow-xudt-request** command. The **cs7 sua-allow-xudt-request** command allows the Signaling Connection Control Part (SCCP) User-Adaptation (SUA) Application Server Processes (ASP) additional control in determining whether an SCCP unitdata (UDT) or XUDT will be generated upon receiving a CLDT message. When the command is specified, the SUA will request the SCCP layer to generate an XUDT message if the ASP has provided either the IMPORTANCE or HOP_COUNTER parameters within the CLDT message.

New Features in Cisco IOS Release 12.2(23)SW

Hardware Features

No new hardware products are supported in Cisco IOS Release 12.2(23)SW.

Software Features

The following new software feature is supported by the Cisco 2600 series routers for Cisco IOS Release 12.2(23)SW:

Secure Shell Support for IP Security

Secure Shell (SSH) support on IP Security (IPSec) is added to the Cisco 2650 and Cisco 2651 routers.

New Features in Cisco IOS Release 12.2(21)SW

Hardware Features

No new hardware products are supported in Cisco IOS Release 12.2(21)SW.

Software Features

The following new software features are supported by the Cisco 2600 series routers for Cisco IOS Release 12.2(21)SW:

CS7 Monitor

The CS7 Monitor feature allows the IP Transfer Point (ITP) to monitor Signaling System 7 (SS7) LSL ports and send copies of the message signal units (MSU) through TCP to a server for collection/storage. This feature was previously available on other ITP platform hardware and is now available on the 2600 platform.

Multi-Layer Routing Extension for Support of ANSI-41 Short Message Service

The Multi-layer Short Message Service (SMS) Routing feature is part of the IP Transfer Point (ITP) product program that implements legacy Signaling System 7 (SS7) routing, as well as an SS7 over IP Signaling Gateway based on SIGTRAN protocols MTP2-User Peer-to-Peer Adaptation (M2PA), MTP3-User Adaptation (M3UA), and Signaling Connection Control Protocol (SCCP)-User Adaptation (SUA). The Multi-layer SMS Routing feature allows the ITP to make SMS message routing decisions based on information found in the Transaction Capabilities Applications Part (TCAP), Mobile Application Part (MAP), and MAP-user layers. This project adds support for routing SMS messages per the ANSI-41 (also known as IS-41) standard, as well as incorporation of MDN-based SMS routing.

New Features in Cisco IOS Release 12.2(20)SW

Hardware Features

No new hardware products are supported in Cisco IOS Release 12.2(20)SW:

Software Features

The following new software features are supported by the Cisco 2600 series routers for Cisco IOS Release 12.2(20)SW:

IP Transfer Point Variant Conversion Feature

This IP Transfer Point (ITP) features adds support for conversion between different variants. This conversion involves modification of the Message Transfer Part Layer 3 (MTP3) and Signaling Connection Control Part (SCCP) portions of the message signal unit (MSU) when crossing from one instance to another. These modifications include point code conversion, network indicator and SCCP parameters. In the first release, ITP supports conversion between International Telecommunications Union (ITU) and American National Standards Institute Inc. (ANSI) variants of Signaling System 7 (SS7).

New Features in Cisco IOS Release 12.2(19)SW

Hardware Features

No new hardware features are supported in Cisco IOS Release 12.2(19)SW:

Software Features

The following new software features are supported by the Cisco 2600 series routers for Cisco IOS Release 12.2(19)SW:

Extensions to the Multi-Layer Routing Feature

The IP Transfer Point (ITP) Multi-Layer Routing (MLR) feature enables intelligent routing of Short Message Service - Mobile Originated (SMS MO) messages based on the application or service from where they originated, or to where they are destined. The MLR feature can make SMS message routing

decisions based on information that is found in the Transaction Capabilities Applications Part (TCAP), Mobile Application Part (MAP), and MAP-user layers. Cisco IOS Release 12.2(19)SW provides new extensions to the commands that support blocking and routing of SMS MO and mobile terminated (MT) MAP messages.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122sw/122_19sw/itpcfgop.htm

Support for SIGTRAN MTP3-User Adaptation and SCCP User Adaptation in Multiple Instances

The Cisco ITP Signaling Gateway (ITP SG) feature provides open-standards-based Signaling System 7 (SS7) over IP solutions through the implementation of SIGTRAN MTP3-User Adaptation (M3UA) and SCCP User Adaptation (SUA) protocols. Previous releases of ITP supported M3UA and SUA in Instance 0 only.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122sw/122_19sw/itpsg.htm

MIBs

Current MIBs

To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml.

Caveats for Cisco IOS Release 12.2 SW

This section documents possible unexpected behavior by Cisco IOS Release 12.2(25)SW8 and describes only severity 1 and 2 caveats and select severity 3 caveats.

Caveats describe unexpected behavior in Cisco IOS software releases. Severity 1 caveats are the most serious caveats; severity 2 caveats are less serious. Severity 3 caveats are moderate caveats, and only select severity 3 caveats are included in the caveats document.

This section contains only open and resolved caveats for the current Cisco IOS maintenance release.

All caveats in Cisco IOS Release 12.2 and Cisco IOS Release 12.2 T are also in Cisco IOS Release 12.2(25)SW8, and so on.

For information on caveats in Cisco IOS Release 12.2, see *Caveats for Cisco IOS Release 12.2*.

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, **log in** to Cisco.com and click **Service and Support: Technical Assistance Center: Select & Download Software: Jump to a software resource: Software Bug Toolkit/Bug Watcher**. Another option is to go to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl.

Caveat Reference

Table 4 contains all known caveats that are specific to the 12.2SW releases.

Table 4 Caveats Reference for Cisco IOS Release 12.2 SW

DDTS Number	Open in Release	Resolved in Release
CSCse71985	-	12.2(25)SW8
CSCse74363	-	12.2(25)SW8
CSCse86887	-	12.2(25)SW8
CSCse96573	-	12.2(25)SW8
CSCse99146	-	12.2(25)SW8
CSCsf08276	-	12.2(25)SW8
CSCsf98340	-	12.2(25)SW8
CSCsf98655	-	12.2(25)SW8
CSCsg11535	-	12.2(25)SW8
CSCsg12763	-	12.2(25)SW8
CSCsg14566	-	12.2(25)SW8
SCSsg18913	-	12.2(25)SW8
CSCse50769	-	12.2(25)SW8
CSCse70944	-	12.2(25)SW8
CSCse49476	12.2(25)SW7	12.2(25)SW7
CSCse45533	12.2(25)SW7	12.2(25)SW7
CSCse28466	12.2(25)SW7	12.2(25)SW7
CSCse22221	12.2(25)SW7	12.2(25)SW7
CSCse17165	12.2(25)SW7	12.2(25)SW7
CSCsd99215	12.2(25)SW7	12.2(25)SW7
CSCsd90336	12.2(25)SW7	12.2(25)SW7
CSCsd90209	12.2(25)SW7	12.2(25)SW7
CSCsd84614	12.2(25)SW7	12.2(25)SW7
CSCsd76797	12.2(25)SW7	12.2(25)SW7
CSCsd73205	12.2(25)SW7	12.2(25)SW7
CSCsd63762	12.2(25)SW56	12.2(25)SW6
CSCsd63672	12.2(25)SW7	12.2(25)SW7
CSCsd35259	12.2(25)SW6	12.2(25)SW6
CSCsd30900	12.2(25)SW6	12.2(25)SW6

Table 4 Caveats Reference for Cisco IOS Release 12.2 SW (continued)

DDTS Number	Open in Release	Resolved in Release
CSCsc78421	12.2(25)SW6	12.2(25)SW6
CSCsc62555	12.2(25)SW5	12.2(25)SW5
CSCsc51378	12.2(25)SW5	12.2(25)SW5
CSCsc46651	12.2(25)SW5	12.2(25)SW5
CSCsc34914	12.2(25)SW5	12.2(25)SW5
CSCsc12670	12.2(25)SW5	12.2(25)SW5
CSCsc02671	12.2(25)SW5	12.2(25)SW5
CSCsb92248	12.2(25)SW5	12.2(25)SW5
CSCsb91588	12.2(25)SW5	12.2(25)SW5
CSCsb64543	12.2(25)SW4	12.2(25)SW4
CSCsb33974	12.2(25)SW4	12.2(25)SW4
CSCsb33575	12.2(25)SW4	12.2(25)SW4
CSCsb19607	12.2(25)SW4	12.2(25)SW4
CSCsb16386	12.2(25)SW4	12.2(25)SW4
CSCsb04849	12.2(25)SW4	12.2(25)SW4
CSCsb04493	12.2(25)SW4	12.2(25)SW4
CSCsb02059	12.2(25)SW4	12.2(25)SW4
CSCsa98311	12.2(25)SW4	12.2(25)SW4
CSCsa98287	12.2(25)SW4	12.2(25)SW4
CSCsa92616	12.2(25)SW3	12.2(25)SW3
CSCsa88289	12.2(25)SW3	12.2(25)SW3
CSCsa78896	12.2(25)SW3	12.2(25)SW3
CSCsa72249	12.2(25)SW3	12.2(25)SW3
CSCsa59599	12.2(25)SW3	12.2(25)SW3
CSCsa57212	12.2(25)SW1	12.2(25)SW1
CSCsa56453	12.2(25)SW1	12.2(25)SW1
CSCsa54632	12.2(25)SW1	12.2(25)SW1
CSCsa42261	12.2(25)SW1	12.2(25)SW1
CSCsa42016	12.2(25)SW1	12.2(25)SW1
CSCei76358	12.2(25)SW3b	12.2(25)SW3b
CSCei61732	12.2(25)SW4	12.2(25)SW4
CSCeh16859	12.2(25)SW3	12.2(25)SW3
CSCeh15067	12.2(25)SW3	12.2(25)SW3
CSCeh13554	12.2(25)SW3	12.2(25)SW3
CSCeg50319	12.2(25)SW1	12.2(25)SW1
CSCeg50304	12.2(25)SW1	-12.2(25)SW1

Table 4 Caveats Reference for Cisco IOS Release 12.2 SW (continued)

DDTS Number	Open in Release	Resolved in Release
CSCeg37718	12.2(25)SW1	-12.2(25)SW1
CSCeg18352	12.2(25)SW3	12.2(25)SW3
CSCeg08298	12.2(25)SW1	12.2(25)SW1
CSCef95065	12.2(23)SW1	12.2(25)SW
CSCef85587	12.2(23)SW1	12.2(25)SW
CSCef84189	12.2(23)SW1	12.2(25)SW
CSCef74580	12.2(23)SW1	12.2(25)SW
CSCef69373	12.2(23)SW1	12.2(25)SW
CSCef68324	12.2(25)SW3a	12.2(25)SW3a
CSCef38050	12.2(23)SW1	12.2(25)SW
CSCef31588	12.2(23)SW1	12.2(25)SW
CSCef29094	12.2(23)SW1	12.2(25)SW
CSCef08522	12.2SW	12.2(23)SW1
CSCee91201	12.2(23)SW	12.2(23)SW1
CSCee86829	12.2(23)SW	12.2(23)SW1
CSCee56986	12.2(21)SW	12.2(23)SW1
CSCee54303	12.2(23)SW	12.2(23)SW1
CSCee41388	12.2(21)SW	12.2(23)SW1
CSCee36139	12.2(21)SW	12.2(23)SW1
CSCee21531	12.2(21)SW	12.2(23)SW
CSCee13367	12.2(25)SW3	12.2(25)SW3
CSCee11874	12.2(21)SW	12.2(23)SW
CSCee09009	12.2(21)SW	12.2(23)SW
CSCee08792	12.2(21)SW	12.2(23)SW
CSCed83705	12.2(25)SW3	12.2(25)SW3
CSCed82922	12.2(21)SW	12.2(23)SW
CSCed44759	12.2(19)SW	12.2(21)SW
CSCed38527	12.2(19)SW	12.2(21)SW
CSCed27956	12.2(19)SW	12.2(21)SW
CSCed20020	12.2(19)SW	12.2(20)SW
CSCed01515	12.2(19)SW	12.2(20)SW
CSCec79617	12.2(19)SW	12.2(20)SW
CSCec70480	12.2(19)SW	12.2(20)SW
CSCec69259	12.2(19)SW	12.2(20)SW
CSCec62567	12.2(19)SW	12.2(20)SW

Table 4 Caveats Reference for Cisco IOS Release 12.2 SW (continued)

DDTS Number	Open in Release	Resolved in Release
CSCec61182	12.2(19)SW	12.2(20)SW
CSCec44189	12.2(4)MB12	12.2(19)SW

Caveats for the Current Release

Release 12.2(25)SW8

Open Caveats—Cisco IOS Release 12.2(25)SW8

There are no known open caveats for Cisco IOS Release 12.2(25)SW8.

Resolved Caveats—Cisco IOS Release 12.2(25)SW8

- CSCse68138

  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

- CSCsd62477: ITP platform crashing by TLB on sms_compare_destSme

  An IP Transfer Point (ITP) platform running the Cisco IOS Release 12.2(25)SW5 may experience a software crash because of a translational bridging (TLB) (load or instruction fetch) exception.

  This issue occurs when the following conditions are met:

  a. ITP is configured with the Short Message Service (SMS) subsystem and is receiving SMS mobile originated (MO) messages (such as, SMS MO Proxy or DSMR feature)

  b. A received SMS MO message has a destination/recipient address greater than 20 digits in length (which is a protocol violation).

  Workarounds: There are two possible workarounds:

  1. Remove the SMS subsystem configuration, or

2. Ensure that the message signaling units (MSCs) do not send SMS MO messages with destination/recipient addresses greater than 20 digits.

- CSCsd99215: Cannot set china point code format on 24 bits

  The point code format cannot be configured to any value other than its default format of 8.8.8 bits.

  Workaround: There are no known workarounds.

- CSCse17165: ITP MAPUA: max-return setting not applied

  The IP Transfer Point (ITP) returns a number of triplets higher than the value set for *max-return* under the **gsm-authent-vlr** configuration of the Map User API (MAPUA).

  This condition occurs when the MAPUA client requests a number of fresh triplets higher than the *max-return* value, and the home location register (HLR)/authentication center (AuC) returns a number of triplets higher than the *max-return* value.

  Workaround: Configure the MAPUA client to request a number of triplets below or equal to the *max-return* value.

- CSCse28466: MLR: Order of triggers in MLR table may reverse after reload

  The order of triggers found in an Multi-Layer Routing (MLR) table may reverse after a reload. For primary triggers, this issue has no impact on MLR operation. However, because secondary triggers are searched sequentially, depending upon the secondary trigger configuration, modifying the order of the secondary triggers can modify the outcome of MLR routing.

  This condition occurs when new triggers of the same location/type are added before existing triggers (instead of after). Triggers are sorted by location (cdpa, cgpa, mtp3, default) and type (gt addr, gt selector, pc). Primary triggers use a best match algorithm, so order is not a factor. However, secondary triggers are searched sequentially to find a match. This problem causes the order of the these triggers to be reversed when the configuration is read in at reload time, that is, the order of the secondary trigger list reverses.

  Workaround: Delete and reconfigure any secondary triggers required so that the trigger list is ordered properly after a router reloads. If a message can match multiple secondary triggers, ensure that the most specific secondary trigger is configured before the less specific trigger.

- CSCse49476: ITP crash on cs7_mlr_result_group_lookup

  An IP Transfer Point (ITP) running the SMS_MO Proxy feature may reload if both of the following conditions are met:

  a. The Short Message Service (SMS) rules are using Multi-Layer Routing (MLR) result groups, and

  b. There are currently no available members within the MLR result group.

  Workaround: The short-term workaround is to create identical SMS result groups and use them explicitly in the SMS rulesets.

- CSCse50769: ITP: Do not use XCO/XCA for Chinese variant

  When the IP Transfer Point (ITP) performs a changeover for a high speed link in the China variant, it uses the H0H1 codes for an extended changeover message. However, the Chinese network does not support these codes and instead uses the H0H1 codes for a standard changeover message. Changeover messages are used to resend any messages that were in transmission when the link failed. The changeover completes due to a timeout, but a few messages can be lost if the changeover messages can not be exchanged due to a mis-match in the H0H1 codes.

  This condition occurs when a network is running the China variant with high speed links, and a high speed link fails

  Workaround: There are no known workarounds.

- CSCse70944: ITP: snmp-server host command NVGENed incorrectly for cs7 traps

  When the **snmp-server traps** *IP address* **version** *version SNMP community string* **cs7** command is configured, the configuration is saved incorrectly in the running-config.

  The condition occurs on all IP Transfer Point (ITP) platforms.

  Workaround: There are no known workarounds.

- CSCse71985: ITP: Suppress TFAs during AS state transitions with SGMP configured

  The IP Transfer Point (ITP) broadcasts extraneous TFA messages during application server (AS) state transitions when the Simple Gateway Monitoring Protocol (SGMP) is configured.

  The condition occurs only when two ITPs are configured as signaling gateway (SG) mates with SGMP enabled, and the AS transitions between the active and inactive-rerouting state.

  Workaround: There are no known workarounds.

- CSCse74363: ITP : Memory leak in M3UA/SUA Inbound process with shut ASPs

  Memory consumption is continuously increasing under the Pool Manager process. Malloc failure messages appear in the log, and the IP Transfer Point (ITP) hangs as a result of memory depletion. Some Application Server Processors (ASPs) are in shutdown status on the ITP and the SMS-C continuously tries to establish the connection with the ITP.

  This condition occurs on Cisco 7500 series routers running ITP images and Cisco IOS Release 12.2(25)SW3 and previous releases.

  Workaround: There are two possible workarounds:

  1. Shut down the cs7 ASP connections, and then enable them back, or

  2. Shut down the ASP connections on only the SMS-C, not on the ITP.

- CSCse86887: Unconfigure primary ip on ASP is not effective until system reload

  An attempt to unconfigure the primary remote-ip address in an SCCP User Adaptation (SUA) Application Server Processor (ASP) fails. The ASP cannot connect to the IP Transfer Point (ITP) using the Stream Control Transmission Protocol (SCTP) using the previous secondary IP address, and the change is not enacted.

  This condition occurs when the ITP boots with a multi-homed configuration and the primary IP address of the ASP is unconfigured.

  Workaround: Save the change, and reload the system.

- CSCse96573: ITP: TTC variant - allow SRTM/SRTA responses for available XUA PCs

  The IP Transfer Point (ITP) ignores the TTC Signaling System 7 (SS7) variant Signaling Route Tests generated for MTP3 User Adaptation/SCCP User Adaptation (M3UA/SUA) point codes that are not shared with any of the ITP's local point codes. No response is generated on reception of such messages.

  Workaround: Disable generation of SRT messages to M3UA/SUA point codes in the network.

- CSCse99146: ITP: SCCP encoding error attempting to insert PC in CgPA

  The IP Transfer Point (ITP) reports a Signaling Connection Control Part (SCCP) encoding error when attempting to route an SCCP message.

  The problem occurs when the ITP attempts to route an SCCP message and the following conditions occur:

  a. The order of the SCCP parameters in the message are as follows: CgPA, Data, CdPA.

  b. No PC exists in the CgPA, and the CgPA RI is route-on-SSN. Both conditions must be present for the problem to occur.

Workaround: There are no known workarounds.

- CSCsf08276: ITP: xUA AS recovery processing causing temp memory spike can leak queue

  An IP Transfer Point (ITP), configured as an MTP3 User Adaptation (M3UA) or SCCP User Adaptation (SUA) Signalling Gateway (SG), may remain memory-constrained after one or more application servers (AS) processing high traffic load fail but recover within the recovery timeout period. MALLOCFAIL messages may occur.

  This condition occurs because the queuing of message buffers during the recovery time period exhausts or fragments memory. The AS recovery queue is a mechanism intended to eliminate message loss due to temporary failures of an AS. If the AS is handling high traffic volume, the queuing of the packets becomes a significant memory burden to the ITP, and may exhaust the system of memory in extreme cases. For most SG deployments, this recovery queue mechanism is not necessary, and immediate failure of an AS results in Message Transfer Part, Level 3 (MTP3) or SCCP layer rerouting of messages to an available backup system

  Workaround: Disable the AS recovery queue by setting the recovery-timeout value to 0.

- CSCsf98340: ITP: MTP3 reports no congestion, SCCP GTT MAP is congested

  Global Title Translation (GTT) traffic is discarded due to congestion.

  This condition occurs during periods of stress when links are flapping over a long duration, and Route Processor (RP) CPU usage was high.

  Workaround: Enter the **cs7 gtt map sp avail** *pc* command for the congested destination point code (DPC) at the Signaling Connection Control Part (SCCP) level.

- CSCsf98655: ITP: Remove colon character in checkpointed GWS/GTT log file name

  A Gateway Screening (GWS) or Global Title Translation (GTT) log fails to be checkpointed to flash.

  The problem occurs on the IP Transfer Point (ITP).

  Workaround: There are no known workarounds.

- CSCsg11535: ITP : CPUHOG issue if the RSP is passing a high rate of traffic

  CPUHOG messages are generated when an Application Server Processor (ASP) goes active.

  This condition occurs when "traffic-mode loadshare bindings" is configured for the Application Server (AS). In this configuration, IP Transfer Point (ITP) must check for any bindings that are owned by the ASP and redistribute the bindings if necessary (to balance the ASP load). The CPUHOG messages can be a problem if the Route/Switch Processor (RSP) is passing a high rate of traffic (such as when M3UA traffic is routed through the RSP).

  Workaround: There are two possible workarounds:

  1. Change the configuration of the AS from "traffic-mode loadshare bindings" to "traffic-mode loadshare roundrobin." This workaround might not be acceptable as an end-to-end solution, however, as messages for the same CIC could be distributed to different ASPs. If the different ASPs can share calls in progress, this can be a possible workaround.

  2) Reduce the number of bindings being handled per AS by changing the AS routing-key to include a CIC range, and having the ASPs support more ASes.

- CSCsg12763: ITP: Linkstate mismatch between VIP and RSP results from controller flap

  Congestion and availability state mismatches occur on the ITP 7500 platform during periods of E1/T1 controller volatility. These mismatches can affect offloaded link, linkset, route, SCCP User Adaptation (SUA), or MTP3 User Adaptation (M3UA) state information. The affected state information might not have any physical or logical relation to the E1 or T1 controller experiencing volatility.

This condition occurs when the E1/T1 controller transitions from the down state to the up state.

There are no known workarounds.

- CSCsg14566: m3ua interface wedge

  A Cisco 7500 router running IOS with the IP Transfer Point (ITP) feature stops processing packets in the input buffer queue.

  This condition occurs because the buffer is full and further input packets are being dropped. A router reload clears the buffer, but the condition reoccurs.

  Workaround: Increase the input buffer queue size on the interface by using the **hold-queue** *xxx* **in** command in interface configuration mode. This action should allow input packets to be processed again, however, the queue can reach its maximum size again over time.

- CSCsg18913: ITP: Slave could be in state where its route table is not in sync

  When running in Non-Stop Operation (NSO) mode and a switchover occurs, Signaling System 7 (SS7) routes that were deleted on the previous active Route/Switch Processor (RSP) exist on the new active RSP. These routes appear in the **sh run** command output, but not in the **sh cs7 route** command output.

  This condition can occur when running in CS7 NSO mode.

  Workaround: After the switchover, the route table should be analyzed for routes that should not exist, these routes should be removed, and the route table should be saved.

Caveats for Prior Releases

This section contains caveats for prior Cisco IOS Software Release 12.2SW releases.

Release 12.2(25)SW7

- CSCsc60249

  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

- CSCsd63672: ITP group links may remain FAILED after restarting with large config/GTT

  Symptoms: Some ITP group links remain in FAILED state after the restarting of either the group manager or alternate.

  Conditions:The ITP must be configured with ITP group capability, and the amount of information requiring synchronization between the manager and alternate is in excess of 1500 bytes. Typically, the presence of global title data will cause the synchronization to exceed 1500 bytes.

  Workaround:Links remaining in the FAILED state may be recovered by issuing a "shutdown" command on the affected links or linksets, followed by a **no shutdown** command.

- CSCsd73205: ITP: Crash with msg for loadshare bindings AS serving zero-weight ASPs

  Symptoms: ITP crashes when processing a message destined for an m3ua/sua AS where all configured ASPs have weight=0.

  Conditions: M3UA/SUA AS is configured with all ASPs having weight = 0.

  Workaround: Ensure that every AS includes at least one ASP with weight greater than 0. If not specified, the default weight is 1.

- CSCsd76797: ITP: Add graceful keyword to ASP and xua instance shut config

  Symptoms: When operator enters **shut** in cs7 asp or cs7 m3ua/sua submode, the ITP closes sctp associations by sending an sctp ABORT chunk instead of an sctp SHUTDOWN chunk.

  Workaround: There is no workaround.

- CSCsd84614: ITP: Crash during linkset configuration

  Symptoms: RSP may crash during linkset configuration

  Conditions: The issue has been observed when a configuration command was entered while in linkset submode.

  Workaround: There is no workaround.

- CSCsd8738: ITP: Offending message not included in some m3ua/sua ERR messages

Symptoms: Some m3ua/sua ERR messages sent by the ITP do not include the diagnostic info parameter.

Conditions: Error conditions detected by the ITP where the ITP responds with an m3ua or sua ERR message. Usually a response to a received m3ua/sua message.

Workaround: There is no workaround.

- CSCsd90336: support for Cisco ios qos in Cisco 26xx itp

  Symptoms: Cisco IOS QOS cannot be implemented on itp with Cisco 2651 on the software image.

  Conditions: match commands and class-map commands cannot be entered.

  Workaround: None on the supported Cisco 26xx. Can use supported Cisco 73xx.

- CSCsd99215: Cannot set china point code format on 24 bits

  Symptoms: The point code format cannot be configured to something else than its

  default format 8.8.8 bits.

  Conditions: It is impossible to change the default 8.8.8 point-code format.

  Workaround: There is no workaround.

- CSCse28466: MLR: Order of triggers in MLR table may reverse after reload.

  Symptoms: The order of triggers found in an MLR table may reverse after a reload. For primary triggers, this issue has no impact in MLR operation. However, secondary triggers are searched sequentially. Depending upon the secondary trigger configuration, modifying the order of the secondary triggers can modify the outcome of MLR routing.

  Conditions: Triggers are sorted by location (cdpa, cgpa, mtp3, default) and type (gt addr, gt selector, pc). New triggers of the same location and type are added BEFORE existing triggers (instead of after). Primary triggers use a best match algorithm, so order is not a factor. However, secondary triggers are searched sequentially to find a match. This problem causes the order of the these triggers to be reversed when configuration is read in at reload time. Thus the order of the secondary trigger list reverses.

  Workaround: Delete & reconfigure any secondary triggers required so that the trigger list is ordered properly after a router reloads. If a mesage can match multiple secondary triggers, make sure that the most specific secondary trigger is configured before the less specific trigger.

- CSCse45533: MLR: Messages routed using MLR result gt may contain invalid es in cdpa

  Symptoms: Messages which are MLR routed with a MLR gt result may contain invalid data in the encoding scheme byte of the called party address.

  Conditions: Problem is random. It may occur when MLR routes a messages received with **gt cdpa** to a new **gt cdpa**.

  Workaround: Avoid using a **result gt** if possible.

- CSCse17165: ITP MAPUA: max-return setting not applied

  Symptoms: ITP returns a number of triplets higher than the value set for max-return under the gsm-authent-vlr configuration of cs7 mapua.

  Conditions: MAPUA client requests a number of fresh triplets higher than max-return. HLR/AuC returns a number of triplets higher than max-return.

  Workaround: Cofigure the mapua client to request a number of triplets below or equal to max-return.

- CSCse49476: 12.2(25)SW5 - ITP crash on cs7_mlr_result_group_lookup

  Symptoms: ITP crash info:

cs7_mlr_result_group_lookup , cs7_sms_result_group_lookup , cs7_sms_route , cs7_sms_gsmMapMoForwardSmRcv , cs7_sms_gsmMapRcvMsg.

An ITP running with the SMS_MO Proxy feature may reload if both of the following conditions are met:

1) The SMS rules are using MLR result groups, AND

2) There are currently no available members within the MLR result group.

Workound : The short-term workaround is to create identical SMS result groups and use them explicitly in the SMS rulesets.

Release 12.2(25)SW6

- CSCsd63762: Network-appearance showing as negative number in ITP config

  Symptoms: The **network-appearance** command in AS configuration mode can range from 1 to 4294967295. However, when configuring values higher than 2147483647 (2 pow 31-1), the **network-appearance** shows up as a negative number in the router configuration. Upon reboot, the router will display an error when tries to configure such a network appearance.

  Workaround: Do not configure **network-appearance** values higher than 2147483647.

- CSCsc78421: ITP: HSL links duplicate sscop retransmissions

  Symptoms: An ITP configured with HSL links may sometimes retransmit lost SD PDUs twice instead of just once

  Conditions: This symptom occurs when a PDU must be transmitted followed by a POLL. The PDU is lost in flight. The remote side responds with a USTAT indicating the missing PDU followed by a STAT in response to the POLL (also indicating the missing PDU). The ITP will incorrectly retransmit the SD PDU in response to the USTAT and the STAT.

  Workaround: There is no workaround.

- CSCsd30900: ITP: Crash when loadshare seed bound to different ASPs on SG mates

  Symptoms: Under rare conditions, the ITP may reload.

  Conditions: The following conditions must all be present to observe the problem:

  – Two ITPs are configured as SG mates.
  – An AS with at least two ASPs and traffic mode of loadshare bindings is configured on both ITPs.
  – Each ITP receives a packet destined for the AS with the same loadshare seed (for example, CIC, SLS), and each ITP binds the loadshare seed to a different ASP.

  Workaround: There is no workaround.

- CSCsd35259: ITP: IMA PA ports switch from LINE to INTERNAL clock on port 0 down

  Symptoms: The IMA PA, by default, is configured on all ports to derive its TX clocking from the LINE. In this configuration, when the first port (port 0) goes down, all ports on the card will switch from LINE to INTERNAL clocking. This action may cause HSL based SS7 links to go down and come back up at the time of the switch.

  Conditions: The ports must be clocked from LINE for this issue to occur.

  Workaround: Configure the following on each IMA/HSL:

  clock source common 7
  clock source line

The number 7 is any unused and shutdown port on the IMA PA. This effectively sets each port to derive its clock from port 7 and then sets it back to source it from line.

Release 12.2(25)SW5

- CSCsb91588: ITP SMS MO Proxy dlg fails when adding origin IMSI

  Symtoms: This case exposes a defect introduced when the “obtain origin IMSI” feature was added in 12.2(25)SW3. The problem is triggered when the origin IMSI is obtained and subsequently inserted into the proxied MO-FORWARD-SM dialogue. The addition of the IMSI is enough to exceed the maximum size that SCCP or MTP3 can transport without segmentation. In the 12.2(25)SW3 release, the intended behavior is that the ITP should build the proxied MO dialogue identical to the original MO message.

  Conditions: Either of the following might be occurring:

  - MAP version 3 MO-FORWARD-SM message received from MSC does not contain an IMSI, and the length of the MSU received from the MSC is greater than 263 octets (including SI).
  - SMS MO Proxy successfully obtains the origin IMSI, as requested by a matched SMS rule with 'result obtain-orig-imsi'.

  Workaround: You can unconfigure the rule which obtains the origin IMSI or configure the SMS MO Proxy for version 2. This would have the SMS MO Proxy negotiate all MO-FWD-SM dialogues down to version 2.

- CSCsb92248: running-config stores HSI SSCOP timer commands in wrong order

  Symptoms: ITP reports Timer_POLL or Timer-Keepalive errors on boot. For example:

  ```
  new Timer_POLL 125 greater than Timer_Keepalive 100. Change keepalive_timer first
  new Timer-Keepalive 250 greater than Timer_Idle 100. Change idle_timer first
  ```

  Conditions: HSL sscop timer commands are stored in incorrect order.

  Workaround: There is no workaround.

- CSCsc02671: ITP: Remote Inhibit Test not sent in ITU CSCsc12670 ITP: wrong effective dest address in **show cs7 linkset** details

  Symptoms: When the ITP receives a remote inhibit, it is supposed to start MTP3 timer T23. The ITP is supposed to send a Remote Inhibit Test message every T23. This prevents the link from being stuck in inhibit mode if the far-end uninhibits the link, but during this process the uninhibit message is lost. The ITP is not sending the Remote Inhibit Test message.

  Conditions: This problem only occurs when the variant is ITU and a remote node inhibits a link.

  Workaround: Under normal conditions no action is required. When the remote side unihibits the link, this clears the remote inhibit status. The Remote Inhibit Test is designed to catch the case where the remote unihbiit message is lost. If this occurs, a shut/no shut of the linkset will correct the inhibit status.

- CSCsc34914: ITP Crashes if PGW is shut down

  Symptoms: The ITP crashes when an M3UA link that is established to a PGW 9.5(2) host is torn down when the PGW shuts down.

  Workaround: There is no workaround.

- CSCsc46651: ITP: SCCP Instance conversion corrupts certain MSUs

  Symptoms: MSU is corrupted during instance conversion.

Conditions: This occurs when converting an MSU from one instance to another where the MSU is formated with the SCCP portion containing the data in between the calling and called parties.

Workaround: Send properly formated MSUs with the data at the end of the MSU.

- CSCsc51378: ITP: Upgrade from 12.2(4)MB10 or earlier to 12.2(25)SW4a fails

  Symptoms: Under certain conditions, an upgrade to release 12.2(25)SW4a may result in config corruption. Errors similar to the following are detected at bootup:

```
%Error: Existing linkset with adjacent pc 0 cannot be changed to a new adjacent pc.
 accounting
   ^
% Invalid input detected at '^' marker.

 link 0 sctp 192.168.20.13 192.168.30.13 4096 4096
   ^
% Invalid input detected at '^' marker.

 link 1 sctp 192.168.30.13 192.168.20.13 4097 4097
   ^
% Invalid input detected at '^' marker.

 route all table system
         ^
% Invalid input detected at '^' marker.
```

  Conditions: The problem occurs when upgrading directly from Cisco IOS Release 12.2(4)MB10 or earlier to release 12.2(25)SW4a.

  Workaround: Upgrade the ITP from Cisco IOS Release 12.2(4)MB10 or earlier to release 12.2(25)SW3, and then upgrade from release 12.2(25)SW3 to release 12.2(25)SW4a.

- CSCsc62555: ITP SGMP: Binding is active on receiving ITP, inactive on other ITP

  Symptoms: For this CDETS fix, the logic is that a new binding is established when the ASP is already active on both ITPs. In this case, the binding is active on the receiving ITP but inactive on the other ITP.

  Workaround: There is no workaround.

Release 12.2(25)SW4

Resolved Caveats Cisco IOS Release 12.2(25)SW4

- CSCei61732: Cisco IOS may permit arbitrary code execution after exploitation of a heap-based buffer overflow vulnerability. Cisco has included additional integrity checks in its software, as further described below, that are intended to reduce the likelihood of arbitrary code execution.

  Cisco has made free software available that includes the additional integrity checks for affected customers.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20051102-timers.shtml

- CSCsa98287: Adding link to shutdown linkset activates link and linkset

  Symptoms: Running ITP software, adding an SS7 link to an existing linkset that is in the “shutdown” state will not prevent the new link from becoming available and causing the linkset to become available as well.

  Conditions: The linkset must be in the shutdown state.

Workaround: Once the new link is added, issue a 'no shutdown' and then a 'shutdown' command on the linkset and the linkset will revert to the 'shutdown' state. The new link will become unavailable.

- CSCsa98311: Traceback on alternate when link is added on manager

  Symptoms: In software versions through 25SW2, if a link is added on the master for a linkset that does not exist on the alternate, the following tracebacks will be generated on the alternate:

  ```
  %CS7CHKPT-3-INTERR: Could not find linkset linkset_name in inst 0 for link utilization
  %CS7CHKPT-3-MSGERR: Received short Link_Util msg: 65 instead of 37386
  ```

  Workaround: There is no workaround.

- CSCsb02059: Hop counter decremented twice when GTT result is an AS

  Symptoms: Hop Counter for XUDT messages is decremented twice when GTT result is an AS

  Conditions: SCCP traffic using message type XUDT on a 7500 with MTP3 offload configured Traffic must be GTT routed to an AS result.

  Workaround: Turn off MTP3 offload

- CSCsb04493: Tracebacks upon configuring new instance on Group Manager

  Symptoms: Tracebacks may be observed on an ITP Group Alternate upon configuring **cs7 instance** *instance-number* **instance** *instance-number* **variant** {**ansi** | **china** | **itu** | **ttc**} on the ITP Group Manager.

  Workaround: There is no workaround.

- CSCsb04849: ITP Generates traceback when receiving SCCP with GTI = 8

  Symptoms: When ITP receives an SCCP message containing GTI (Global Title Indicator) equals 8, a traceback will be generated. The router will not crash, and there will be no impact in the performance of the device.

  Workaround: There is no workaround. ITP only supports GTI 2 and 4. This can be considered a cosmetic issue.

- CSCsb16386: ITP not performing GTT when M3UA ASP shares PC with ITP

  Symptoms: When ITP and an associated AS share the point code (both have the same point code), SCCP packets arriving to the ITP will be forwarded immediately to the ASP, instead of performing global title translation (GTT) first.

  Workaround: configure different point codes in the ASP and ITP.

- CSCsb19607: Link activation fails if apc matches local pc of another instance

  Symptoms: Link does not activate if adjacent point code is identical to a local point code of another instance on the ITP.

  Conditions: MTP3 offload must be enabled and **cs7 multi-instance** must be configured. Adjacent pointcode must be identical to local point code of another instance. This problem exists in 12.2-25.SW3.

  Workaround: If the configuration is saved and the ITP loaded with this as it's starting configuration, the links will activate normally.

- CSCsb33974: ISUP MSUs with CIC 9, 10, 17 not sent on correct link

  Symptoms: The ITP should send ISUP MSUs with the same SLS on the same link in order to guarantee that they arrive in order. But when **cs7 distribute-sccp-unsequenced** is configured and the ITP routes an ISUP message with CIC 9, 10, or 17, the ITP distributes the MSUs using a round-robin. This can cause MSUs to arrive out of sequence at the destination.

Conditions: The code for sccp distributed sls was not checking if the packet was SCCP. It was assuming the packet was an SCCP, and looking at the SCCP Message type and class, which are always in the same place in an SCCP message. If the message type field was UDT (9) XUDT (17) or LUDT (19), the class field was checked. If the class field is 0, it is assumed to be sccp unsequence, and the sls is ignored and instead uses a round-robin load distribution

For an ISUP message, this means that the code was actually examining the CIC field. If the CIC field was 9 00 (hex 0900), 17 00 (hex 1100), or 19 00 (hex 1300) the message was routed using round robin.

Workaround: There is no workaround.

- CSCsb64543: Linkset & route available, but destination INACC

  Symptoms: If SS7 links bounce due to service provider problem, after the links come back in service, some of the destinations would show as INACC even though the links to that destination are active and route to that destination is available. Signalling traffic seems to be flowing as normal.

  Workaround: Re-enter the **update route** command used to create those routes, and the destination status will get reset to the correct state. You could take the route commands from the **show running config** output and cut-and-paste them back in once you are in **config-cs7-rt** submode.

Open Caveats Cisco IOS Release 12.2(25)SW4

There are no open caveats reported for Cisco IOS Release 12.2(25)SW4

Release 12.2(25)SW3b

Resolved Caveats—Cisco IOS Release 12.2(25)SW3b

- CSCei76358: cleanup of user interface data

Through normal software maintenance processes, Cisco is removing deprecated functionality. These changes have no impact on system operation or feature availability.

Open Caveats—Cisco IOS Release 12.2(25)SW3b

There are no open caveats in this release.

Release 12.2(25)SW3a

Resolved Caveats—Cisco IOS Release 12.2(25)SW3a

- CSCef68324: Cisco Internetwork Operating System (IOS) software is vulnerable to a Denial of Service (DoS) and potentially an arbitrary code execution attack from a specifically crafted IPv6 packet. The packet must be sent from a local network segment. Only devices that have been explicitly configured to process IPv6 traffic are affected. Upon successful exploitation, the device may reload or be open to further exploitation.

  Cisco has made free software available to address this vulnerability for all affected customers.

  More details can be found in the security advisory that is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050729-ipv6.shtml.

Open Caveats—Cisco IOS Release 12.2(25)SW3a

There are no open caveats in this release.

Release 12.2(25)SW3

Open Caveats—Cisco IOS Release 12.2(25)SW3

There are no open caveats in this release.

Resolved Caveats—Cisco IOS Release 12.2(25)SW3

- CSCed83705: ITP: Alignment traceback upon issuing ping cs7 stop

  Symptoms: On a Cisco ITP 7507 running IOS version 12.2(20)SW, when using cs7 ping, alignment corrections & traceback errors may be seen occasionally. This does not seem to have any impact on operation however.

  Workaround: There is no workaround.

- CSCee13367: CS7 ping fails to report if RTT is over 1 second

  Symptoms: When running the Cisco IP Transfer Point software versions 12.2(4)MB13 or 12.2(20)SW no report of success or failure may be seen under some circumstances.

  Conditions: This only occurs if the RTT between the ping endpoints is over 1 second (over satellite links for example). This is known to be a problem due to the time taken to set up the Q.751 traffic test - by the time the test is setup over slow links the test is already finished and no data is sent to test.

  Workaround: A workaround is to specify a test duration greater than the RTT between the test endpoint using the **cs7 ping -duration** command.

- CSCeg18352: ITP: ATM PA BITS clock source in show command and need syslog event

  Symptoms: For the given ATM PA, the clock source can be LINE and that clock source can be distributed to other lines. When the LINE fails, the ATM PA reverts back to INTERNAL clock source. The current clock source (LINE, INTERNAL or COMMON) could not be determined from the show commands.

  The **show controller ATM** has been modified to display the current clock source.

  Conditions: For the ATM PA, LINE source of the clock fails, there is no indication or syslog event to tell the operator about it.

  Workaround: There is no workaround.

- CSCeh13554: ITP: Q782 Test 9.4.1 fails for ITU without TFP option

  Symptoms: When the ITP begins routing on an alternate route to a destination, it sends a preventive TFP to prevent circular routing. When the ITP switches to using the normal route for the destination, the ITP should send a TFA on the alternate route, to indicate that node may now route through the ITP for that destination. But the ITP does not send this TFA in ITU networks without the national TFR option configured.

  Workaround: The ITP will send a TFA on the alternate linkset when it receives an RSP poll message. The adjacent node for the alternate route should send the ITP an RSP every T10.

- CSCeh15067: ITP: Management MSU for XUA PC processed by ITP

  Symptoms: When the ITP receives an MSU destined for an xUA point code with SI set to 0, 1, or 2 (ANSI Only), the ITP will process the MSU as if it were destined for the ITP's PC.

SI 0 is for MTP3 Network Management messages while SI 1 is for Link Test Messages. SI 2 is used in ANSI for Link Test Messages.

Conditions: This occurs when ITP configured with an xUA point code.

Workaround: There is no workaround.

- CSCeh16859: ITP: Management MSU for XUA PC processed by ITP

  Symptoms: Subsystem 12 on ITP will be reported "not available" but not subsystem 112.

  Conditions: This occurs if the connection between the ITP and the SCP is dropped.

  Workaround: This issue is cosmetic and has no operational impact.

  Further Problem Description: When the connection is established, there is no message "Subsystem 12 at 4608 is available." It is announced as unavailable instead. This issue will require a software fix.

- CSCsa59599: ITP: MTU on serial interface reset to 1500 after encapsulation change

  Symptoms: After changing encapsulation types on a serial interface, the physical MTU of the interface resets back to the default value of 1500 bytes.

  Conditions: The issue only appears to affect ITP software.

  Workaround: There is no workaround other than manually reconfiguring the interface MTU.

  Further Problem Description:< The problem may manifest itself after a router reset if a serial interface has a non default encapsulation type. That is, if the serial interface is using an encapsulation other than HDLC.

- CSCsa72249: ITP: ASP in Blocking state does not correctly respond to an ASPUP

  The Cisco IP Transfer Point will incorrectly respond to an ASPUP message received by M3UA ASP in Blocking state with an ASPUPAK, instead it should send an error message.

  Workaround: There is no workaround although the ITP will correctly respond to an ASPAC message on the same M3UA ASP with an error - which will prevent any operation impact (the ASP cannot become active). This has been observed in Cisco IOS versions 12.2(25)SW and 12.2(25)SW1.

- CSCsa78896: ITP output TFP messages for UNAVAIL links while debug is enabled.

  Symptoms: When a cs7 linkset is in UNAVAIL or SHUTDOWN state and the only route to the adjacent point code X is via that linkset (i.e. this APC is inaccessible), then another destination Y becomes inaccessible, the ITP outputs a debug message on the console indicating a TFP was sent to X concerning destination Y if **debug cs7 mtp3 mgmt packet** is enabled. In reality, no TFP is actually sent to X. The debug message is misleading, and it does not cause any ITP functional problem. The same is true of other MTP3 management messages.

  Conditions: Cisco IOS Release 12.2(25)SW1

  Workaround: There is no workaround.

- CSCsa88289: ITP: ATM line protocol is down after unconfig atm nni

  Symptoms: On Cisco 7500 series and Cisco 7301 series platforms running ITP software, when ATM interfaces (PA-A3-8T1IMA, PA-A3-8E1IMA, PA-A3-OC3) are configured as a NNI interface (atm nni) to be used as High Speed SS7 Links, and then the configuration (atm nn i) is removed, the line protocol may not be restored to "up" as shown under the **show interfaces** output.

  Workaround: The reload procedure restores the atm interface to "line protocol up" for the same configuration.

- CSCsa92616: ITP: SGM client cannot monitor link utilization

Symptoms: The Cisco Signalling Gateway Manager Client is unable to monitor link utilization threshold status compared when the IP Transfer Point is running Cisco IOS versions 12.2(25)SW1 and 12.2(25)SW2.

Workaround: There are two possible workarounds:

- Use an earlier Cisco IOS version of the IP Transfer Points.
- Within the client, you can right-click on the link in the left hand panel of the client where it show the SLC value and choose View->Real-time Data And charts. This will display the current utilization values in a panel that will update itself every 15 seconds.

Release 12.2(25)SW2

Caveat Advisory - Resolved Caveats Cisco IOS Release 12.2(25)SW2

- CSCsa81379: Deprecate NetFlow Feature Acceleration

  NetFlow Feature Acceleration has been deprecated and removed from Cisco IOS. The global command **ip flow-cache feature-accelerate** will no longer be recognized in any IOS configuration.

  If your router configuration does not currently contain the command **ip flow-cache feature-accelerate**, this change does not affect you.

  The removal of NetFlow Feature Acceleration does not affect any other aspects of Netflow operation, for example Access-list processing. The features are separate and distinct.

  Cisco Express Forwarding (CEF) supercedes the deprecated NetFlow Feature Acceleration.

  Additionally, the following MIB objects and OIDs have been deprecated and removed from the netflow mib (CISCO-NETFLOW-MIB):

```
cnfFeatureAcceleration        1.3.6.1.4.1.9.9.99999.1.3
cnfFeatureAccelerationEnable  1.3.6.1.4.1.9.9.99999.1.3.1
cnfFeatureAvailableSlot       1.3.6.1.4.1.9.9.99999.1.3.2
cnfFeatureActiveSlot          1.3.6.1.4.1.9.9.99999.1.3.3
cnfFeatureTable               1.3.6.1.4.1.9.9.99999.1.3.4
cnfFeatureEntry               1.3.6.1.4.1.9.9.99999.1.3.4.1
cnfFeatureType                1.3.6.1.4.1.9.9.99999.1.3.4.1.1
cnfFeatureSlot                1.3.6.1.4.1.9.9.99999.1.3.4.1.2
cnfFeatureActive              1.3.6.1.4.1.9.9.99999.1.3.4.1.3
cnfFeatureAttaches            1.3.6.1.4.1.9.9.99999.1.3.4.1.4
cnfFeatureDetaches            1.3.6.1.4.1.9.9.99999.1.3.4.1.5
cnfFeatureConfigChanges       1.3.6.1.4.1.9.9.99999.1.3.4.1.6
```

Release 12.2(25)SW1

Open Caveats—Cisco IOS Release 12.2(25)SW1

- CSCsa56453: DSMR: detailed show rule cmd needs cdr-service-queue parameter

  Symptoms: This issue may cause a crash even without the CDR variable because of string buffer overflow. The crash may happen if the maximum values are set for each parameter.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(25)SW1

- CSCeg08298: ITP: SCCP dest stuck in congestion when congested link fails

Symptom: If a link in a multilink linkset fails while it is congested, and the other links in the linkset are available and not congested, GTT will treat destinations that use the linkset as still being congested, resulting in lost MSUs.

Workaround: The problem will clear when the failed link recovers. Deleting and adding back the failed link will also clear the problem.

- CSCeg37718: ITP: Ordered multihomed address list cause unbalanced load sharing

  Symptom: The incoming TDM traffic is evenly distributed among the links within the incoming TDM linkset. When he ITP is configured for SCTP multihoming in configurations that balances the IP traffic over multiple IP interfaces, the SCTP traffic is not properly balanced over the IP interfaces.

  The **show interface** command statistics for the IP interfaces being used will have a large imbalance between the input and output packet statistics for the sending and receiving interfaces.

  Conditions: This problem was seen in 12.2(23)SW1. With a configuration similar to the following:

```
ITP-A
cs7 local-peer 7000 local-ip 10.0.0.1 local-ip 10.0.0.3
cs7 local-peer 8000 local-ip 10.0.0.3 local-ip 10.0.0.1
cs7 linkset to-ITP-B link 0 sctp 10.0.0.5 10.0.0.7 7000 7000 link 1 sctp 10.0.0.7
10.0.0.5 8000 8000
ITP-B cs7 local-peer 7000 local-ip 10.0.0.5 local-ip 10.0.0.7
cs7 local-peer 8000 local-ip 10.0.0.7 local-ip 10.0.0.5
cs7 linkset to-ITP-B link 0 sctp 10.0.0.1 10.0.0.3 7000 7000 link 1 sctp 10.0.0.3
10.0.0.1 8000 8000
```

  Workaround: There is no workaround.

- CSCeg50304: ITP:SCTP assoc statistics double counting packets

  Symptom: The SCTP statistics for ordered and unordered chunks are reported higher than the number of chunks that were actually transmitted.

  Conditions: This problem occurs in 12.2 MB11 and on.

  Workaround: There is no workaround.

- CSCeg50319: ITP:SCTP show output reports checksum type as nego

  Symptom: The SCTP show command **show ip sctp association parameters** reports the checksum type as negotiable (nego) after the association is established.

  Conditions: This problem occurs in 12.2 MB9 and on.

  Workaround: Shut and no shut the link that reports the negotiable checksum status.

- CSCsa42016: TP:TTC A/B combined linkset loadsharing and TFP restart suppression

  Symptom: This report addresses two issues found with the ITP software only using the TTC SS7 Variant.

  1) TFP messages are broadcast when a link becomes available for all destinations in the MTP3 routing table that are unavailable. The appropriate behavior for the TTC variant is not to broadcast the TFP in this circumstance.

  2) ITP currently implements an enhanced loadsharing feature when a combined linkset is configured. For the TTC variant, it is sometimes desirable for loadsharing between linkset in a combined linkset to be strictly done based on the A/B bit in the SLS field instead of doing enhanced loadsharing. The current ITP implementation only provides enhanced loadsharing.

  Conditions: These issues are only applicable for the TTC variant based ITP systems.

  Workaround: There is no workaround.

- CSCsa42261: ITP-S: instance conversion incorrectly codes spare bits for SCCP

Symptom: 0xF for last nibble is seen during instance conversion from ITU to ANSI when going from odd to even number of digits.

Conditions: Performing E214 to E212 conversion between ITU and ANSI instance.

Workaround: There is no workaround.

- CSCsa54632: memory leak in ip input on itp router

  Symptoms: The ITP SCCP-User Adaptation (SUA) Signalling Gateway (SG) may leak buffers in the IP input process.

  Condition: The problem happens when both of the following conditions occur:

  1) The sending SUA Application Server Process (ASP) has sent a Connectionless Data (CLDT) message that is too large to fit into a single Message Signal Unit (MSU).

  2) The ASP has not indicated “return on error” in the SUA PROTOCOL_CLASS parameter.

  Workaround: Configure the ASPs to discontinue sending messages too large to fit in a single MSU, or configure the ASPs to always indicate “return on error” within generated CLDT messages.

- CSCsa57212: ITP S: memory leak per telnet session where config mode is used

  A router running Cisco IOS Release 12.2(25)SW may experience a memory leak in the *Dead* process. This appears to be caused by opening a telnet session and entering configuration changes.

  Conditions: This occurs when you use configuration sessions on terminals other than the console.

  Workaround: Limit the number of open telnet sessions for configuration changes. Run in HSA mode where the configuration is not synched to the secondary RSP.This fixes the memory leak but leaves the box open to longer down time should the active RSP fail. If the memory leak occurs and memory is low, perform a switchover if you are in RPR+ or SSO mode. Use the **redundancy force-swithover** command to achieve this. The memory will be reclaimed on the newly active RSP with minimal or no traffic losss. The problem will still occur and the memory loss can continue, but memory can be temporarily reclaimed using this fix.

Release 12.2(25)SW

Caveat Advisories - Resolved Caveats

- CSCef60659: More stringent checks required for ICMP unreachables

  A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled “ICMP Attacks Against TCP” (draft-gont-tcpm-icmp-attacks-03.txt).

  These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

  1. Attacks that use ICMP “hard” error messages
  2. Attacks that use ICMP “fragmentation needed and Don’t Fragment (DF) bit set” messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
  3. Attacks that use ICMP “source quench” messages

  Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

  Multiple Cisco products are affected by the attacks described in this Internet draft.

Cisco has made free software available to address these vulnerabilities. In some cases 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-20050412-icmp.shtml.

The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at: http://www.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en.

- CSCsa59600: IPSec PMTUD not working [after CSCef44225]

  A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled "ICMP Attacks Against TCP" (draft-gont-tcpm-icmp-attacks-03.txt).

  These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

  1. Attacks that use ICMP "hard" error messages
  2. Attacks that use ICMP "fragmentation needed and Don't Fragment (DF) bit set" messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
  3. Attacks that use ICMP "source quench" messages

  Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

  Multiple Cisco products are affected by the attacks described in this Internet draft.

  Cisco has made free software available to address these vulnerabilities. In some cases 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-20050412-icmp.shtml.

  The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at: http://www.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en.

- CSCef43691: L2TPv3 and UTI sessions doing PMTUD vulnerable to spoofed ICMP paks

  A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled "ICMP Attacks Against TCP" (draft-gont-tcpm-icmp-attacks-03.txt).

  These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

  1. Attacks that use ICMP "hard" error messages
  2. Attacks that use ICMP "fragmentation needed and Don't Fragment (DF) bit set" messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
  3. Attacks that use ICMP "source quench" messages

  Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

  Multiple Cisco products are affected by the attacks described in this Internet draft.

Cisco has made free software available to address these vulnerabilities. In some cases 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-20050412-icmp.shtml.

The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at: http://www.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en.

- CSCef44225: IPSec (ESP-AH) doing PMTUD vulnerable to spoofed ICMP packets

  A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled "ICMP Attacks Against TCP" (draft-gont-tcpm-icmp-attacks-03.txt).

  These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

  1. Attacks that use ICMP "hard" error messages
  2. Attacks that use ICMP "fragmentation needed and Don't Fragment (DF) bit set" messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
  3. Attacks that use ICMP "source quench" messages

  Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

  Multiple Cisco products are affected by the attacks described in this Internet draft.

  Cisco has made free software available to address these vulnerabilities. In some cases 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-20050412-icmp.shtml.

  The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at: http://www.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en.

- CSCef44699: GRE and IPinIP doing PMTUD vulnerable to spoofed ICMP packets

  A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled "ICMP Attacks Against TCP" (draft-gont-tcpm-icmp-attacks-03.txt).

  These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

  1. Attacks that use ICMP "hard" error messages
  2. Attacks that use ICMP "fragmentation needed and Don't Fragment (DF) bit set" messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
  3. Attacks that use ICMP "source quench" messages

  Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

  Multiple Cisco products are affected by the attacks described in this Internet draft.

Cisco has made free software available to address these vulnerabilities. In some cases 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-20050412-icmp.shtml.

The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at: http://www.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en.

- CSCef61610: Incorrect handling of ICMPv6 messages can cause TCP performance problems

  A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled "ICMP Attacks Against TCP" (draft-gont-tcpm-icmp-attacks-03.txt).

  These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

  1. Attacks that use ICMP "hard" error messages
  2. Attacks that use ICMP "fragmentation needed and Don't Fragment (DF) bit set" messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
  3. Attacks that use ICMP "source quench" messages

  Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

  Multiple Cisco products are affected by the attacks described in this Internet draft.

  Cisco has made free software available to address these vulnerabilities. In some cases 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-20050412-icmp.shtml.

  The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at: http://www.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en.

- CSCsa61864: Enhancements to L2TPv3 PMTUD may not work [Follow-up to CSCef43691]

  A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled "ICMP Attacks Against TCP" (draft-gont-tcpm-icmp-attacks-03.txt).

  These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

  1. Attacks that use ICMP "hard" error messages
  2. Attacks that use ICMP "fragmentation needed and Don't Fragment (DF) bit set" messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
  3. Attacks that use ICMP "source quench" messages

  Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

  Multiple Cisco products are affected by the attacks described in this Internet draft.

Cisco has made free software available to address these vulnerabilities. In some cases 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-20050412-icmp.shtml.

The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at: http://www.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en.

- CSCed78149: TCP connections doing PMTU discovery vulnerable to spoofed ICMP pkts

  A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled "ICMP Attacks Against TCP" (draft-gont-tcpm-icmp-attacks-03.txt).

  These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

  1. Attacks that use ICMP "hard" error messages
  2. Attacks that use ICMP "fragmentation needed and Don't Fragment (DF) bit set" messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
  3. Attacks that use ICMP "source quench" messages

  Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

  Multiple Cisco products are affected by the attacks described in this Internet draft.

  Cisco has made free software available to address these vulnerabilities. In some cases 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-20050412-icmp.shtml.

  The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at: http://www.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en.

- CSCsa52807: L2TP doing PMTUD vulnerable to spoofed ICMP paks

  A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled "ICMP Attacks Against TCP" (draft-gont-tcpm-icmp-attacks-03.txt).

  These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

  1. Attacks that use ICMP "hard" error messages
  2. Attacks that use ICMP "fragmentation needed and Don't Fragment (DF) bit set" messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
  3. Attacks that use ICMP "source quench" messages

  Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

  Multiple Cisco products are affected by the attacks described in this Internet draft.

Cisco has made free software available to address these vulnerabilities. In some cases 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-20050412-icmp.shtml.

The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at: http://www.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en.

Open Caveats—Cisco IOS Release 12.2(25)SW

No open caveats specific to Cisco IOS Release 12.2(25)SW require documentation in the release notes.

Resolved Caveats—Cisco IOS Release 12.2(25)SW

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(25)SW. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

Table 5 Resolved Caveats for Cisco IOS Release 12.2(25)SW

DDTS ID Number	Description
CSCef29094	ITP: crash during display of sh cs7 gtt config Symptom: ITP may crash during **sh cs7 gtt** config. Conditions: This crash is caused because of a prompt stuck at the automore state and then the GTT database is modified. If the propmt is continued is there is a small chance of hitting a crash due to accessing freed memory. Workaround: Whenever the MORE prompt is seen during the display of GTT config, hit Q and re-enter the display command. Avoid doing show commands while bulk loading or provisioning data.
CSCef31588	ITP: No response to RCP when summary route is available Symptom: When summary route exists, and the ITP receives a cluster poll message (RCP or RCR) for a cluster that does not exist in the routing table, but is accessible by the summary route, the ITP does not respond to the poll message with a TCA. This causes the adjacent node to treat the cluster as unavailable when it is accessible. Workaround: Provision the cluster route or provision a full point code that is available within the cluster. For example if a summary route for 4-0-0/8 exists and is available, and the ITP is receiving poll messages for cluster 4-4-0 which does not exist as a provisioned route, the ITP will not respond to the poll. If the user provisions the cluster route 4-4-0/16, the ITP will respond correctly to the poll. Or if the user provisions a full point code route to 4-4-1 and this destination is available, the ITP will respond correctly to the poll message.

Table 5 Resolved Caveats for Cisco IOS Release 12.2(25)SW (continued)

DDTS ID Number	Description
CSCef38050	SUA Source and Destination addresses limited to 15 digits Symptom: SCCP Calling and Called Party Addresses are truncated to 15 digits when sent to and received from an SUA AS. For example: • Existing functionality-Incoming SCCP CdPA = 123456789012345678901234567 8 ITP config: gta 123456789012345 pcssn 4601 pcssn (where 4601 represents an SUA AS PC) Outgoing SUA Source Address (CdPA) = 123456789012345 • Required functionality- Incoming SCCP CdPA = 123456789012345678901234567 8 ITP config: gta 123456789012345 pcssn 4601 pcssn Outgoing SUA Source Address (CdPA) = 123456789012345678901234567 8 Conditions: This limitation exists in all ITP images supporting SUA. Workaround: This has been base behavior on the ITP since SUA SG function was released. There is no workaround.
CSCef74580	ITP cs7 monitor did not send traffic from high speed int (atm) to tcp Symptom: CS7 Monitor will stop working on High speed interfaces (atm) if ITP version Workaround: No workaround is available.
CSCef85587	ITP: ASP-UP from ASP ignored unless sent twice Symptom: ASP-UP message from m3ua/sua ASP is ignored until retried. Then 2 ASP-UP-ACK messages are returned by the ITP. Conditions: ITP with m3ua or sua offloaded. ASP sends ASP-UP immediately upon sctp association establishment. Workaround: Repeat ASP-UP message. Further Problem Description: The ASP sends ASP_UP immediately following the successful sctp association establishment, and this has uncovered a window where the association is established but xua is not ready to receive data yet. This data is held by sctp until another “data received” signal occurs and all received data is processed. This only happens with xua offloaded, because the offload scenario requires an additional exchange between the rsp and vip when setting up an association. Resolved by adding vip code to check for received data following this exchange.

Table 5 Resolved Caveats for Cisco IOS Release 12.2(25)SW (continued)

DDTS ID Number	Description

CSCef84139	ITP: malloc failures when running m3ua with instance conversionports not put in OOS-DSBLD as requested when circuits are deleted
	Symptom: Malloc failure while running m3ua:
	`00:50:32: %SYS-2-MALLOCFAIL: Memory allocation of 65544 bytes failed from 0x404`
	`Pool: Processor  Free: 2153168  Cause: Memory fragmentation Alternate Pool: None`
	`Free: 0  Cause: No`
	`Alternate pool`
	
	`-Process= "MTP3 Input", ipl= 0, pid= 117 -Traceback= 40492B2C 40496B3C 404A78B4`
	`40E49DB0 40EA694C`
	`40EA6F74 40E4ADCC 40E44`
	`00:50:32: %CS7MTP3-7-INTERR: Internal Software Error Detected: CS7 cs7_convert_e`
	`-Traceback=`
	`40EA6968 40EA6F74 40E4ADCC 40E4B780 40E4B97C 40E4C2F0 40E4C454`
	`00:50:32: %CS7MTP3-7-INTERR: Internal Software Error Detected: CS7 cs7_convert_e`
	`-Traceback=`
	`40EA6968 40EA6F74 40E4ADCC 40E4B780 40E4B97C 40E4C2F0 40E4C454`
	`00:50:32: %CS7MTP3-7-INTERR: Internal Software Error Detected: CS7 cs7_convert_e`
	`-Traceback=`
	`40EA6968 40EA6F74 40E4ADCC 40E4B780 40E4B97C 40E4C2F0 40E4C454`
	`00:50:32: %CS7MTP3-7-INTERR: Internal Software Error Detected: CS7 cs7_convert_e`
	`-Traceback=`
	`40EA6968 40EA6F74 40E4ADCC 40E4B780 40E4B97C 40E4C2F0 40E4C454`
	`00:50:32: %CS7MTP3-7-INTERR: Internal Software Error Detected: CS7 cs7_convert_e`
	`-Traceback=`
	`40EA6968 40EA6F74 40E4ADCC 40E4B780 40E4B97C 40E4C2F0 40E4C454`
	`00:50:32: %CS7MTP3-7-INTERR: Internal Software Error Detected: CS7 cs7_convert_e`
	`-Traceback=`
	`40EA6968 40EA6F74 40E4ADCC 40E4B780 40E4B97C 40E4C2F0 40E4C454......`
	`............................................`
	`etc`
	`etc.....`
	
	Conditions: ITP running m3ua with multiple instances and pc-conversion configured. Malloc failure appears after about 7 minutes at about 2000 MSU/sec.
	Workaround: None

CSCef69373	ITP stop processing for few sec if write mem is issue Symptom: If a write mem is issued in a ITP router, a pause in the processing of data packets may be observed, possibly leading to lost calls and failed links during times of otherwise high CPU utilization. Workaround: This problem was introduced in 12.2(23)SW. One workaround is to use 12.2(21)SW, if possible. Another workaround is to avoid issuing the **write mem** or **copy running-config startup-config** commands outside of a maintenance window or period of low traffic volume.
CSCef95065	ITP: route/gtt deploy adds delay to ss7 processing Symptom: During Route or GTT replace DB or Route/GTT deployment via SGM, processing time of SS7 traffic is impacted, causing added delay. Conditions: This could occur whenever the main RP is responsible for both SS7 processing and GTT/Route DB management. For example, this would not occur during VIP forwarding. Workaround: No work around in most circumstances. Best advice until fix is available, is to perform GTT and route management during off peak hours.

Table 5 Resolved Caveats for Cisco IOS Release 12.2(25)SW (continued)

DDTS ID Number	Description
CSCeg01587	ITP: F5 OAM HSL ATM loopback cell transmission broken Symptom: This caveat occurs on Cisco 7500-based ITP images using High Speed Signaling links when sending and receiving OAM cells. This issue occurs on all 7500 based ITP images prior to 25SW. The problem only exhibits itself when the far end of the ATM link is configured to generate OAM cells, or the ITP itself is configured to generate OAM cells via the 'oam-pvc' command under the interface. Workaround: The work around is to not use OAM cells on the High Speed Signaling links or disable the pvc state from being tied to the acknowledgment of OAM cells.Typically, the pvc will be shown as 'down' on one or both sides of the link and the ITP may show input errors on the ATM interface. The HSL link will eventually fail due to link test not being responded. This is due to the fact that the pvc is down and unable to pass traffic.

Release 12.2(23)SW1

Open Caveats—Cisco IOS Release 12.2(23)SW1

No open caveats specific to Cisco IOS Release 12.2(23)SW1 require documentation in the release notes.

Resolved Caveats—Cisco IOS Release 12.2(23)SW1

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(23)SW1. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

Table 6 Resolved Caveats for Cisco IOS Release 12.2(23)SW

DDTS ID Number	Description

CSCee36139	ITP:Source address selection algorithm fails for two addresses
	Symptom: When the Cisco IP Transfer Point (ITP) is configured with two source IP addresses under the 'local peer', only one IP address will be used. This can cause trouble for the SCTP link alignment when only one address is available.
	Conditions: This problem was seen in Cisco IOS Release 12.2(21)SW with the following configuration:
	`cs7 local-peer 8000`
	` local-ip 192.168.100.99`
	` local-ip 192.168.100.35`
	Workaround: There is no workaround.
	Further Problem Description: It seems to be an issue in the source selection algorithm.

Table 6 Resolved Caveats for Cisco IOS Release 12.2(23)SW (continued)

DDTS ID Number	Description
CSCee41388	ITP will send INIT immediately to second dest. address if lower Symptom: When configuring a SCTP link on the Cisco IP Transfer Point (ITP), the INIT message is sent only to one destination address under certain circumstance. Conditions: This problem happens when there are two destination addresses configured for the SCTP link on the ITP and the second address is lower than the first address. Thus the INIT message will send only to the second destination address. Workaround: Swap the order of IP addresses on the SCTP link to force the order in which the addresses are used in the INIT.
CSCee54303	ITP: Non-segmented XUDT messages failed with Unequipped SSN Symptom: ITP MAP Proxy application reports Subsystem Number (SSN) unequipped error: `May 7 14:20:19.415 GMT: %CS7SCCP-5-UNEQUIPSS: SCCP received message for invalid or unequipped SSN.` Conditions: An extended unitdata (XUDT) message is received carrying the response to the MAP Send Authentication Info message sent by the Cisco IP Transfer Point (ITP). Workaround: Disable sending an XUDT message type to the Cisco ITP in the SS7 network. Further Problem Description: The Cisco ITP performs final Global Title Translation (GTT) for the XUDT message received, and sets the routing indicator (RI) to “route-on-subsystem”. However, the delivery to the local subsystem fails as specified above.
CSCee56986	flapping primary address is used to send data Symptom: The primary address of a multihomed association can fail when the Round Trip Time exceeds RTO for the number of maximum retries. The Heartbeat exchange marks the primary address available again although the RTT still exceeds RTO, causing the primary address to fail again. The primary address can flap between inactive/active as long as RTT exceeds RTO. Conditions: Primary address flaps between active/inactive and is used to send data. Workaround: The RTO min and max should be adjusted for the longest anticipated delay among all of the paths.
CSCee86829	ITP: Need for SUA to generate XUDT messages based on ASP parms Symptom: The Cisco IP Transfer Point (ITP) does not send extended unitdata (XUDT) messages into the SS7 network for any non-segmented messages originated by SCCP User-Adaptation (SUA) Application Servers (AS). Workaround: There is no workaround for deployments requiring XUDTs and the SUA Application Server Processes (ASP) support sending either the HOP COUNTER or IMPORTANCE parameter.

Table 6 Resolved Caveats for Cisco IOS Release 12.2(23)SW (continued)

DDTS ID Number	Description

CSCee91201	cgspInstanceTable table not populated
	Symptom: The cgspInstanceTable in the CISCO-ITP-GSP-MIB is always empty when network-name not specified. The table being empty can prevent network management applications like Signalling Gateway Manager (SGM) from properly discovering the device.
	Conditions: This symptom can occur on all platforms running Cisco IOS Release 12.2(23)SW software.
	Workaround: Use the following commands on all impacted devices.
	`conf t`
	`cs7 network-name string`

CSCef08522	ITP: Destinations flapping between Restricted and Allowed
	Symptom: The Cisco IP Transfer Point (ITP) tries to use the summary route and the Virtual linkset from 1 to 0 as a backup for the full point code (PC) routes in instance 1. Since the full PC is down, the summary route is used to instance 0 and in instance 0, there is a full PC route going back to instance 1. This created a circular route within the ITP. This causes the destinations to change status rapidly from Restricted to Prohibited and back to Restricted. The ITP is designed to prevent message signal units (MSUs) from looping within the ITP. But in this situation, destinations could change status very rapidly, such as every couple milliseconds, which causes the linksets to go into level 3 congestion due to the high number of Transfer-Prohibited (TFP) messages and Transfer-Restricted (TFR) messages that the ITP is broadcasting.
	Conditions: This symptom occurs when the default conversion is going from instance 1 to instance 0, and does not have summary-routing-exception defined for instance 1.
	The problem did not occur with Cisco IOS Release 12.2(4)MB13, and did not occur in Cisco IOS Release 12.2(21)SW when summary-routing-exception is configured in instance 1.
	Workaround: When configuring the default pc-conversion parameter, summary-routing-exception should also be configure for the source instance. When configuring:
	`cs7 i x pc-conversion default y`
	A summary route is entered in the instance y routing table. The summary-routing-exception parameter should then be configured for instance y:
	`cs7 i y summary-routing-exception`
	This means that if a full PC route exists in instance y, the ITP will not use the Virtual Linkset as a backup route. The ITP will use the Virtual Linkset as the primary route for any MSUs whose destination point codes (DPCs) does not match a full PC destination in the route table.

Release 12.2(23)SW

Open Caveats—Cisco IOS Release 12.2(23)SW

No open caveats specific to Cisco IOS Release 12.2(23)SW require documentation in the release notes.

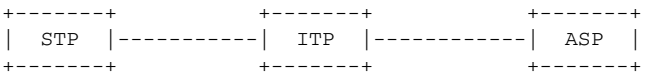
Resolved Caveats—Cisco IOS Release 12.2(23)SW

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(23)SW. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

Table 7 Resolved Caveats for Cisco IOS Release 12.2(23)SW

DDTS ID Number	Description
CSCed82922	MLR: add support for OPC preservation in CgPA when required **Symptom:** When using the Multi-Layer Routing Feature (MLR) of the IP Transfer Point (ITP) product in networks using point-code and subsystem routing, the responses to request packets routed by MLR may not be properly backrouted to the originator. **Workaround:** Either use the global title-based routing prior to the ITP MLR routing, or have the originator use a global title address specified in the request's calling party address field.
CSCee11874	First link test msg and ack lost on HSL link **Symptom:** Restart, link test or link test ACK messages may get dropped. **Conditions:** The messages will be dropped only when the IP Transfer Point (ITP) initially reloads or is executing the RESTART procedure. The link test message will be re-sent after 8 seconds and the RESTART after 12 seconds. **Workaround:** There is no workaround.
CSCee21532	M3UA ASP binding required for SCCP class 0 traffic **Symptom:** When using an MTP3-User Adaptation (M3UA) Application Server (AS) with a loadshare bindings traffic mode, all Signaling Connection Control Protocol (SCCP) traffic is bound to a specific ASP using the received SLS value. Specifying the **cs7 distribute-sccp-unsequenced** command should allow SCCP Class 0 traffic to be round-robin distributed among the ASPs, but still permit SCCP Class 1 traffic to be bound to a specific ASP. **Workaround:** The Application Server must use loadshare roundrobin or the ASP must use SUA.
CSCee09009	ITP: Failure to send DUNA upon receiving TCP **Symptom:** The IP Transfer Point (ITP) receives a Transfer Cluster Prohibited (TCP) from the network but does not send Destination Unavailable (DUNA) to an M3UA application server (AS). **Conditions:** 1. The AS shares the ITP local point code. 2. The ITP has a cluster route configured that includes the local point code. 3. The concerned point code in the received TCP matches that cluster route. **Workaround:** There is no workaround. **Further Problem Description:** None.

Table 7 Resolved Caveats for Cisco IOS Release 12.2(23)SW (continued)

DDTS ID Number	Description
CSCee08792	ITP: Failure to send DRST upon receiving TFR/TCR **Symptom:** When an MTP3-User Adaptation (M3UA) Application Server (AS) shares the local point code of the IP Transfer Point (ITP), and the ITP receives a transfer restricted (TFR) or transfer cluster restricted (TCR) from the network, the ITP does not send Destination Restricted (DRST) message to the AS. **Conditions:**  Consider an M3UA AS that shares the local PC of the ITP in the above figure. **Issue 1:** If the signaling transfer point (STP) sends a TFR to the ITP with some concerned PC n.c.m (i.e. the destination parameter), then the ITP marks PC n.c.m as restricted in the route-table, but fails to send a DRST to the ASP. **Issue 2:** If the STP sends a TCR to the ITP with some concerned cluster n.c.* (i.e. the destination parameter), then the ITP marks cluster n.c.* as restricted in the route-table, but fails to send a DRST to the ASP. In both these cases, the DRST is not sent if the concerned destination on the ITP made a transition from Accessible status to Restricted status. The ITP does send DRST if the destination made a transition from Inaccessible status to Restricted status. **Workaround:** There is no workaround. **Further Problem Description:** None.

Release 12.2(21)SW

Open Caveats—Cisco IOS Release 12.2(21)SW

No open caveats specific to Cisco IOS Release 12.2(21)SW require documentation in the release notes.

Resolved Caveats—Cisco IOS Release 12.2(21)SW

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(21)SW. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

Table 8 Resolved Caveats for Cisco IOS Release 12.2(21)SW

DDTS ID Number	Description
CSCed27956	A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality. All Cisco products which contain TCP stack are susceptible to this vulnerability. This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml, and it describes this vulnerability as it applies to Cisco products that run Cisco IOS® software. A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml.
CSCed38527	A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality. All Cisco products which contain TCP stack are susceptible to this vulnerability. This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml, and it describes this vulnerability as it applies to Cisco products that run Cisco IOS® software. A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml.
CSCed44759	ITP: TTC M3UA traffic from ASP not handled properly **Symptom:** This issue occurs on IP Transfer Points (ITPs) configured for the Telecommunications Technology Committee (TTC) variant. Traffic coming from an MTP3-User Adaptation (M3UA) Application Server Process (ASP) is not handled properly. **Workaround:** There is no workaround for this issue.

Release 12.2(20)SW

Open Caveats—Cisco IOS Release 12.2(20)SW

No open caveats specific to Cisco IOS Release 12.2(20)SW require documentation in the release notes.

Resolved Caveats—Cisco IOS Release 12.2(20)SW

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(20)SW. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

Table 9 Resolved Caveats for Cisco IOS Release 12.2(20)SW

DDTS ID Number	Description
CSCec61182	High CPU in Virtual exec after privilege configure level 7 cs7 **Symptom:** This symptom is observed that a Cisco Route Switch Processor 8 (RSP8) that is running Cisco IOS Release 12.2(4)MB12 uses 100% of the CPU in the "Virtual Exec" process, after you enter the **privilege configure level 7 cs7** command in a Telnet session. **Workaround:** There is no workaround.
CSCec62567	ITP <-> SGM have unusual high values (send Erlang values) **Symptom:** Sent-link utilization is incorrect in certain configurations. The cgspLinkL2BytesSent(CISCO-ITP-GSP-MIB.my) and cItpSpLinkL2BytesSent (CISCO-ITP-SP-MIB.my) object provide incorrect values in these situations. This can result in incorrect information for [send erlang values] in SGM. Conditions: These symptoms may occur when you run routers on Cisco IOS Release 12.2(4)MB10 through Cisco IOS Release MB13, Cisco IOS Release 12.2(18)SW, or Cisco IOS Release 12.2(19)SW images. **Workaround:** There is no workaround.
CSCec69259	ITP-S: snmp traceback prior to cs7 config **Symptom:** Traceback occurs while walking the event table in CISCO-ITP-GSP2-MIB. This may happen with Simple Network Management Protocol (SNMP) configured but without the **cs7** command configured. Conditions: These symptoms may occur when you run routers on IP Transfer Point (ITP) images Cisco IOS Release 12.2(4)MB6 through Cisco IOS Release 12.2(4)MB13, Cisco IOS Release 12.2(18)SW, or Cisco IOS Release 12.2(19)SW. After a reboot, a walk of the event table in CISCO-ITP-GSP2.my MIB usingthe **getmany** command may produce a traceback. **Workaround:** There is no workaround.

Table 9 Resolved Caveats for Cisco IOS Release 12.2(20)SW (continued)

DDTS ID Number	Description
CSCec79617	ITP: various problems with summary routes and GTT **Symptom:** 1. The **show cs7 gtt map stat** command shows Global Title Translation (GTT) maps stuck in a congested state. 2. Signaling Connection Control Part (SCCP) does not choose alternate congested point-codes. Conditions: These symptoms occur when summary or cluster routes are used, and GTT is translated to point-codes for which a full route does not exist. **Workaround:** For all point-codes that GTT translates to, ensure that there is a full route to the destination.
CSCed20020	ITP: could use non avail item in GTT app-grp **Symptom:** IP Transfer Point (ITP) sends Global Title Translation (GTT) traffic to unavailable subsystems. Conditions: This symptom occurs when you use GTT application groups under the following conditions: 1. Item(s) in a group are PCs without a Subsystem Number (SSN). 2. RI=PCSSN. 3. Message signal units (MSU) Signaling Connection Control Part (SCCP) Called Party Address (CDPA) contains SSN=X. 4. PC/SSN=X exists in the GTT map table, and SSN is prohibited. **Workaround:** Specify explicit SSN in the application group entry; specify HLR, MSC, VLR, and so on. Further Problem Description: When performing a final GTT, ITP must have all end points in the GTT map table, so that you can track the status. When entering into the application group, if RI=PCSSN and SSN is specified, the GTT map is automatically created. Not specifying an SSN is supported and the ITP will rely on the SSN in the MSU, but corresponding SSNs must be manually entered in that case.

Release 12.2(19)SW

Open Caveats—Cisco IOS Release 12.2(19)SW

No open caveats specific to Cisco IOS Release 12.2(19)SW require documentation in the release notes.

Resolved Caveats—Cisco IOS Release 12.2(19)SW

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(19)SW. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

Table 10 Resolved Caveats for Cisco IOS Release 12.2(19)SW

DDTS ID Number	Description
CSCec44189	Response to SST message contains wrong OPC **Symptom:** Nodes receiving subsystem status test messages (SST) from the IP Transfer Point (ITP) may ignore the status because the ITP obtains the Signaling Connection Control Part (SCCP) management messages (SCMG) from the primary local point code only. **Workaround:** There is no workaround.

Additional References

The following sections describe the documentation available for the Cisco 2650, Cisco 2651, Cisco 2650XM, and Cisco 2651XM series routers. Typically, these documents consist of hardware and software installation guides, Cisco IOS configuration and command references, system error messages, feature modules, and other documents. Documentation is available as printed manuals or electronic documents, except for feature modules, which are available online on Cisco.com in pdf or html form.

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

- Release-Specific Documents, page 48
- Platform-Specific Documents, page 48

Release-Specific Documents

The following documents are specific to Release 12.2. They are located on Cisco.com:

- *Cross-Platform Release Notes for Cisco IOS Release 12.2*
- *Field Notices:* http://www.cisco.com/warp/public/tech_tips/index/fn.html.
- *Caveats for Cisco IOS Release 12.2.*

Platform-Specific Documents

Hardware installation guides, configuration and command reference guides, and additional documents specific to theCisco 2650, Cisco 2651, Cisco 2650XM, and Cisco 2651XM series routers are available on Cisco.com at the following location:

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

Feature Modules

Feature modules describe new features supported by Cisco IOS Release 12.2 and are updates to the Cisco IOS documentation set. A feature module consists of a brief overview of the feature, benefits, configuration tasks, and a command reference. As updates, the feature modules are available online only.

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. Cisco Feature Navigator is available 24 hours a day, 7 days a week.

To use Cisco 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.

Cisco 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

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

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feed-back, 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

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