Release Notes for Cisco 7000 Series Routers for Cisco IOS Release 12.2 SW

February 28, 2007

Cisco IOS Release 12.2(25)SW9

EDCS-578788

(also known as OL-4835-19)

These release notes for the Cisco 7000 family describe the enhancements provided in Cisco IOS Release 12.2(25)SW9 and later. These release notes are updated as needed.

For a list of the software caveats that apply to Cisco IOS Release 12.2(25)SW9, see the "Caveats for Cisco IOS Release 12.2 SW" section on page 26.

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 IOS Release 12.2(25)SW9 is synced from Cisco IOS Release 12.2(17)S and contains all fixes contained in Cisco IOS Release 12.2(17)S.

Documentation Survey

Is Cisco documentation helpful? Click here to give us your feedback or go to the following URL to give us your feedback:

http://forums.cisco.com/eforum/servlet/viewsflash?cmd=showform&pollid=rtgdoc01!rtgdoc.

Contents

These release notes describe the following topics:

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

System Requirements

This section describes the system requirements for Cisco IOS Release 12.2(25)SW9 and includes the following sections:

Memory Recommendations

Table 1 Images and Memory Recommendations for Cisco IOS Release 12.2(25)SW9

Platforms	Feature Sets	Image Name	Software Image	Flash Memory Recommended	DRAM Memory Recommended	Runs From
Cisco 7200	IP Standard Feature Set	IP Transfer Point	c7200-itpk91-mz	32 MB Flash	256 MB DRAM	FLASH
Cisco 7300	IP Standard Feature Set	IP Transfer Point	c7301-itpk91-mz	32 MB Flash	256 MB DRAM	FLASH
Cisco 7500	IP Standard Feature Set	IP Transfer Point	rsp-itpk91v-mz	32 MB Flash	256 MB DRAM	FLASH

Table 2 Images and Memory Recommendations for Cisco IOS Release 12.2(25)SW8

Platforms	Feature Sets	Image Name	Software Image	Flash Memory Recommended	DRAM Memory Recommended	Runs From
Cisco 7200	IP Standard Feature Set	IP Transfer Point	c7200-itpk91-mz	32 MB Flash	256 MB DRAM	FLASH
Cisco 7300	IP Standard Feature Set	IP Transfer Point	c7301-itpk91-mz	32 MB Flash	256 MB DRAM	FLASH
Cisco 7500	IP Standard Feature Set	IP Transfer Point	rsp-itpk91v-mz	32 MB Flash	256 MB DRAM	FLASH

Table 3 Images and Memory Recommendations for Cisco IOS Release 12.2(25)SW7

Platforms	Feature Sets	Image Name	Software Image	Flash Memory Recommended	DRAM Memory Recommended	Runs From
Cisco 7200	IP Standard Feature Set	IP Transfer Point	c7200-itpk91-mz	32 MB Flash	256 MB DRAM	FLASH
Cisco 7300	IP Standard Feature Set	IP Transfer Point	c7301-itpk91-mz	32 MB Flash	256 MB DRAM	FLASH
Cisco 7500	IP Standard Feature Set	IP Transfer Point	rsp-itpk91v-mz	32 MB Flash	256 MB DRAM	FLASH

Table 4 Images and Memory Recommendations for Cisco IOS Release 12.2(25)SW6

Platforms	Feature Sets	Image Name	Software Image	Flash Memory Recommended	DRAM Memory Recommended	Runs From
Cisco 7200	IP Standard Feature Set	IP Transfer Point	c7200-itpk91-mz	32 MB Flash	256 MB DRAM	FLASH
Cisco 7300	IP Standard Feature Set	IP Transfer Point	c7301-itpk91-mz	32 MB Flash	256 MB DRAM	FLASH
Cisco 7500	IP Standard Feature Set	IP Transfer Point	rsp-itpk91v-mz	32 MB Flash	256 MB DRAM	FLASH

Table 5 Images and Memory Recommendations for Cisco IOS Release 12.2(25)SW5

Platforms	Feature Sets	Image Name	Software Image	Flash Memory Recommended	DRAM Memory Recommended	Runs From
Cisco 7200	IP Standard Feature Set	IP Transfer Point	c7200-itp-mz	32 MB Flash	128 MB DRAM	FLASH
Cisco 7300	IP Standard Feature Set	IP Transfer Point	c7301-itp-mz	32 MB Flash	256 MB DRAM	FLASH
Cisco 7500	IP Standard Feature Set	IP Transfer Point	rsp-itpv-mz	32 MB Flash	256 MB DRAM	FLASH

Table 6 Images and Memory Recommendations for Cisco IOS Release 12.2(25)SW4

Platforms	Feature Sets	Image Name	Software Image	Flash Memory Recommended	DRAM Memory Recommended	Runs From
Cisco 7200	IP Standard Feature Set	IP Transfer Point	c7200-itp-mz	32 MB Flash	128 MB DRAM	FLASH

Table 6 Images and Memory Recommendations for Cisco IOS Release 12.2(25)SW4

Cisco 7300	IP Standard Feature Set	IP Transfer Point	c7301-itp-mz	32 MB Flash	256 MB DRAM	FLASH
Cisco 7500	IP Standard Feature Set	IP Transfer Point	rsp-itpv-mz	32 MB Flash	256 MB DRAM	FLASH

Table 7 Images and Memory Recommendations for Cisco IOS Release 12.2(25)SW3b

Platforms	Feature Sets	Image Name	Software Image	Flash Memory Recommended	DRAM Memory Recommended	Runs From
Cisco 7200	IP Standard Feature Set	IP Transfer Point	c7200-itp-mz	32 MB Flash	128 MB DRAM	FLASH
Cisco 7300	IP Standard Feature Set	IP Transfer Point	c7301-itp-mz	32 MB Flash	256 MB DRAM	FLASH
Cisco 7500	IP Standard Feature Set	IP Transfer Point	rsp-itpv-mz	32 MB Flash	256 MB DRAM	FLASH

Table 8 Images and Memory Recommendations for Cisco IOS Release 12.2(25)SW3a

Platforms	Feature Sets	Image Name	Software Image	Flash Memory Recommended	DRAM Memory Recommended	Runs From
Cisco 7200	IP Standard Feature Set	IP Transfer Point	c7200-itp-mz	32 MB Flash	128 MB DRAM	FLASH
Cisco 7300	IP Standard Feature Set	IP Transfer Point	c7301-itp-mz	32 MB Flash	256 MB DRAM	FLASH
Cisco 7500	IP Standard Feature Set	IP Transfer Point	rsp-itpv-mz	32 MB Flash	256 MB DRAM	FLASH

Table 9 Images and Memory Recommendations for Cisco IOS Release 12.2(25)SW3

Platforms	Feature Sets	Image Name	Software Image	Flash Memory Recommended	DRAM Memory Recommended	Runs From
Cisco 7200	IP Standard Feature Set	IP Transfer Point	c7200-itp-mz	32 MB Flash	256 MB DRAM	FLASH
Cisco 7300	IP Standard Feature Set	IP Transfer Point	c7301-itp-mz	32 MB Flash	256 MB DRAM	FLASH
Cisco 7500	IP Standard Feature Set	IP Transfer Point	rsp-itpv-mz	32 MB Flash	256 MB DRAM	FLASH

Table 10 Images and Memory Recommendations for Cisco IOS Release 12.2(25)SW2

Platforms	Feature Sets	Image Name	Software Image	Flash Memory Recommended	DRAM Memory Recommended	Runs From
Cisco 7200	IP Standard Feature Set	IP Transfer Point	c7200-itp-mz	32 MB Flash	128 MB DRAM	FLASH
Cisco 7300	IP Standard Feature Set	IP Transfer Point	c7301-itp-mz	32 MB Flash	256 MB DRAM	FLASH
Cisco 7500	IP Standard Feature Set	IP Transfer Point	rsp-itpv-mz	32 MB Flash	256 MB DRAM	FLASH

Table 11 Images and Memory Recommendations for Cisco IOS Release 12.2(25)SW1

Platforms	Feature Sets	Image Name	Software Image	Flash Memory Recommended	DRAM Memory Recommended	Runs From
Cisco 7200	IP Standard Feature Set	IP Transfer Point	c7200-itp-mz	32 MB Flash	128 MB DRAM	FLASH
Cisco 7300	IP Standard Feature Set	IP Transfer Point	c7301-itp-mz	32 MB Flash	256 MB DRAM	FLASH
Cisco 7500	IP Standard Feature Set	IP Transfer Point	rsp-itpv-mz	32 MB Flash	256 MB DRAM	FLASH

Table 12 Images and Memory Recommendations for Cisco IOS Release 12.2(25)SW

Platforms	Feature Sets	Image Name	Software Image	Flash Memory Recommended	DRAM Memory Recommended	Runs From
Cisco 7200	IP Standard Feature Set	IP Transfer Point	c7200-itp-mz	32 MB Flash	128 MB DRAM	FLASH
Cisco 7300	IP Standard Feature Set	IP Transfer Point	c7301-itp-mz	32 MB Flash	256 MB DRAM	FLASH
Cisco 7500	IP Standard Feature Set	IP Transfer Point	rsp-itpv-mz	32 MB Flash	256 MB DRAM	FLASH

Table 13 Images and Memory Recommendations for Cisco IOS Release 12.2(23)SW1

Platforms	Feature Sets	Image Name	Software Image	Flash Memory Recommended	DRAM Memory Recommended	Runs From
Cisco 7200	IP Standard Feature Set	IP Transfer Point	c7200-itp-mz	32 MB Flash	128 MB DRAM	FLASH

Table 13 Images and Memory Recommendations for Cisco IOS Release 12.2(23)SW1

Cisco 7300	IP Standard Feature Set	IP Transfer Point	c7301-itp-mz	32 MB Flash	256 MB DRAM	FLASH
Cisco 7500	IP Standard Feature Set	IP Transfer Point	rsp-itpv-mz	32 MB Flash	256 MB DRAM	FLASH

Table 14 Images and Memory Recommendations for Cisco IOS Release 12.2(23)SW

Platforms	Feature Sets	Image Name	Software Image	Flash Memory Recommended	DRAM Memory Recommended	Runs From
Cisco 7200	IP Standard Feature Set	IP Transfer Point	c7200-itp-mz	32 MB Flash	128 MB DRAM	FLASH
Cisco 7300	IP Standard Feature Set	IP Transfer Point	c7301-itp-mz	32 MB Flash	256 MB DRAM	FLASH
Cisco 7500	IP Standard Feature Set	IP Transfer Point	rsp-itpv-mz	32 MB Flash	256 MB DRAM	FLASH

Table 15 Images and Memory Recommendations for Cisco IOS Release 12.2(21)SW1

Platforms	Feature Sets	Image Name	Software Image	Flash Memory Recommended	DRAM Memory Recommended	Runs From
Cisco 7200	IP Standard Feature Set	IP Transfer Point	c7200-itp-mz	32 MB Flash	128 MB DRAM	FLASH
Cisco 7300	IP Standard Feature Set	IP Transfer Point	c7301-itp-mz	32 MB Flash	256 MB DRAM	FLASH
Cisco 7500	IP Standard Feature Set	IP Transfer Point	rsp-itpv-mz	32 MB Flash	256 MB DRAM	FLASH

Table 16 Images and Memory Recommendations for Cisco IOS Release 12.2(21)SW

Platforms	Feature Sets	Image Name	Software Image	Flash Memory Recommended	DRAM Memory Recommended	Runs From
Cisco 7200	IP Standard Feature Set	IP Transfer Point	c7200-itp-mz	32 MB Flash	128 MB DRAM	FLASH
Cisco 7300	IP Standard Feature Set	IP Transfer Point	c7301-itp-mz	32 MB Flash	256 MB DRAM	FLASH
Cisco 7500	IP Standard Feature Set	IP Transfer Point	rsp-itpv-mz	32 MB Flash	256 MB DRAM	FLASH

Table 17 Images and Memory Recommendations for Cisco IOS Release 12.2(20)SW

Platforms	Feature Sets	Image Name	Software Image	Flash Memory Recommended	DRAM Memory Recommended	Runs From
Cisco 7200	IP Standard Feature Set	IP Transfer Point	c7200-itp-mz	32 MB Flash	128 MB DRAM	FLASH
Cisco 7300	IP Standard Feature Set	IP Transfer Point	c7301-itp-mz	32 MB Flash	256 MB DRAM	FLASH
Cisco 7500	IP Standard Feature Set	IP Transfer Point	rsp-itpv-mz	32 MB Flash	256 MB DRAM	FLASH

Table 18 Images and Memory Recommendations for Cisco IOS Release 12.2(19)SW

Platforms	Feature Sets	Image Name	Software Image	Flash Memory Recommended	DRAM Memory Recommended	Runs From
Cisco 7200	IP Standard Feature Set	IP Transfer Point	c7200-itp-mz	32 MB Flash	128 MB DRAM	FLASH
Cisco 7300	IP Standard Feature Set	IP Transfer Point	c7301-itp-mz	32 MB Flash	256 MB DRAM	FLASH
Cisco 7500	IP Standard Feature Set	IP Transfer Point	rsp-itpv-mz	32 MB Flash	256 MB DRAM	FLASH

Table 19 Images and Memory Recommendations for Cisco IOS Release 12.2(18)SW

Platforms	Feature Sets	Image Name	Software Image	Flash Memory Recommended	DRAM Memory Recommended	Runs From
Cisco 7300	IP Standard Feature Set	IP Transfer Point	c7301-itp-mz	32 MB Flash	256 MB DRAM	FLASH

Supported Hardware

Cisco IOS Release 12.2(25)SW9 supports the following Cisco 7000 family platforms:

- Cisco 7200 series routers
- Cisco 7301 router
- Cisco 7500 series routers

For detailed descriptions of the new hardware features, see the "New and Changed Information" section on page 10.

Determining the Software Version

To determine the version of Cisco IOS software running on your Cisco 7000 family router, log in to the Cisco 7000 family router and enter the **show version** EXEC command:

```
Router> show version
Cisco Internetwork Operating System Software
IOS (tm) 7301 Software (c7301-itp-mz), Version 12.2(25)SW9, RELEASE SOFTWARE
```

Upgrading to a New Software Release

For information about selecting a new Cisco IOS software release, please refer to *How to Choose a Cisco IOS Software Release* at:

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

For information about upgrading to a new software release, refer to the appropriate platform-specific document:

Cisco 7200 Series, 7300 Series, 7400 Series, and 7500 Series Routers

http://www.cisco.com/en/US/products/hw/routers/ps133/products_tech_note09186a0080094c07.shtml

For *Cisco IOS Upgrade Ordering Instructions*, refer to the document at the following location:

http://www.cisco.com/warp/public/cc/pd/iosw/prodlit/957_pp.htm

To choose a new Cisco IOS software release by comparing feature support or memory requirements, use Cisco Feature Navigator. Cisco Feature Navigator is a web-based tool that enables you to determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or by feature set (software image). Under the release section, you can compare Cisco IOS software releases side by side to display both the features unique to each software release and the features that the releases have in common.

To access Cisco Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

http://tools.cisco.com/RPF/register/register.do

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp

To choose a new Cisco IOS software release based on information about defects that affect that software, use Bug Toolkit at:

http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl.

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.

Caution Cisco IOS images with strong encryption (including, but not limited to 168-bit (3DES) data encryption feature sets) are subject to U.S. 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 U.S. government regulations. When applicable, the purchaser/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.

The feature set tables have been removed from the Cisco IOS Release 12.2 release notes to improve the usability of the release notes documentation. The feature-to-image mapping that was provided by the feature set tables is available through Cisco Feature Navigator.

Cisco Feature Navigator is a web-based tool that enables you to determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or by feature set (software image). Under the release section, you can compare Cisco IOS software releases side by side to display both the features unique to each software release and the features that the releases have in common.

To access Cisco Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

http://www.cisco.com/register

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

http://www.cisco.com/go/fn

For frequently asked questions about Cisco Feature Navigator, see the FAQs at the following URL:

http://www.cisco.com/support/FeatureNav/FNFAQ.html

Determining Which Software Images (Feature Sets) Support a Specific Feature

To determine which software images (feature sets) in Cisco IOS Release 12.2 support a specific feature, go to the Cisco Feature Navigator home page, enter your Cisco.com login, and perform the following steps:

Step 1 From the Cisco Feature Navigator home page, click **Feature**.

Step 2 To find a feature, use either “Search by full or partial feature name” or “Browse features in alphabetical order.” Either a list of features that match the search criteria or a list of features that begin with the number or letter selected from the ordered list will be displayed in the text box on the left side of the web page.

Step 3 Select a feature from the left text box, and click the **Add** button to add a feature to the Selected Features text box on the right side of the web page.

Note To learn more about a feature in the list, click the **Description** button below the left box.

Repeat this step to add additional features. A maximum of 20 features can be chosen for a single search.

Step 4 Click **Continue** when you are finished selecting features.

Step 5 From the Major Release drop-down menu, choose **12.2**.

Step 6 From the Release drop-down menu, choose the appropriate maintenance release.

Step 7 From the Platform Family drop-down menu, select the appropriate hardware platform. The "Your selections are supported by the following:" table will list all the software images (feature sets) that support the feature(s) that you selected.

Determining Which Features Are Supported in a Specific Software Image (Feature Set)

To determine which features are supported in a specific software image (feature set) in Cisco IOS Release 12.2, go to the Cisco Feature Navigator home page, enter your Cisco.com login, and perform the following steps:

Step 1 From the Cisco Feature Navigator home page, click **Compare/Release**.

Step 2 In the "Find the features in a specific Cisco IOS release, using one of the following methods:" box, choose **12.2** from the Cisco IOS Major Release drop-down menu.

Step 3 Click **Continue**.

Step 4 From the Release drop-down menu, choose the appropriate maintenance release.

Step 5 From the Platform Family drop-down menu, choose the appropriate hardware platform.

Step 6 From the Feature Set drop-down menu, choose the appropriate feature set. The "Your selections are supported by the following:" table will list all the features that are supported by the feature set (software image) that you selected.

New and Changed Information

The following sections list the new hardware and software features supported by the Cisco 7000 family for Cisco IOS Release 12.2 SW.

New Hardware Features in Cisco IOS Release 12.2(25)SW9

There are no new hardware features supported in Cisco IOS Release 12.2(25)SW9.

New Software Features in Cisco IOS Release 12.2(25)SW9

The following new software features are supported by IP Transfer Point (ITP) on the Cisco 7500 router on Cisco IOS Release 12.2(25)SW9:

MLR SCCP Error Return

Platforms: Cisco 7500

Cisco IOS Release 12.2(25)SW9 allows you to configure Multi-Layer Routing (MLR) to return a unitdata service(UDTS) to the source of the Signaling Connection Control Part (SCCP) packet when the SCCP packet is blocked. You configure this feature by specifying an optional sccp-error parameter on block results in MLR rules and MLR address tables.

Refer to the following document for more information about MLR SCCP Error Return:

IP Transfer Point (ITP)

GWS SCCP Error Return

Platforms: Cisco 7500

Cisco IOS Release 12.2(25)SW9 allows you to configure Gateway Screening (GWS) to return a unitdata service(UDTS) to the source of the Signaling Connection Control Part (SCCP) packet when the SCCP packet is dropped. You configure a returnUDTS when you define the gateway screening action set in enhanced GWS.

Refer to the following document for more information about GWS SCCP Error Return:

IP Transfer Point (ITP)

SCCP/MAP Address Modification for SRI-SM Messages

Platforms: Cisco 7500

Cisco IOS Release 12.2(25)SW9 permits Signaling Connection Control Part (SCCP) and Mobile Application Part (MAP) address modification using a Multi-Layer Routing (MLR) **modify-profile**. MLR currently supports modifying only the service center address (orig-smsc) and the calling party address (CgPA) for SRI-SM messages.

With Cisco IOS Release 12.2(25)SW9, the user can also now optionally configure the desired action for failed modifications using the **modify-failure** command within the MLR options submode. A user can also configure the **preserve-opc** function within the global MLR options submode. The **preserve-opc** function retains the original Originating Point Code (OPC). The user may configure MLR to return a unitdata service(UDTS) to the source of the SCCP packet when the SCCP packet is blocked by specifying an optional **sccp-error** parameter on block results.

Refer to the following document for more information about SCCP/MAP Address Modification for SRI-SM Messages:

IP Transfer Point (ITP)

C-Link Backup Routing of M3UA/SUA Traffic

Platforms: Cisco 7500

Cisco IOS Release 12.2(25)SW9 supports a C-link Backup Routing feature that provides backup routing to MTP3-User Adaptation (M3UA) and SCCP User Adaptation (SUA) application servers (ASs). It uses an MTP3/MTP2-User Peer-to-Peer Adaptation Layer (M2PA) linkset to a remote signaling gateway (SG) serving the same ASs over Stream Control Transmission Protocol (SCTP) /IP. This configurable software feature is available to any IP Transfer Point (ITP) running a sigtran protocol (M3UA and/or SUA) and offloaded Message Transfer Part Level 3 (MTP3). The remote SG that is reachable through the C-link may be another ITP, or any SG serving the same ASs.

Refer to the following document for more information about C-link Backup Routing:

IP Transfer Point (ITP)

New Hardware Features in Cisco IOS Release 12.2(25)SW8

There are no new hardware features supported in Cisco IOS Release 12.2(25)SW8.

New Software Features in Cisco IOS Release 12.2(25)SW8

The following new software features are supported by the Cisco 7000 family for Cisco IOS Release 12.2(25)SW8:

Multi-Layer Routing (MLR) Generic Opcode Support

Cisco IOS Release 12.2(25)SW8 extends Mobile Application Part (MAP) operation support to include all GSM-MAP (3GPP TS 29.002 version 5.9.0 Release 5) operations in Multi-Layer Routing (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 destination point code (DPC) into the Called Party (CDPA) point code (PC) for packets that are Multi-Layer Routing (MLR)-routed.

New Hardware Features in Cisco IOS Release 12.2(25)SW7

There are no new hardware features supported in Cisco IOS Release 12.2(25)SW7.

New Software Features in Cisco IOS Release 12.2(25)SW7

The following new software features are supported by the Cisco 7000 family for Cisco IOS Release 12.2(25)SW7:

Preventative Cyclic Redundancy Check (PCR) Error Corrections

Platforms: Cisco 7200 routers, Cisco 7301 routers, and Cisco 7500 series routers

Cisco IOS Release 12.2(25)SW7 supports Preventative Cyclic Redundancy (PCR) Error Corrections as described in Q.703 and GR-246. PCR is an alternative form of error correction for Message Transfer Part Level 2 (MTP2) links and is typically used on links that have a long delay (for example, satellite links).

CISCO-ITP-MSU-RATES-MIB

Platforms: Cisco 7200 routers, Cisco 7301 routers, and Cisco 7500 series routers

Cisco IOS Release 12.2(25)SW7 supports the new CISCO-ITP-MSU-RATES-MIB. This MIB provides statistics for the number of message signaling units (MSUs) per second being processed by the Route/Switch Processor (RSP) and Versatile Interface Processor (VIP).

New Hardware Features in Cisco IOS Release 12.2(25)SW6

There are no new hardware features supported in Cisco IOS Release 12.2(25)SW6.

New Software Features in Cisco IOS Release 12.2(25)SW6

The following new software features are supported by the Cisco 7000 family for Cisco IOS Release 12.2(25)SW6:

Secure Shell (SSH)

Platforms: Cisco 7200 routers, Cisco 7301 routers, and Cisco 7500 series routers

Cisco IOS Release 12.2(25)SW6 supports the Secure Shell (SSH) feature on the IP Transfer Point (ITP) in the Cisco 7500 (image rsp-itpk91v-mz), Cisco 7301 (image c7301-itpk91-mz), and Cisco 7200 (image c7200-itpk91-mz) platforms. SSH enables secure sessions by establishing an encrypted connection between an SSH client and an SSH server.

JT1 interface

Platforms: Cisco 7200 routers, Cisco 7301 routers, and Cisco 7500 series routers

Cisco IOS Release 12.2(25)SW6 supports the JT1 interface, the Japanese variation of the standard framing formats for T1 controller settings. The JT1 interface is a 1544 kbit/s line type specified by the Japanese standards organization, Telecommunications Technology Committee (TTC).

New Hardware Features in Cisco IOS Release 12.2(25)SW5

There are no new hardware features supported in Cisco IOS Release 12.2(25)SW5.

New Software Features in Cisco IOS Release 12.2(25)SW5

The following new software features are supported by the Cisco 7000 family for Cisco IOS Release 12.2(25)SW5:

MLR Call Tracing Feature

The IP Transfer Point (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. In Cisco IOS Release 12.2(25)SW5, the new component **cs7 mlr** 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:

- Tracing of Global System for Mobile Communications (GSM) Short Message Service (SMS) mobile-originated (MO) messages for a set of originating International Mobile Subscriber Identities (IMSIs).
- Tracing of GSM SMS MO messages for a set of different Mobile Station Integrated Services digital networks (MSISDNs) that represent either the A-address or B-address of an SMS message.
- Tracing of ANSI41 SMDPP messages for a set of different addresses that represent either the A-address or B-address of an SMS message.
- Display of trace entries on the router console using show commands.
- Indicate whether a message has been processed by MLR for a given traceable address, including the final routing result.
- Allow message trace logs to be obtained using the File Transfer Protocol (FTP) or Trivial File Transfer Protocol (TFTP).

The MLR Call Tracing feature is documented in the *Cisco IP Transfer Point (ITP) in IOS Release 12.2(25)SW5* configuration guide at the following URL:

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

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:

- Insertion of the originating IMSI into the proxied Short Message Service (SMS) mobile-originated (MO) dialogue, if known, must be allowed 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 SMS center (SMSC) address should be modified to match the recipient SMSC.

- If the B-address is modified using Distributed Short Message Routing (DSMR) Address Translation, then the modified address should be included in the proxied SMS MO dialogue.

The SMS MO Proxy Message Modification feature in the *Cisco IP Transfer Point (ITP) in IOS Release 12.2(25)SW5* configuration guide at the following URL:

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

Support for Q.703 Annex A High-speed Links

Cisco IOS Release 12.2(25)SW5 provides support for Q.703 Annex A high-speed links on the IP Transfer Point (ITP). A new port adapter, the SS7 Q.703 high-speed port adapter (PA-MCX-4TE1-Q), supports enhanced Message Transfer Part Level 2 (MTP2) functions and procedures that are suitable for the operation and control of signaling links at data rates of 1.5 and 2.0 Mb. The ITP software for Cisco IOS Release 12.2(25)SW5 enables configuration of the card type and controller and enables configuration of the interface for SS7 high-speed MTP2 encapsulation.

Support for Q.703 Annex A high-speed links in the *Cisco IP Transfer Point (ITP) in IOS Release 12.2(25)SW5* configuration guide at the following URL:

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

New Hardware Features in Cisco IOS Release 12.2(25)SW4a

There are no new hardware features supported in Cisco IOS Release 12.2(25)SW4a.

New Software Features in Cisco IOS Release 12.2(25)SW4a

There are no new software features supported in Cisco IOS Release 12.2(25)SW4a.

New Hardware Features in Cisco IOS Release 12.2(25)SW4

There are no new hardware features supported in Cisco IOS Release 12.2(25)SW4.

New Software Features in Cisco IOS Release 12.2(25)SW4

The following new software features are supported by the Cisco 7000 family for Cisco IOS Release 12.2(25)SW4:

Enhanced Gateway Screening

Platforms: Cisco 7200 routers, Cisco 7301 routers, and Cisco 7500 series routers

Gateway Screening is a process in Signaling Transfer Point (STP) to check the contents of the incoming/outgoing message and either allow or reject the message based on the provisioned screening. If the incoming message is allowed, it is sent to Message Transfer Part (MTP) /Signaling Connection Control Part (SCCP) /ISDN User Part (ISUP)/XUA for further processing. If the outgoing message is allowed, MTP/ XUA routes the message to the destination as specified in the outgoing message. Gateway

Screening can be used with Access Lists, Global Title Translation (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 application server (AS) in case of XUA) and tables shall be created to configure the screening rule.

MLR Dynamic B-address Routing/Binding

Platforms: Cisco 7200 routers, Cisco 7301 routers, and Cisco 7500 series routers

When SMS center (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 Hardware Features in Cisco IOS Release 12.2(25)SW3b

There are no new hardware features supported in Cisco IOS Release 12.2(25)SW3b.

New Software Features in Cisco IOS Release 12.2(25)SW3b

There are no new software features supported in Cisco IOS Release 12.2(25)SW3b.

New Hardware Features in Cisco IOS Release 12.2(25)SW3a

There are no new hardware features supported in Cisco IOS Release 12.2(25)SW3a.

New Software Features in Cisco IOS Release 12.2(25)SW3a

There are no new software features supported in Cisco IOS Release 12.2(25)SW3a.

New Hardware Features in Cisco IOS Release 12.2(25)SW3

There are no new hardware features supported in Cisco IOS Release 12.2(25)SW3.

New Software Features in Cisco IOS Release 12.2(25)SW3

The following new software features are supported by the Cisco 7000 family for Cisco IOS Release 12.2(25)SW3:

DSMR UCP Application Oriented to GSM Mobile Terminated Short Message Delivery

Platforms: Cisco 7200 routers, Cisco 7301 routers, and Cisco 7500 series routers

This feature allows operators to distribute Short Message Service (SMS) messages generated by various service applications to their subscribers using the User Control Point (UCP) protocol.

IS-41 SMS Multicast Notification

Platforms: Cisco 7200 routers, Cisco 7301 routers, and Cisco 7500 series routers

When the IP Transfer Point (ITP) is loadsharing Short Message Service (SMS) messages across a bank of message centers, (MCs), the ITP must duplicate the incoming SMSNOT message to send to each MC.

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

Platforms: Cisco 7200 routers, Cisco 7301 routers, and Cisco 7500 series routers

The Global System for Mobile Communications (GSM) SRI-SM procedure will be invoked towards the home location register (HLR) of the A-address Mobile Station Integrated Services digital network (MSISDN) in order to obtain the International Mobile Subscriber Identities (IMSIs) value.

M2PA v13. Support for draft version 13 of the M2PA protocol

Platforms: Cisco 7200 routers, Cisco 7301 routers, and Cisco 7500 series routers

Support for draft version 2 is continued. The version is configurable.

ITP Group multi-instance support

Platforms: Cisco 7200 routers and Cisco 7301 routers

The IP Transfer Point (ITP) Group feature can now be enabled within each of the multiple instances.

New Hardware Features in Cisco IOS Release 12.2(25)SW2

There are no new hardware features supported in Cisco IOS Release 12.2(25)SW2.

New Software Features in Cisco IOS Release 12.2(25)SW2

There are no new software features supported in Cisco IOS Release 12.2(25)SW2.

New Hardware Features in Cisco IOS Release 12.2(25)SW1

There are no new hardware features supported in Cisco IOS Release 12.2(25)SW1.

New Software Features in Cisco IOS Release 12.2(25)SW1

The following new software features are supported by the Cisco 7000 family for Cisco IOS Release 12.2(25)SW1:

GSM Short Message Routing Mobile-Originated to Mobile-Terminated

Platforms: Cisco 7200 routers, Cisco 7301 routers, and Cisco 7500 series routers

This feature provides the ability to deliver Global System for Mobile Communications (GSM) mobile originated (MO) Short Message Service messages to mobile-terminated (MT) users.

Extended number of Capability Point Codes from 2 to 200

Platforms: Cisco 7200 routers, Cisco 7301 routers, and Cisco 7500 series routers

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

New Hardware Features in Cisco IOS Release 12.2(25)SW

There are no new hardware features supported in Cisco IOS Release 12.2(25)SW.

New Software Features in Cisco IOS Release 12.2(25)SW

The following new software features are supported by the Cisco 7000 family for Cisco IOS Release 12.2(25)SW:

ITP First Delivery Attempt (FDA)

Platforms: Cisco 7200 routers, Cisco 7301 routers, and Cisco 7500 series routers

The IP Transfer Point (ITP) performs a first delivery attempt of a GSM Mobile-Originated Short Message Service (SMS) message to an Application Server.

New Hardware Features in Cisco IOS Release 12.2(23)SW1

There are no new hardware features supported in Cisco IOS Release 12.2(23)SW1.

New Software Features in Cisco IOS Release 12.2(23)SW1

The following new software features are supported by the Cisco 7000 family for Cisco IOS Release 12.2(23)SW1:

Distributed Clock On HSL Port Adapters (PA-A3-8T1IMA, PA-A3-8E1IMA)

Platforms: Cisco 7500 series routers

Used in conjunction with the IP Transfer Point (ITP) Signaling System 7 (SS7) port adapter (PA-MCX-8TE1-M) High-Speed Links can be externally clocked from a BITS source.

New Hardware Features in Cisco IOS Release 12.2(23)SW

There are no new hardware features supported in Cisco IOS Release 12.2(23)SW.

New Software Features in Cisco IOS Release 12.2(23)SW

The following new software features are supported by the Cisco 7000 family for Cisco IOS Release 12.2(23)SW:

Non-Stop Operation

Platforms: Cisco 7500 series routers

This is an enhancement to the 7500 platform redundancy feature. The feature provides the ability for links to remain active during a Master to Slave switchover.

Support For The G1 Processor On The 7200 Platform

Platforms: Cisco 7200 routers

Cisco IOS Release 12.2(23)SW provides support for the NPE-G1 processor for Cisco 7200 routers.

The NPE-G1 is the first network processing engine for the Cisco 7200 VXR routers to provide the functionality of both a network processing engine and I/O controller. If used without an I/O controller, an I/O blank panel must be in place.

While its design provides I/O controller functionality, it can also work with any I/O controller supported in the Cisco 7200 VXR routers. The NPE-G1, when installed with an I/O controller, provides the primary input/out functionality; that is, the NPE-G1 input/out functionality enhances that of the existing I/O controller. However, when both the I/O controller and NPE-G1 are present, the functionality of the auxiliary port and console port are on the I/O controller.

The NPE-G1 maintains and executes the system management functions for the Cisco 7200 VXR routers and also holds the system memory and environmental monitoring functions.

The NPE-G1 consists of one board with multiple interfaces. It is keyed so that it can be used only in the Cisco 7200 VXR routers.

New Hardware Features in Cisco IOS Release 12.2(21)SW1

There are no new hardware features supported in Cisco IOS Release 12.2(21)SW1.

New Software Features in Cisco IOS Release 12.2(21)SW1

There are no new software features supported in Cisco IOS Release 12.2(21)SW1.

New Hardware Features in Cisco IOS Release 12.2(21)SW

There are no new hardware features supported in Cisco IOS Release 12.2(21)SW.

New Software Features in Cisco IOS Release 12.2(21)SW

The following new software features are supported by the Cisco 7000 family for Cisco IOS Release 12.2(21)SW:

MLR Extension for support of ANSI-41 SMS

Platform: Cisco 7500 series routers

The Multi-layer 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 the SIGTRAN protocols MTP2-User Peer-to-Peer Adaptation Layer (M2PA), MTP3-User Adaptation (M3UA) and SCCP User Adaptation (SUA). The Multi-layer SMS Routing feature allows the ITP to make Short Message Service (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 (aka, IS-41) standard, as well as incorporation of Mobile Directory Number (MDN)-based SMS routing.

New Hardware Features in Cisco IOS Release 12.2(20)SW

There are no new hardware features supported in Cisco IOS Release 12.2(20)SW.

New Software Features in Cisco IOS Release 12.2(20)SW

The following new software features are supported by the Cisco 7000 family for Cisco IOS Release 12.2(20)SW:

ITP Japan TTC SS7 Variant

Platform: Cisco 7500 series routers

This IP Transfer Point (ITP) feature incorporates Signaling System 7 (SS7) layers Message Transfer Part Level 2 (MTP2), Message Transfer Part Level 3 (MTP), and Signaling Connection Control Part (SCCP) to support the Japanese TTC SS7 variant specified by the JT-Q7xx documents.

ITP Variant Conversion

Platforms: Cisco 7200 routers, Cisco 7301 routers, and Cisco 7500 series routers

This IP Transfer Point (ITP) features adds support for conversion between different variants. This conversion involves modification of the Message Transfer Part Level 3 (MTP3) and Signaling Connection Control Part (SCCP) portions of the message signaling 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 will support conversion between ITU and ANSI variants of Signaling System 7 (SS7).

New Hardware Features in Cisco IOS Release 12.2(19)SW

The following new hardware feature is supported by the Cisco 7000 family for Cisco IOS Release 12.2(19)SW:

Support for Port Adapter PA-MC-8TE1+

Platforms: Cisco 7200 routers, Cisco 7301 routers, and Cisco 7500 series routers

The Cisco PA-MC-8TE1+ is a single-wide port adapter designed to provide a full eight-port PRI multichannel solution for the Cisco 7200 and Cisco 7400. The interfaces can be channelized, fractional or ISDN-PRI, or unframed (E1) with up to 256 independent High-Level Data Link Control (HDLC) channels definable for T1 and E1 applications. The PA-MC-8TE1+ port adapter is ideal for services providers and large enterprises looking to cost-effectively deploy high-density ISDN terminations of multiple remote-sites.

This port adapter is now supported for WAN applications. For Signaling System 7 (SS7) applications PA-MCX-8TE1-M is required.

SS7 over ATM High Speed Link (HSL) Support

Platforms: Cisco 7301 routers

HSL allows full bandwidth utilization of a 1.55Mbps T1 or a 2.048 Mbps E1 for a single Signaling System 7 (SS7) link. ITP HSL is compliant with both ANSI per Telcordia GR-2878-CORE and ITU per Q.2100 and includes the following protocol stack components:AAL5, SSCOP, SSCF-NNI and MTP3b.

New Software Features in Cisco IOS Release 12.2(19)SW

The following new software features are supported by the Cisco 7000 family for Cisco IOS Release 12.2(19)SW:

Extensions to the Multi-Layer Routing Feature

Platforms: Cisco 7200 routers, Cisco 7301 routers, and Cisco 7500 series routers

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

Platforms: Cisco 7200 routers, Cisco 7301 routers, and Cisco 7500 series routers

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 MTP3-User Adaptation (M3UA) and SCCP User Adaptation (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

New Hardware Features in Cisco IOS Release 12.2(18)SW

The following new hardware feature is supported by the Cisco 7000 family for Cisco IOS Release 12.2(18)SW:

Support for the SS7 Port Adapter (Product number PA-MCX-8TE1-M)

Platforms: Cisco 7301 routers

The Signaling System 7 (SS7) Port Adapter is a single-width, eight-port T1/E1 port adapter with a custom hardware-assist engine to support SS7 signaling. The PA features full channelization of up to 127 High-Level Data Link Control (HDLC)-encoded SS7 (or DS0) channels at 56 Kbps or 64 Kbps. Performance monitoring, Drop and Insert, BERT functionality, external clocking (with multiple backups), internal clocking, and standard alarm integration are also supported. The hardware-assist engine provides a 30% message signaling unit (MSU) per second performance improvement on the Versatile Interface Processor (VIP) under typical conditions.

New Software Features in Cisco IOS Release 12.2(18)SW

The following new software features are supported by the Cisco 7000 family for Cisco IOS Release 12.2(18)SW:

CS7 Monitor

Platforms: Cisco 7301 routers

The CS7 monitor feature allows the IP Transfer Point (ITP) to monitor Signaling System 7 (SS7)/High Speed Link (HSL) ports and send the message signaling units (MSUs) (using the Transmission Control Protocol (TCP)) to a server for collection/storage. This feature is available on the Cisco 7200 and Cisco 7500 platforms only.

ITP Instance Translation

Platforms: Cisco 7301 routers.

The ITP Instance Translation feature enables the conversion of packets between instances on the IP Transfer Point (ITP). Each instance is a separate domain with a defined variant, network indicator, ITP point code, optional capability point code, and optional secondary point code.

ITP M3UA/SUA Signaling Gateway

Platforms: Cisco 7301 routers

Based on open industry standards, Cisco's IP Transfer Point (ITP) product is designed for transporting Signaling System 7 (SS7) traffic over IP (SS7oIP) networks. Its design provides significant cost efficiencies and scalability enhancements over legacy SS7 networks. Using the IETF's MTP2-User Peer-to-Peer Adaptation Layer (M2PA) and Stream Control Transmission Protocol (SCTP) protocols, the initial release of the ITP product provided the base functionality to off load SS7 traffic to IP. Subsequent releases provided the full functionality found in typical legacy signaling transfer point (STP) nodes, such as global title translation (GTT), gateway screening and ISDN User Part (ISUP) transport. In addition, support for high speed links (HSLs) was added. Using the MTP3-User Adaptation (M3UA) and SCCP User Adaptation (SUA) protocols, this latest release of the ITP provides signaling gateway functionality between a legacy SS7 network and IP-enabled signaling end points (SEP) nodes.

ITP Multi-Layer Short Message Service Routing

Platforms: Cisco 7301 routers

The ITP Multi-Layer Routing (MLR) feature enables intelligent routing of Short Message Service (SMS) mobile originated (MO) messages based on the application or service from which they originated or to which they are destined. The MLR feature can make SMS message routing decisions based on information found in the Transaction Capabilities Applications Part (TCAP), Mobile Application Part (MAP), and MAP-user layers.

ITP Multiple Instances

Platforms: Cisco 7301 routers

The Multiple Instance feature enables multiple variant and network indicator combinations to run concurrently on one IP Transfer Point (ITP). Up to 8 instances can be configured.

ITP Packet Logging Facility

Platforms: Cisco 7301 routers

The ITP Packet Logging facility uses the Berkeley Software Distribution (BSD) Syslog protocol (RFC 3164) to send selected message signaling units (MSUs) to a user-selected monitoring tool using the User Datagram Protocol (UDP) connectionless protocol (RFC 768). Cisco Systems, Inc. does not provide monitoring tools specifically for receiving and decoding messages sent by the facility. The user must obtain a suitable tool for receiving syslog messages.

ITP SCCP/GTT

Platforms: Cisco 7301 routers

- GTT Support

  A global title is an application address, such as an 800 number, calling card number, or mobile subscriber identification number. Global Title Translation (GTT) is the process by which the Signaling Connection Control Part (SCCP) translates a global title into the point code and subsystem number of the destination service switching point (SSP) where the higher-layer protocol processing occurs.

  The two forms of GTT are as follows:

  - Intermediate GTT—A subsequent global title is required by another node; thus, the routing indicator is set to zero, indicating route by global title (GT).
  - Final GTT—No subsequent global title is required by another node; thus, the routing indicator is set to 1, indicating route by point code and subsystem number (PCSSN).

- Enhanced QoS for Signaling System 7 (SS7) Traffic

  Quality of service (QoS) refers to the performance of packet flow through networks. The goal in a QoS-enabled environment is to enable predictable service delivery to certain traffic classes or types regardless of other traffic flowing through the network at any given time. ITP QoS provides the framework that allows end-to-end QoS for SS7 packet flow through SS7-over-IP (SS7oIP) networks. End-to-end QoS is the ability of the network to deliver service required by specific network traffic from one end of the network to another. In particular, QoS features ensure improved and more predictable network service by providing the following services:

  - Dedicated bandwidth
  - Improving loss characteristics
  - Avoiding and managing network congestion
  - Shaping network traffic
  - Setting traffic priorities across the network

  QoS enables networks to control and predictably service a variety of network applications and traffic types. SS7 networks generally achieve QoS capabilities by over-provisioning bandwidth. Conventional SS7 networks lack the ability to identify different traffic types and provide network prioritization based on these traffic types. For instance, SS7 networks cannot separate ISUP and SCCP traffic and route this traffic over specific output links.

- SCCP Screening

  SCCP screening is a method of screening message signal units (MSUs) on inbound and outbound linkset. If the access list is inbound when the ITP receives a packet, the ITP checks the access list criteria statements for a match. If the packet is permitted, the ITP continues to process the packet. If the packet is denied, the ITP discards it.

  If the access list is outbound after receiving and routing a packet to the outbound interface, the ITP checks the access list criteria statements for a match. If the packet is permitted, the ITP transmits the packet. If the packet is denied, the ITP discards it.

- SCCP Management
- SCCP and GTT Screening
- SCCP and GTT Accounting
- Multiple Point Code support
- ITP Summary Routing and ANSI Cluster Routing

Refer to the document at the following URL for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122mb/122_4mb1/itp20/index.htm

ITP SCCP Load Balancing Enhancements

Platforms: Cisco 7301 routers

The ITP SCCP Load Balancing Enhancements included support for Signaling Connection Control Part (SCCP) class 1 traffic as well as SCCP address conversion (sometimes referred to as flexible numbering).

SIM Authentication and Authorization for Cisco WLAN Solution

Platforms: Cisco 7301 routers.

Cisco IOS Release 12.2(18)SW adds support for SIM Authentication/Authorization for Cisco WLAN Solution Architecture to the IP Transfer Point (ITP) product.

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.

Important Notes

Cisco 7500 Series Routers on Cisco IOS Release 12.2(19)SW

Cisco IOS Release 12.2(19)SW is not Route Processor Redundancy (RPR) compatible with previous IP Transfer Point (ITP) software releases, thus requiring a complete reload during deployment.

Caveats for Cisco IOS Release 12.2 SW

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 S are also in Cisco IOS Release 12.2(25)SW.

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.

Table 20 Caveats Reference for Cisco IOS Release 12.2 SW

DDTS Number	Open in Release	Resolved in Release
CSCdu53656		12.2(18)SW
CSCdz71127		12.2(18)SW
CSCea02355		12.2(18)SW
CSCea28131		12.2(18)SW
CSCec22954		12.2(25)SW5
CSCec44189		12.2(19)SW
CSCec45088		12.2(19)SW
CSCec61182		12.2(20)SW
CSCec62567		12.2(20)SW
CSCec69259		12.2(20)SW
CSCec79617		12.2(20)SW
CSCed01515		12.2(20)SW
CSCed08031	12.2(20)SW, 12.2(21)SW	
CSCed20020		12.2(20)SW

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

CSCed27956		12.2(21)SW
CSCed38527		12.2(21)SW
CSCed44759		12.2(21)SW
CSCed67628		12.2(21)SW1, 12.2(23)SW
CSCed82922		12.2(21)SW1, 12.2(23)SW
CSCed83705		12.2(25)SW3
CSCee08792		12.2(23)SW
CSCee09009		12.2(23)SW
CSCee11874		12.2(23)SW
CSCee13367		12.2(25)SW3
CSCee36139		12.2(23)SW1
CSCee41388		12.2(23)SW1
CSCee50294		12.2(25)SW
CSCee54303		12.2(23)SW1
CSCee86829		12.2(23)SW1
CSCee91201		12.2(23)SW1
CSCef08522		12.2(23)SW1
CSCef29094		12.2(25)SW
CSCef31588		12.2(25)SW
CSCef38050		12.2(25)SW
CSCef44438		!2.2(25)SW7
CSCef46191		12.2(25)SW4a
CSCef67682		12.2(25)SW4a
CSCef68324		12.2(25)SW3a
CSCef69373		12.2(25)SW
CSCef74580		12.2(25)SW
CSCef85587		12.2(25)SW
CSCef95065		12.2(25)SW
CSCeg01587		12.2(25)SW1
CSCeg08298		12.2(25)SW1
CSCeg18352		12.2(25)SW3
CSCeg37718		12.2(25)SW1
CSCeg40188		12.2(25)SW1
CSCeg50304		12.2(25)SW1
CSCeg50319		12.2(25)SW1
CSCeg72013		12.2(25)SW1
CSCeg83024		12.2(25)SW1, 12.2(25)SW3

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

CSCeh13554		12.2(25)SW3
CSCeh15067		12.2(25)SW3
CSCeh16859		12.2(25)SW3
CSCei61732		12.2(25)SW4, 12.2(25)SW4a
CSCei76358		12.2(25)SW3b
CSCek37177		12.2(25)SW8
CSCsa42016		12.2(25)SW1
CSCsa42261		12.2(25)SW1
CSCsa45054		12.2(25)SW1
CSCsa54632		12.2(25)SW1
CSCsa54864		12.2(25)SW1
CSCsa57699		12.2(25)SW3
CSCsa58560		12.2(25)SW3
CSCsa59599		12.2(25)SW3
CSCsa64953		12.2(25)SW3
CSCsa72249		12.2(25)SW3
CSCsa78896		12.2(25)SW3
CSCsa81379		12.2(25)SW2
CSCsa84521		12.2(25)SW3
CSCsa86279		12.2(25)SW4
CSCsa86523		12.2(25)SW4
CSCsa88289		12.2(25)SW3
CSCsa92616		12.2(25)SW3
CSCsa98311		12.2(25)SW4
CSCsa99303		12.2(25)SW4
CSCsb02059		12.2(25)SW3, 12.2(25)SW4
CSCsb02106		12.2(25)SW4
CSCsb03447		12.2(25)SW3
CSCsb04849		12.2(25)SW4
CSCsb05969		12.2(25)SW4
CSCsb11785		12.2(25)SW4
CSCsb15605		12.2(25)SW4
CSCsb15611		12.2(25)SW4
CSCsb19607		12.2(25)SW4
CSCsb26616		12.2(25)SW5
CSCsb33575		12.2(25)SW4
CSCsb34813		12.2(25)SW4

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

CSCsb58611		12.2(25)SW4
CSCsb64543		12.2(25)SW4
CSCsb74441		12.2(25)SW5
CSCsb91222		12.2(25)SW4a
CSCsb91588		12.2(25)SW5
CSCsb92248		12.2(25)SW5
CSCsc01492		12.2(25)SW5
CSCsc02671		12.2(25)SW5
CSCsc03807		12.2(25)SW5
CSCsc05943		12.2(25)SW5
CSCsc06052		12.2(25)SW5
CSCsc09788		12.2(25)SW5
CSCsc22745		12.2(25)SW5
CSCsc27995		12.2(25)SW5
CSCsc34914		12.2(25)SW5
CSCsc46651		12.2(25)SW5
CSCsc51378		12.2(25)SW5
CSCsc59050		12.2(25)SW5
CSCsc62555		12.2(25)SW5
CSCsc63988		12.2(15)SW6
CSCsc78421		12.2(25)SW6
CSCsd03523		12.2(25)SW6
CSCsd07326		12.2(25)SW6
CSCsd30900		12.2(25)SW6
CSCsd35259		12.2(25)SW6
CSCsd40334		12.2(25)SW7
CSCsd50936		12.2(25)SW6
CSCsd58381		12.2(25)SW7
CSCsd62477		12.2(25)SW7
CSCsd63672		12.2(25)SW7
CSCsd63762		12.2(25)SW6
CSCsd73205		12.2(25)SW7
CSCsd76797		12.2(25)SW7
CSCsd82015		12.2(25)SW7
CSCsd84614		12.2(25)SW7
CSCsd87381		12.2(25)SW7
CSCsd99215		12.2(25)SW7

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

CSCse17165		12.2(25)SW7
CSCse22221		12.2(25)SW7
CSCse22255		12.2(25)SW7
CSCse28466		12.2(25)SW7
CSCse45533		12.2(25)SW7
CSCse49379		12.2(25)SW7
CSCse49476		12.2(25)SW7
CSCse50769		12.2(25)SW8
CSCse58529		12.2(25)SW8
CSCse65471		12.2(25)SW8
CSCse70944		12.2(25)SW8
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
CSCsf32840		12.2(25)SW9
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
CSCsg18913		12.2(25)SW8
CSCsg21314		12.2(25)SW9
CSCsg34131		12.2(25)SW9
CSCsg45613		12.2(25)SW9
CSCsg45763		12.2(25)SW9
CSCsg47608		12.2(25)SW9
CSCsg54127		12.2(25)SW9
CSCsg59330		12.2(25)SW9
CSCsg62398		12.2(25)SW9
CSCsg89437		12.2(25)SW9
CSCsh23712		12.2(25)SW9
CSCsh26503		12.2(25)SW9
CSCsh28691		12.2(25)SW9
CSCsh37628		12.2(25)SW9

Caveats Reference for Cisco IOS Release 12.2 SW (continued)

591	12.2(25)SW9	
422	12.2(25)SW9	
649	12.2(25)SW9	

Open Caveats—Cisco IOS Release 12.2(25)SW9

This section documents possible unexpected behavior by Cisco IOS Release 12.2(25)SW9 and describes only severity 1 and 2 caveats and select severity 3 caveats.

There are no known open caveats for Cisco IOS Release 12.2(25)SW9.

Resolved Caveats—Cisco IOS Release 12.2(25)SW9

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(25)SW9. This section describes only severity 1 and 2 caveats and select severity 3 caveats

*CSCsf19615- ASP is not receiving traffic. There are no known workarounds..

- CSCsf32840

  When adding links to a linkset that is not in service, the route becomes restricted. Even if you remove these newly added links, the restriction will not clear, even though all the links in the linkset are available. The expected behavior would be to recalculate the available linksets, and remove the restriction.

  There are no known workarounds.

- CSCsg21314

  On a Cisco 7600 or a Cisco 7500 router with an E1 serial interface, the **show interfaces** output either reports incrementing input errors even though the links are running perfectly, or the reported input/output rates exceed the physical ability of the interface.

  This condition occurs when a FlexWAN interface encounters errors in the past and keeps them in its history. With each reporting period, the old values are added to the running total, making the error input seem to increment.

  Workaround: To verify whether there really are any slips or error seconds, check the **show controller** output. Log on to the FlexWAN console and issue a **clear count** command to reset the line card counters and to stop incrementing on the Supervisor. This solution should work provided no new errors are being encountered.

- CSCsg34131

  High CPU usage occurs in the Route/Switch Processor (RSP) of the Cisco 7500 IP Transfer Point (ITP). The **debug ip packet detail** output on the RSP shows Stream Control Transmission Protocol (SCTP) packets that should be handled by the Versatile Interface Processor (VIP) card; these packets should not be seen on the RSP.

  This condition occurs when an SCTP offload is enabled in the ITP, and SCTP association requests from an offloaded SCTP port are sent to the wrong VIP.

Workaround: There are two possible workarounds:

- Modify the configuration in the offending node to stop the SCTP association requests to the wrong VIP card, or
- Use an access control list (ACL) to block the SCTP packets from the offending nodes from reaching the RSP. For example:

```
access-list 101 deny 132 host node_ip_addr any log
access-list 101 permit ip any
interface FastEthernet X/Y/Z
ip access-group 101 in
```

- CSCsg45613

  After a mobile originated (MO) message comes in and goes to Multi Layer Routing (MLR), the IP Transfer Point (ITP) stops working

  This condition occurs after loading and replacing an address table. The scenario under which this error occurs is as follows: 1. The correct International Mobile Subscriber Identity (IMSI) table is loaded and active, ITP is working, and the table is scanned whenever a message comes in. (However, the config which uses this table is NOT saved to startup-config. As a result, at the next restart, the startup config is loaded without the IMSI table.) 2. A corrupted IMSI file is copied to the disk using the Trivial File Transfer Protocol (TFTP). The file is corrupted by a typo that is situated after the !eof keyword. (This is a typical error when using ultraedit in column edit mode.) 3. The **replace** command is issued. 4. ITP loads the corrupted file and says it has loaded successfully.

  Workaround: Power on/off to get ITP back up and running

- CSCsg45763

  When updating a route priority that has a single route for that destination, the associated **pc-conversion** statement is removed from the configuration. The problem does not occur if there is more than one route for that destination.

  There are no known workarounds.

- CSCsg47608

  A software-forced reload of a line card on the Cisco 7500 platform occurs when the router cannot allocate memory to handle an inbound Signaling Connection Control Part (SCCP) packet.

  This condition occurs when line card memory is exhausted. This problem is not the cause of any memory leak or fragmentation.

  There are no known workarounds.

- CSCsg54127

  If the Signaling System 7 (SS7) of an MTP2-User Peer-to-Peer Adaptation Layer (M2PA) link fails on an IP Transfer Point (ITP) group alternate peer as it takes over as the group manager, the link may not recover. Although the link show s as “avail” at the Message Transfer Part Level 3 (MTP3), it is failed at Level 2.

  Workaround: Issue the **shutdown** command followed by the **no shutdown** command while in link configuration submode to recover the link.

- CSCsg59330

  After a reload, the virtual linkset stays inaccessible. The **show cs7 route detail** command indicates that the virtual linkset is up and the non-adjacent status is allowed, but the destination status for the alias point codes is marked inaccessible. To resolve the problem all routing that used the linksets has to be removed, and then, the point code-conversion rows have to be removed and inserted. Upon insertion of the point code-conversion rows, the virtual linksets again become accessible. Then, all routing that used the virtual-linksets can be inserted again.

  Workaround: Remove the fast-restart option (**no instance x fast-restart**).

- CSCsg62398

  The IP Transfer Point (ITP) refuses to load a Global Title Translation (GTT) config file at boot time. This condition occurs when the GTT config Instance 0 references an application group in instance 1. This behavior is not allowed, and should have been prevented by the command line interface (CLI).

  Workaround: Delete the gta default for the GTT-Inter selector, create a new application group in instance 0, and then add back the default using the new application group.

- CSCsg89437

  An unsolicited Application Server Processor (ASP) state change in override mode generates only one Simple Network Management Protocol (SNMP) trap.

  This condition occurs when two ASPs are configured on an application server (AS) in override mode: ASP1 is active, and ASP2 is inactive. When ASP2 sends asp active to the signaling gateway (SG), the ASP1 status is changed to inactive. but no SNMP trap message is generated.

  There are no known workarounds.

- CSCsh23712

  The Versatile Interface Processor (VIP) on a Cisco 7500 platform running IP Transfer Point (ITP) software runs out of memory when processing traffic from an offloaded link to a non-offloaded link. The VIP may issue the following messages or reload due to CSCsg47608 (if not already installed).

  ```
  %IPC-5-SLAVELOG: VIP-SLOT5:
  %SYS-2-MALLOCFAIL: Memory allocation of 381032 bytes failed from 0x6039D468, alignment
  32
  Pool: Processor Free: 614300 Cause: Memory fragmentation
  Alternate Pool: None Free: 0 Cause: No Alternate pool
  -Process= "Chunk Manager", ipl= 2, pid= 1
  -Traceback= 602EDC88 60382AD0 60387A98 6039D470 603827A0 603825B8
  %SYS-2-CHUNKEXPANDFAIL: Could not expand chunk pool for DS7 Pkt Info c. No memory
  available
  -Process= "Chunk Manager", ipl= 2, pid= 1
  -Traceback= 602EDC88 603825FC
  ```

  The following conditions must be met for the memory depletion to occur: Message Transfer Part Level 3(MTP3) offload is configured, but the MTP2-User Peer-to-Peer Adaptation Layer (M2PA) links are not offloaded. Packets arriving on an offloaded link are MTP3 routed to a link that is not offloaded.

  Workaround: The following workarounds exist for this problem: 1. Offload all links, including the M2PA. 2. Turn off MTP3 offload to force all links to be serviced on the Route/Switch Processor (RSP), which will increase RSP CPU demand.

- CSCsh26503

  A Cisco 7200 series router IP Transfer Point (ITP) changeover that contains more than 16 combined linksets corrupts the Signaling Link Terminal (SLT) table.

  This condition occurs because each time a **shut/no shut** is performed on the linkset, the link is not added back to the SLT table. When this action is done to all the links, you end up with no links in the SLT table and cannot route traffic.

  Workaround: Remove the alternate routes for certain destinations.

- CSCsh28961

  The IP Transfer Point (ITP) reloads due to a process watchdog timeout when configured as an SCCP User Adaptation (SUA) Signaling Gateway (SG) and memory is depleted. The failing process is the CS7 SCCP Input process.

  This condition occurs when ITP is configured as an SUA SG, processor memory is exhausted such that a new buffer cannot be obtained at process level, and the received SCCP message indicates a "return on error."

  There are no known workarounds.

- CSCsh37628

  The "%ALIGN-1-FATAL: Corrupted program counter" bus error is output when the **snmpwalk** command is issued for an IP Transfer Point (ITP) MIB.

  There are no known workarounds.

- CSCsh49591

  Preventive transfer-prohibited (TFP) is not sent to the C-link peer when the point code goes inactive.

  This condition occurs when you bring an XUA point code active on a pair of IP Transfer Points (ITPs) with C-link configured, the point code is configured in an ANSI instance (or ITU with **cs7 national-options TFR** not enabled), and you bring the point code inactive on one ITP such that XUA traffic is routed using the C-link.

  There are no known workarounds.

- CSCsh66422

  Unable to move point code (PC) from instance 1 to instance 0.

  There are no known workarounds.

- CSCsh79649

  The SCCP User Adaptation (SUA) Application Server Processor (ASP) causes the router to crash after a **shut/no shut**.

  There are no known workarounds.

Open Caveats—Cisco IOS Release 12.2(25)SW8

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.

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

Resolved Caveats—Cisco IOS Release 12.2(25)SW8

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(25)SW8. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCek37177

  The Cisco IOS Transmission Control Protocol (TCP) listener in certain versions of Cisco IOS software is vulnerable to a remotely-exploitable memory leak that may lead to a denial of service condition.

  This vulnerability only applies to traffic destined to the Cisco IOS device. Traffic transiting the Cisco IOS device will not trigger this vulnerability.

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

  This issue is documented as Cisco bug ID CSCek37177.

  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-20070124-crafted-tcp.shtml

- CSCse50769

  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

  There are no known workarounds.

- CSCse58529

  On Cisco 7500 and 7600-based IP Transfer Points (ITPs), the PA DS0 loopback options for **internal** and **line** are not available. The **local** and **remote** loopback options are available, but do not provide the desired functionality.

  This condition occurs in certain SW ITP releases.

  Workaround: Only use DS0 loopback on remote device nodes or entire T1/E1 interfaces, if possible.

- CSCse65471

  The system becomes unresponsive after a Versatile Interface Processor (VIP) online insertion and removal.

  This condition occurs when a large route table containing the 0.0.0.0 default gateway causes the system to enter an endless loop of routing updates. The console will not be available and links may fail.

  Workaround: Remove the default 0.0.0.0 gateway route from the route table.

- CSCse70944

  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.

  There are no known workarounds.

- CSCse71985

  The IP Transfer Point (ITP) broadcasts extraneous transfer-allowed (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.

  There are no known workarounds.

- CSCse74363

  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

  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

  The IP Transfer Point (ITP) ignores the Telecommunications Technology Committee (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 source-route transparent bridging (SRT) messages to M3UA/SUA point codes in the network.

- CSCse99146

  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:

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

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

  There are no known workarounds.

- CSCsf08276

  An IP Transfer Point (ITP), configured as an MTP3 User Adaptation (M3UA) or SCCP User Adaptation (SUA) Signaling 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 Signaling Connection Control Part (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

  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

  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).

  There are no known workarounds.

- CSCsg11535

  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 application servers.

- CSCsg12763

  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

  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

  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 **show run** command output, but not in the **show 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.

Open Caveats—Cisco IOS Release 12.2(25)SW7

This section documents possible unexpected behavior by Cisco IOS Release 12.2(25)SW7 and describes only severity 1 and 2 caveats and select severity 3 caveats.

There are no known open caveats for Cisco IOS Release 12.2(25)SW7.

Resolved Caveats—Cisco IOS Release 12.2(25)SW7

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(25)SW7. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCef44438

  A Cisco router crashes when Cisco Express Forwarding (CEF) is processing new routing updates while entries are being deleted from the CEF table (for example, following a **clear cef table** command or an online insertion and removal (OIR) of a line card).

  This condition occurs on Cisco routers running Cisco IOS Release 12.2(25)S or later releases.

  There are no known workarounds.

- CSCsd40334

  Processing a specially crafted IPv6 Type 0 Routing header can crash a device running Cisco IOS software. This vulnerability does not affect IPv6 Type 2 Routing header which is used in mobile IPv6. IPv6 is not enabled by default in Cisco IOS.

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

  There are workarounds available to mitigate the effects of the vulnerability. The workaround depends on if Mobile IPv6 is used and what version on Cisco IOS is being currently used.

  This advisory is posted at
  http://www.cisco.com/warp/public/707/cisco-sa-20070124-IOS-IPv6.shtml

- CSCsd58381

  Processing a specially crafted IPv6 Type 0 Routing header can crash a device running Cisco IOS software. This vulnerability does not affect IPv6 Type 2 Routing header which is used in mobile IPv6. IPv6 is not enabled by default in Cisco IOS.

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

  There are workarounds available to mitigate the effects of the vulnerability. The workaround depends on if Mobile IPv6 is used and what version on Cisco IOS is being currently used.

  This advisory is posted at
  http://www.cisco.com/warp/public/707/cisco-sa-20070124-IOS-IPv6.shtml

- CSCsd62477

  A Cisco router may crash on **sms_compare_destSme.** The following traceback appears:

  ```
  TLB (load or instruction fetch) exception, CPU signal 10, PC = 0x41184100
  -Traceback= 41184100 41461158 41462000 4116EFAC 411729D8 41186E68 41187890 41114C98
  41115454 411125D8 410FAE34 410FB29C 41108478 41108610 41108138
  ```
  This condition can occur within normal working conditions.

  There are no known workarounds.

- CSCsd63672

  Some IP Transfer Point (ITP) group links remain in the FAILED state after restarting either the group manager or the alternate.

  This condition occurs when the ITP is configured with ITP group capability, and the amount of information requiring synchronization between the manager and the 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

  IP Transfer Point (ITP) crashes when processing a message destined for an MTP3 User Adaptation/SCCP User Adaptation (M3UA/SUA) application server (AS) when all configured Application Server Processors (ASPs) have weight=0.

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

- CSCsd76797

  When an operator enters a **shut** command in cs7 asp or cs7 MTP3 User Adaptation/SCCP User Adaptation (M3UA/SUA) submode, the IP Transfer Point (ITP) closes Stream Control Admission Protocol (SCTP) associations by sending an SCTP ABORT chunk instead of an SCTP SHUTDOWN chunk.

  There are no known workarounds.

- CSCsd82015

  The Application Server Processor (ASP) state is out of sync between the active and the standby.

  This condition occurs when an ASP is shut with **shut AS** and is seen after the Route/Switch Processor (RSP) switchover. When the new standby boots after the switchover, it receives a bulk sync from the master RSP. During this process the active RSP rejects any Stream Control Admission Protocol (SCTP) associations for a shut AS, and those ASPs become out of sync.

  There are no known workarounds.

- CSCsd84614

  The Route/Switch Processor (RSP) may crash during linkset configuration.

  This condition occurs when a configuration command is entered while in linkset submode.

  There are no known workarounds.

- CSCsd87381

  Some MTP3 User Adaptation/SCCP User Adaptation (M3UA/SUA) ERR messages sent by the IP Transfer Point (ITP) do not include the diagnostic info parameter.

  This issue occurs during error conditions detected by the ITP when the ITP responds with an M3UA or SUA ERR message. This is usually a response to a received M3UA/SUA message.

  There are no known workarounds.

- CSCsd99215

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

  There are no known workarounds.

- CSCse17165

  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 *max-return* value.

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

- CSCse22221

  IP Transfer Point (ITP) crashes when two users from two different telnet sessions are concurrently configuring High Speed Link (HSL) profile parameters for the same cs7 profile.

  Workaround: Ensure no concurrent configurations are done on the hsl profile.

- CSCse22255

  A slave IP Transfer Point (ITP) in a cs7 group enters into high CPU usage caused by the CS7 Group Mgmt process and finally crashes.

  This occurs when one of the Signaling System 7 (SS7) links configured is flapping.

  There are no known workarounds.

- CSCse28466

  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.

- CSCse45533

  Messages that are routed by Multi-Layer Routing (MLR) with a MLR **gt** result may contain invalid data in the encoding scheme byte of the called party address.

  This condition occurs randomly. It may occur when MLR routes a messages received with **gt cdpa** to a new gt cdpa.

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

- CSCse49379

  An internal Versatile Interface Processor (VIP)/Route/Switch Processor (RSP) routing loop may occur.

  This condition can be caused by high RSP CPU usage before or during the routing loop and can occur during the following related conditions: Application Server Processor (ASP) congestion, IP and Signaling System 7 (SS7) network instability, malfunctioning ASP nodes, and heavy console output over multiple telnet sessions. To diagnose the routing loop, enter repeated **show cs7 asp statistics** commands and look for the Outbound Packets Sent value to increment while the Inbound Packets Rcvd value does not.

  There are no known workarounds.

- CSCse49476

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

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

  2. 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.

Open Caveats—Cisco IOS Release 12.2(25)SW6

This section documents possible unexpected behavior by Cisco IOS Release 12.2(25)SW6 and describes only severity 1 and 2 caveats and select severity 3 caveats.

There are no known open caveats for Cisco IOS Release 12.2(25)SW6.

Resolved Caveats—Cisco IOS Release 12.2(25)SW6

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(25)SW6. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCsc63988

  Links are reported as available, but the interfaces are down/failed.

  This issue occurs in Cisco 7500 series routers under the following conditions:

  - When there is high traffic
  - When one of the Versatile Interface Processors (VIPs) in the system must reload due to a software or hardware failure.

  Workaround: Load balance traffic to prevent the system from being overloaded.

- CSCsc78421

  An IP Transfer Point (ITP) configured with High Speed Links (HSLs) sometimes retransmits lost signal degrade (SD) power distribution units (PDUs) twice instead of just once.

  This condition occurs when a PDU transmit is followed by a POLL. When this happens, 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.

  There are no known workarounds.

- CSCsd03523

  After a switchover, all links remain in the RESTART state. After approximately five minutes, the following error message is observed for all Versatile Interface Processors (VIPs) on the Cisco 7500 router:

  ```
  *Jan 11 17:24:54.387: %DCS7-3-DCS7DISABLE: Fatal error, slot 1: No window message, LC
  to RP IPC is not operational RC=0
  *Jan 11 17:24:54.387: %DCS7-5-INFO: Starting fatal error recovery for line card in
  slot  1
  ```

  This issue only occurs on the IP Transfer Point (ITP) Cisco 7500 platform when **cs7 offload mtp3** is configured and **cs7 nso** is not configured.

  Workaround: Disable **cs7 offload mtp3** or enable **cs7 nso**.

- CSCsd07326

  The MTP3 User Adaptation (3UA) or SCCP User Adaptation (SUA) (XUA) Application Server Processor (ASP) cannot connect to the IP Transfer Point (ITP) if the ASP is configured with remote (ephemeral) port 0, and the ASP is offloaded to a Versatile Interface Processor (VIP).

  This issue only occurs on a Cisco 7500 router with offloaded ASPs. For the non-offloaded ASPs, the ephemeral port 0 can be configured and the ASPs can connect.

Workaround: Perform the following:

1. Do not offload the ASP with remote port 0 to a VIP.

2. Configure a valid, non-zero remote port for the ASP that needs to be offloaded. The corresponding, remote ASP has to use the configured non-zero port for a successful connection to ITP.

- CSCsd30900

  Under rare conditions, the IP Transfer Point (ITP) may reload.

  This issue is observed when all of the following conditions occurs:

  1. Two ITPs are configured as Signaling Gateway (SG) mates.

  2. An application server (AS) with at least 2 Application Server Processors (ASPs) and traffic mode of loadshare bindings is configured on both ITPs.

  3. Each ITP receives a packet destined for the application server (AS) with the same loadshare seed (for example, CIC, SLS), and each ITP binds the loadshare seed to a different ASP.

  There are no known workarounds.

- CSCsd35259

  The IMA port adapter, 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 High Speed Link (HSL) based Signaling System 7 (SS7) links to go down and come back up at the time of the switch.

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

  Workaround: Configure each IMA/HSL port as follows where 7 is any unused, shutdown port on the IMA PA:

  ```
  clock source common 7
  clock source line
  ```
  This effectively sets each port to derive its clock from port 7 and then sets it back to source it from line.

- CSCsd50936

  After an Ethernet cable is pulled out, the line protocol state of the interface is incorrectly displayed as “up” on the /Route/Switch Processor (RSP) console. The actual sequence of events is that the line protocol will transition to down, and the appropriate traps and console messages will be generated. When the offloaded MTP3 User Adaptation/SCCP User Adaptation (M3UA/SUA) Stream Control Transmission Protocol (SCTP) link fails, the line protocol on the RSP will then show as “up” but a console message will not be generated.

  For example:

  ```
  Router#show int fastEthernet 0/0/0
   FastEthernet0/0/0 is up, line protocol is up
  ```
  However, the line protocol state on the Versatile Interface Processor (VIP) is correctly displayed as down.

  ```
  VIP-Slot0>show int
   FastEthernet0/0 is up, line protocol is down
  ```
  This issue requires an offloaded M3UA/SUA SCTP association to exist on the VIP in question.

  Workaround: Perform a **shut/no shut** of the interface to correct the line protocol state on the RSP.

- CSCsd63762

  The **network-appearance** command under a configuration 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 a reboot, the router displays an error when it tries to configure such a network appearance.

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

Open Caveats—Cisco IOS Release 12.2(25)SW5

This section documents possible unexpected behavior by Cisco IOS Release 12.2(25)SW5 and describes only severity 1 and 2 caveats and select severity 3 caveats.

There are no known open caveats for Cisco IOS Release 12.2(25)SW5.

Resolved Caveats—Cisco IOS Release 12.2(25)SW5

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(25)SW5. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCec22954

  After rebooting a Cisco 7500 router that has a PA-A3-8T1IMA/PA-A3-8E1IMA PA and ima-group interface configuration, the following error message can be seen in the logs of the Versatile Interface Processor (VIP):

  ```
  %ATMPA-1-RPTFAIL: ATM0/ima0 failed to send report 0 at ../pas/if_vip_loki.c
  ```

  This caveat is a duplicate of CSCin15053.

- CSCsb26616

  MTP2-User Peer-to-Peer Adaptation Layer (M2PA) links remain in initial alignment state after a Versatile Interface Processor (VIP) online insertion and removal (OIR). This defect can be seen in a VIP OIR and when the next hop interface for the Stream Control Transmission Protocol (SCTP) association(s) resides on another VIP.

  Workaround: Set up the IP routing where the destination for an M2PA link is reachable only by interfaces on the VIP wo which the M2PA link is off-loaded.

- CSCsb74441

  When the Cisco 7507 router operates in Non-Stop Operation (NSO) mode with MTP3 User Adaptation (M3UA) and SCCP User Adaptation (SUA) traffic offloaded to a Versatile Interface Processor (VIP) card, if the user changes the order of remote-ip addresses defined under Application Server Processor (ASP) configuration, the ASP state goes to the down state.

  This condition occurs on a Cisco 7507 router configured as an IP Transfer Point (ITP) with the NSO feature enabled in Cisco IOS Release 12.2(25)SW3.

  Workaround: To avoid this problem, keep the order of the IP address definition for the ASPs, and avoid changing the order after the Stream Control Transmission Protocol (SCTP) associations have been established from the application server (AS) to the Signaling Gateway (SG).

- CSCsb91588

  When the origin International Mobile Subscriber Identity (IMSI) feature is obtained and subsequently inserted into a proxied MO-FORWARD-SM dialogue, the insertion of the IMSI exceeds the maximum size that Signaling Connection Control Part (SCCP) or Message Transfer Part, Level 3 (MTP3) can transport without segmentation.

  This situation occurs under the following conditions:

  – When a MAP version 3 MO-FORWARD-SM message received from the message service center (MSC) does not contain an International Mobile Subscriber Identity (IMSI), and the length of the message signaling unit (MSU) received from the MSC is greater than 263 octets (including SI).

  – When SMS MO Proxy successfully obtains the origin IMSI, as requested by a matched Short Message Service (SMS) rule with the **result obtain-orig-imsi**.

  – When the configured SMS MO Proxy version is 3.

  Workaround:

  1) Unconfigure the rule which obtains the origin IMSI.

  2) 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

  High Speed Link (HSL) sscop timer commands are stored in incorrect order in the running-config.

  IP Transfer Point (ITP) reports Timer_POLL or Timer-Keepalive errors on boot-up. An example error follows:

  ```
  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
  ```

  The correct order in the running-config should be: cs7 profile 01 hsl sscop idle-timer 250 sscop keepalive-timer 250 sscop poll-timer 125.

  The incorrect order displayed in running-config is: cs7 profile 01 hsl sscop poll-timer 125 sscop keepalive-timer 250 sscop idle-timer 250.

  There are no known workarounds.

- CSCsc01492

  A Cisco 7500 router running IP Transfer Point (ITP) software configured with an Asynchronous Transfer Mode (ATM) High Speed Link (HSL) that uses **oam-pvc manage** encounters a situation in which the link is up and passing traffic and the permanent virtual circuit (PVC) is up, but the line protocol displays as down in the Route/Switch Processor (RSP) **show interface** command.

  The condition occurs when the above configuration is in place and a remote failure in the ATM network occurs such that an Operation, Administration, and Maintenance (OAM) alarm indication signal (AIS) is sent to the ITP for this link/PVC. Upon recovery of the error, OAM must recover before the Service Specific Connection Oriented Protocol (SSCOP) link recovers for the stuck condition to occur.

  Workaround: Do not use **oam-pvc manage** on these links. If **oam-pvc manage** is used, a local disconnect of the interface may resolve the state, but it is dependent on the timing on the other side of the link.

- CSCsc02671

  The IP Transfer Point (ITP) is not sending the Remote Inhibit Test message. This occurs when the variant is ITU and when a remote node inhibits a link.

  When the ITP receives a remote inhibit, it is supposed to start the Message Transfer Part, Level 3 (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 the uninhibit message is lost.

  Workaround: Under normal conditions no action is required - when the remote side uninhibits the link, this will clear the remote inhibit status. The Remote Inhibit Test is designed to catch the case where the remote uninhibit message is lost. If this occurs, a **shut/no shut** of the linkset will correct the inhibit status.

- CSCsc03807

  Under rare conditions, the IP Transfer Point (ITP) may reload while viewing the output of the **show cs7 gtt config** command. A reload may occur if a user makes a change in Global Title Translation (GTT) configuration while in the middle of viewing the output of the **show cs7 gtt config** command.

  Workaround: Do not make GTT configuration changes while in the middle of viewing the output of the **show cs7 gtt config** command.

- CSCsc05943

  A verification and regression test does not pass.

  Workaround: Not applicable because this test is not performed in a production environment.

- CSCsc06052

  On a Cisco 7500 router, IP Transfer Point (ITP) systems configured with low speed links do not generate %LINEPROTO-5-UPDOWN console messages consistently when serial links transition the line protocol up and down.

  Workaround: Use %CS7MTP3-5-LINKUPDOWN messages and their associated traps, which are generated. These messages are the best method of tracking the Signaling System 7 (SS7) link availability.

- CSCsc09788

  When the High Speed Link (HSL) is activated and connected to a legacy Signaling Transfer Point (STP), STP sends out too many packets initially. Due to this heavy packet stream, the rx buffer exceeds its limit, which causes the Asynchronous Transfer Mode (ATM) driver to use a fallback buffer; console error messages are generated.

  There are no known workarounds.

- CSCsc22745

  The IP Transfer Point (ITP) always sets the national indicator within the calling and called party address indicator field to '1'b when generating Signaling Connection Control Part (SCCP) management messages for non-ANSI variants. The Signaling Transfer Point (STP) and Signaling Control Point (SCP) implementations may reject or discard these messages for non-ANSI variants.

  This problem occurs under the following conditions:

  – The configured Message Transfer Part 3 (MTP3) and SCCP variant is not ANSI (for example, ITU, China, or Japan).

  – An STP or SCP that processes SCCP management messages from the ITP performs screening or validation on the national indicator setting.

  There are no known workarounds.

- CSCsc27995

  On a Cisco 7500 router, IP Transfer Point (ITP) systems, configured with high speed Signaling System 7 (SS7) over Asynchronous Transfer Mode (ATM) links, do not consistently generate %LINEPROTO-5-UPDOWN console messages (and associated traps) when ATM links transition the line protocol up and down.

  Workaround: Use %CS7MTP3-5-LINKUPDOWN messages and their associated traps, which are generated. These messages are the best method of tracking SS7 link availability.

- CSCsc34914

  When an MTP3 User Adaptation (M3UA) link established to a PGW 9.5(2) host is torn down due to the PGW host shutting down, the IP Transfer Point (ITP) fails.

  There are no known workarounds.

- CSCsc46651

  A message signaling unit (MSU) was corrupted during instance conversion.

  This condition occurs when converting an MSU from one instance to another where the MSU is formatted with the Signaling Connection Control Part (SCCP) portion containing the data in between the calling and called parties.

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

- CSCsc51378

  When upgrading directly from Cisco IOS Release 12.2(4)MB10 or earlier to Cisco IOS Release 12.2(25)SW4a, the upgrade to Cisco IOS Release 12.2(25)SW4a can result in configuration 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.
  ```

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

- CSCsc59050

  Shutting down and unconfiguring IP Transfer Point (ITP) E1 links using either a cut-and-paste operation or through a script can result in a Versatile Interface Processor (VIP) failure due to a timing issue.

  Workaround: Shut down the ITP E1 links first, and then wait for 10 seconds before unconfiguring those links.

- CSCsc62555

  A new binding is established when the Application Server Processor (ASP) is already active on both IP Transfer Points (ITPs). The binding is active on the receiving ITP, but inactive on the other ITP.

  There are no known workarounds.

Open Caveats—Cisco IOS Release 12.2(25)SW4a

This section documents possible unexpected behavior by Cisco IOS Release 12.2(25)SW4a and describes only severity 1 and 2 caveats and select severity 3 caveats.

There are no known open caveats for Cisco IOS Release 12.2(25)SW4a.

Resolved Caveats—Cisco IOS Release 12.2(25)SW4a

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(25)SW4a. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCef46191

  A specifically crafted Transmission Control Protocol (TCP) connection to a telnet or reverse telnet port of a Cisco device running Internetwork Operating System (IOS) may block further telnet, reverse telnet, Remote Shell (RSH), Secure Shell (SSH), and in some cases Hypertext Transport Protocol (HTTP) access to the Cisco device. Telnet, reverse telnet, RSH and SSH sessions established prior to exploitation are not affected.

  All other device services will operate normally.

  User initiated specially crafted TCP connection to a telnet or reverse telnet port results in blocking further telnet sessions. Whereas, services such as packet forwarding, routing protocols and all other communication to and through the device remains unaffected.

  Workaround: The detail advisory is available at the following URL:

  http://www.cisco.com/warp/public/707/cisco-sa-20040827-telnet.shtml

- CSCef67682

  Reception of certain IPv6 fragments with carefully crafted illegal contents may cause a router running Cisco IOS to reload if it has IPv6 configured. This applies to all versions of Cisco IOS that include support for IPv6.

  The system may be protected by installing appropriate access lists to filter all IPv6 fragments destined for the system. For example:

  ```
  interface Ethernet0/0
    ipv6 traffic-filter nofragments in
  !
  ipv6 access-list nofragments
    deny ipv6 any my-address1 undetermined-transport
    deny ipv6 any my-address2 fragments
    permit ipv6 any any
  ```

  This must be applied across all interfaces, and must be applied to all IPv6 addresses which the system recognizes as its own.

  This will effectively disable reassembly of all IPv6 fragments. Some networks may rely on IPv6 fragmentation, so careful consideration should be given before applying this workaround.

  We would recommend for customers to upgrade to the fixed IOS release. All IOS releases listed in IPv6 Routing Header Vulnerability Advisory at http://www.cisco.com/warp/public/707/cisco-sa-20070124-IOS-IPv6.shtml contain fixes for this issue.

- 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.

- CSCsb91222

  Valid message signaling units (MSUs) with an Signaling Connection Control Part (SCCP) portion of 256 octets or greater are not properly routed by the IP Transfer Point (ITP) SCCP layer. The following message is issued to the ITP console:

  ```
  %CS7SCCP-5-SCCPSYNTAX: SCCP received message containing a syntax error.
  LS=linkset0 DPC=22.2.1:0 OPC=1.4.5:0 Type=9 Class=
  ```
  This condition occurs when an MSU with an SCCP portion of 256 octets or greater is received by the ITP for local SCCP processing, such as global title translation.

  There are no known workarounds.

Open Caveats—Cisco IOS Release 12.2(25)SW4

This section documents possible unexpected behavior by Cisco IOS Release 12.2(25)SW4 and describes only severity 1 and 2 caveats and select severity 3 caveats.

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

Resolved Caveats—Cisco IOS Release 12.2(25)SW4

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(25)SW4. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- 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.

- CSCsa86279

  On an IP Transfer Point (ITP) running Cisco IOS Release 12.2(25)SW3 or earlier, the parameters configured for an off-loaded MTP2-User Peer-to-Peer Adaptation Layer (M2PA) link may not be applied after a reload.

  Workaround: Re-configure the link parameters.

- CSCsa86523

  On an IP Transfer Point (ITP) running Cisco IOS Release 12.2(25)SW3 or earlier releases, packet loss may occur during a changeover due to a shutdown of an interface on which an off-loaded MTP2-User Peer-to-Peer Adaptation Layer (M2PA) links resides.

  There are no known workarounds.

- CSCsa98287

  When running IP Transfer Point (ITP) software, adding a Signaling System 7 (SS7) link to an existing linkset that is in the shutdown state will not prevent the new link from becoming available and will cause the linkset to become available as well.

  This condition occurs when the linkset is 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

  In Cisco IOS Release 12.2(2)5SW2 or earlier releases, 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
  ```
  There are no known workarounds.

- CSCsa99303

  Link drops fail to be reported in the output of **show cs7 linkset statistics** when **cs7 offload mtp3** is configured.

  There are no known workarounds.

- CSCsa99440

  The **show controllers** output will not show any clock slip, even if there are mismatches in the clock reference at both ends of an E1 line for the PA-MCX-8TE1-M port adapter.

  There are no known workarounds.

- CSCsb02059

  The Hop Counter for Extended Unitdata (XUDT) messages is decremented twice when the Global Title Translation (GTT) result is an application server (AS).

  This condition occurs on a Cisco 7500 router with Message Transfer Part, Level 3 (MTP3) offload configured, when Signaling Connection Control Part (SCCP) traffic using message type XUDT with MTP3 offload is configured, and traffic is GTT routed to an AS result.

  Workaround: Turn off MTP3 offload.

- CSCsb02106

  A “DCS7-4-DCS7MSG: Invalid message received” error may be observed on the IP Transfer Point (ITP) upon receiving an User Part Unavailable (UPU) with user part identity 3 (from the Signaling Connection Control Part (SCCP)), if the affected PC is configured in the Global Title Translation (GTT) MAP table and **cs7 offload mtp3** is configured.

  There are no known workarounds.

- CSCsb04849

  When IP Transfer Point (ITP) receives a Signaling Connection Control Part (SCCP) message containing a GTI (Global Title Indicator) that equals 8, a traceback will be generated. The router will not unexpectedly reload and there will be no impact in the performance of the device.

  ITP only supports GTI 2 and 4. This can be considered a cosmetic issue.

  There are no known workarounds.

- CSCsb05969

  The following parameters configured for an MTP3 User Adaptation/SCCP User Adaptation (M3UA/SUA) instance are not applied if the M3UA/SUA instance is off loaded:

  - receive-window
  - unordered-priority
  - init-retransmit
  - init-timeout
  - max-inbound-streams

  There are no known workarounds.

- CSCsb11785

  The Route/Switch Processor (RSP) unexpectedly reloads when loading the Multi-Layer Routing (MLR) address table.

  This condition occurs when loading an MLR address table file for an address table that already exists.

  There are no known workarounds.

- CSCsb15605

  A Versatile Interface Processor (VIP) unexpectedly reloads with a translational bridging (TLB) exception and reports a fatal hardware failure (signal=22).

  This condition occurs on a VIP6-80 running Cisco IOS Release 12.2(23)SW1 with a PA-MCX-8TE1-M port adapter (PA).

  There are no known workarounds.

- CSCsb15611

  A Versatile Interface Processor (VIP) unexpectedly reloads with a translational bridging (TLB) exception and reports a fatal hardware failure (signal=22).

  This condition occurs on a VIP6-80 running Cisco IOS Release 12.2(23)SW1 with a PA-MCX-8TE1-M port adapter (PA).

  There are no known workarounds.

- CSCsb19607

  The link does not activate if an adjacent point code is identical to a local point code of another instance on the IP Transfer Point (ITP).

  This issue occurs under the following conditions:

  - Message Transfer Part, Level 3 (MTP3) offload must be enabled
  - cs7 multi-instance must be configured

  - An adjacent point code is identical to local point code of another instance
  - The release must be Cisco IOS Release 12.2-25.SW3

  Workaround: If the config is saved and ITP loaded with this as its starting config, the links will activate normally.

- CSCsb33575

  On a Cisco 7200 or Cisco 7300 router, Message Transfer Part Level 2 (MTP2) links fail and do not recover. Executing a **show controller serial x/x:x** for the failed link shows that the ds->tx_count is at 12, when it should be 0 when the link is not in service.

  This issue can occur when some other interfaces on the PA are down, and the links that are available have a lot of errors that cause retransmissions.

  Workaround: Reload the IP Transfer Point (ITP) to bring the links back up.

- CSCsb34813

  A multi-homed Stream Control Transmission Protocol (SCTP) association goes down.

  This condition occurs when the primary interface is shutdown.

  There are no known workarounds.

- CSCsb42738

  The Versatile Interface Processor (VIP) on a Cisco 7500 router unexpectedly reloads while running the Cisco IP Transfer Point (ITP) feature image. The Route/Switch Processor (RSP) will report the following Cybus error when the VIP unexpectedly reloads:

  ```
  Jun 10 07:36:41.103 CST: %RSP-3-ERROR: CyBus1 error 10
  Jun 10 07:36:41.103 CST: %RSP-3-ERROR:     command/address mismatch
  Jun 10 07:36:41.103 CST: %RSP-3-ERROR:   bus command write 2bytes (0xD)
  Jun 10 07:36:41.103 CST: %RSP-3-ERROR:   address offset (bits 3:1) 0
  Jun 10 07:36:41.107 CST: %RSP-3-ERROR:   virtual address (bits 23:17) 000000
  ```

  The VIP unexpected reload will produce a crashinfo file that has no traceback information in it.

  This issue occurs under the following conditions:

  - Message Transfer Part, Level 3 (MTP3) Offload is configured
  - The configuration includes a loopback interface definition
  - The first interface on the VIP that crashes is configured and is being used

  Workaround: One of the three conditions above must be removed:

  - Disable MTP3 Offload and reload the router
  - Remove loopback interface and reload the router
  - Disable the first interface on the VIP. A router reload to correct the situation is not required if this workaround option is chosen

- CSCsb58611

  After an Non-Stop Operation (NSO) switchover on an IP Transfer Point (ITP) on a Cisco 7500 router, a Versatile Interface Processor (VIP) unexpected reloads due to a watchdog timeout at the Signaling System 7 (SS7) port adapter (PA) process:

  ```
  Jul 29 10:50:30.435 EDT: %SYS-2-WATCHDOG: Process aborted on watchdog timeout, process
  = SS7 PA Proc.
  ```

This issue occurs under the following conditions:

- The failing VIP has an Message Transfer Part Level 2 (MTP2) link defined on at least one serial interface
- A administratively down E1/T1 controller with an MTP2 link defined on it is activated using a **no shutdown** command
- An NSO switchover to the Standby Route/Switch Processor (RSP) occurs

Workaround: Do not issue a **no shutdown** command for E1/T1 controllers that have MTP2 links defined on them. If the **no shutdown** command cannot be avoided, reload the Standby RSP using the **hw-module sec-cpu reset** command after activating the controller.

- CSCsb64543

  If Signaling System 7 (SS7) links bounce due to a 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. Signaling 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. Take the route commands from the **show running config** output and cut-n-paste them back in once you are in **config-cs7-rt** submode.

Open Caveats—Cisco IOS Release 12.2(25)SW3b

This section documents possible unexpected behavior by Cisco IOS Release 12.2(25)SW3b and describes only severity 1 and 2 caveats and select severity 3 caveats.

There are no known open caveats for Cisco IOS Release 12.2(25)SW3b.

Resolved Caveats—Cisco IOS Release 12.2(25)SW3b

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(25)SW3b. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCei76358

  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)SW3a

This section documents possible unexpected behavior by Cisco IOS Release 12.2(25)SW3a and describes only severity 1 and 2 caveats and select severity 3 caveats.

There are no known open caveats for Cisco IOS Release 12.2(25)SW3a.

Resolved Caveats—Cisco IOS Release 12.2(25)SW3a

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(25)SW3a. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- 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)SW3

This section documents possible unexpected behavior by Cisco IOS Release 12.2(25)SW3 and describes only severity 1 and 2 caveats and select severity 3 caveats.

There are no known open caveats for Cisco IOS Release 12.2(25)SW3.

Resolved Caveats—Cisco IOS Release 12.2(25)SW3

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(25)SW3. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCed83705

  When using cs7 ping on an IP Transfer Point (ITP) running Cisco IOS Release 12.2(20)SW on a Cisco 7507 router, alignment corrections and traceback errors may be seen occasionally. This does not seem to have any impact on operation however.

  There are no known workarounds.

- CSCee13367

  When running IP Transfer Point on Cisco IOS Release 12.2(4)MB13 or 12.2(20)SW, no report of success or failure may be seen under some circumstances.

  This condition only occurs if the Round Trip Time (RTT) between the ping endpoints is over 1 second (over satellite links for example). This condition occurs because of the time taken to set up the Q.751 traffic test. By the time the test is set up over slow links, the test is already finished and no data is sent to test.

  Workaround: Specify a test duration greater than the RTT between the test endpoint using the **cs7 ping -duration** command.

- CSCeg18352

  For the Asynchronous Transfer Mode (ATM) port adapter (PA), the LINE source of the clock fails. There is no indication or syslog event to tell the operator about it.

  This condition occurs because when the LINE fails, the ATM PA reverts back to its INTERNAL clock source. The current clock source (LINE, INTERNAL or COMMON) can not be determined from the **show** commands.

As an enhancement the **show controller ATM** command has been modified to display the current clock source.

There are no known workarounds.

- CSCeg83024

  The Standby Route/Switch Processor (RSP) of a Cisco 7500 IP Transfer Point (ITP) with the Non-Stop Operation (NSO) feature configured, is reloaded after a **cs7 as** is entered.

  This condition occurs when Cisco IOS Release 12.2(25)SW is used.

  There are no known workarounds.

- CSCeh13554

  When the IP Transfer Point (ITP) begins routing on an alternate route to a destination, it sends a preventive transfer-prohibited (TFP) to prevent circular routing. When ITP switches to using the normal route for the destination, the ITP should send a transfer-allowed (TFA) on the alternate route, to indicate that the node may now route through the ITP for that destination. But the ITP does not send this TFA in ITU networks without the national transfer-restricted (TFR) option configured.

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

- CSCeh15067

  When the IP Transfer Point (ITP) receives a message signaling unit (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 point code (PC).

  SI 0 is for Message Transfer Part, Level 3 (MTP3) Network Management messages. SI 1 is for Link Test Messages. SI 2 is used in ANSI for Link Test Messages.

  This condition occurs when ITP is configured with an XUA point code.

  There are no known workarounds.

- CSCeh16859

  Subsystem 12 on the IP Transfer Point (ITP) is reported as "not available" but not subsystem 112.

  This condition occurs if the connection between the ITP and the Signaling Control Point (SCP) is dropped.

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

- CSCsa57699

  Operation, Administration, and Maintenance (OAM) High Speed Link (HSL) Asynchronous Transfer Mode (ATM) loopback cell transmission is not working correctly. Typically, the Permanent Virtual Circuit (PVC) will display as "down" on one or both sides of the link and the IP Transfer Point (ITP) may show input errors on the ATM interface. The High Speed Link (HSL) will eventually fail due to a non responsive link test because the PVC is down and unable to pass traffic.

  This caveat occurs on Cisco 7500 ITP images using HSLs when sending and receiving OAM cells on Enhanced Asynchronous Transfer Mode (ATM) Port Adapters.

  This condition occurs on all Cisco 7500 based ITP images prior to Cisco IOS Release12.2(25)SW. 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 using the **oam-pvc** command under the interface.

  Work around: Do not use OAM cells on the High Speed Signaling links or disable the PVC state from being tied to the acknowledgment of OAM cells.

- CSCsa58560

  After several **shut/no shut**s of an E1 or T1 controller on a PA-MCX-8TE1-M port adapter (PA) containing Message Transfer Part Level 2 (MTP2) links, the MTP2 links remaining failed.

  This condition occurs when the controller is up, but the line protocol is down. An MTP2 decode show alignment fails due to a T2 timeout. A **show controller** command on the Versatile Interface Processor (VIP) shows FISU received is 0:

  ```
  router# execute slot 1 show contr ser 0/0:0 | incl FISU
  show contr ser 0/0:0 | incl FISU from slot 1:
    FISU filter on, last rcv: 0x0000000000(0), count 0
    FISU insert on, last snd: 0xFFFFC10300(4), count 1, fail 0
   shut/no shut of controller, interface, linkset, links do not resolve the problem.
  ```

  Workaround: Reload the VIP containing the affected PA, or reload the entire router.

- CSCsa59599

  After changing encapsulation types on a serial interface, the physical maximum transmission unit (MTU) of the interface resets back to the default value of 1500 bytes.

  The condition only affects IP Transfer Point (ITP) software.

  Workaround: Manually reconfigure the interface MTU.

- CSCsa64953

  The Standby Route/Switch Processor (RSP) of a Cisco IP Transfer Point (ITP) with Non-Stop Operation (NSO) enabled is reloaded after multiple **route deletion** commands are entered using the CLI in rapid succession due to a console cut-and-paste operation or a script. When this condition occurs the following message is displayed:

  ```
  %HA_CONFIG_SYNC-3-LBL_POLICY: Active and Standby lbl configuration out of sync
  ```

  This condition occurs on Cisco IOS Releases 12.2(25)SW and SW1.

  Workaround: Do not enter **route deletion** commands as part of a cut-and-paste operation with multiple commands. The **route deletion** commands should be entered individually.

- CSCsa72249

  The IP Transfer Point (ITP) incorrectly responds to an AASPUP message received by an MTP3 User Adaptation (M3UA) Application Server Processor (ASP) in a blocking state with an ASPUPAK. It should send an error message.

  This condition occurs in Cisco IOS Releases 12.2(25)SW and 12.2(25)SW1.

  There are no known workarounds. However, the ITP correctly responds to an ASPAC message on the same M3UA ASP with an error, which prevents any operational impact. (The ASP cannot become active.)

- CSCsa78896

  When a cs7 linkset is in the UNAVAIL or SHUTDOWN state, and the only route to the adjacent point code X is using that linkset (that is, this adjacent point code (APC) is inaccessible), and another destination Y becomes inaccessible, the IP Transfer Point (ITP) outputs a debug message on the console indicating a transfer-prohibited (TFP) was sent to X concerning destination Y. In reality, no TFP is actually sent to X.

  This condition occurs on Cisco IOS Release 12.2(25)SW1when **debug cs7 mtp3 mgmt packet** is enabled. Although the debug message is misleading, it does not cause any ITP functional problem.

  There are no known workarounds.

- CSCsa84521

  An IP Transfer Point (ITP) running on a Cisco 7500 router experiences high CPU utilization on Versatile Interface Processors (VIPs) with interfaces configured on a PA-MCX-8TE1-M port adapter with the Message Transfer Part Level 2 (MTP2) encapsulation set. This condition can lead to link drops during VIP online insertion and removal (OIR) or after an Route/Switch Processor (RSP) switchover.

  This condition occurs on multiple shutdown serial interfaces configured with MTP2 encapsulation and an active T1/E1 controller.

  Workaround: Remove the shutdown serial interfaces from the IOS configuration.

- CSCsa88289

  On Cisco 7500 series and Cisco 7301 series platforms running IP Transfer Point (ITP) software, when Asynchronous Transfer Mode (ATM) interfaces (PA-A3-8T1IMA, PA-A3-8E1IMA, PA-A3-OC3) are configured as a Network-to Network Interface (NNI) (**atm nni**) to be used as High Speed Signaling System 7 (SS7) links, and then the configuration (**atm nni**) is removed, the line protocol may not be restored to "up" as shown under the **show interfaces** output.

  Workaround: The reload procedure restores the Asynchronous Transfer Mode (ATM) interface to "line protocol up" for the same configuration.

- CSCsa92616

  When the IP Transfer Point (ITP) is running Cisco IOS Releases 12.2(25)SW1 and 12.2(25)SW2, the Cisco Signaling Gateway Manager Client is unable to monitor link utilization threshold status compared.

  Workaround 1: Use an earlier IOS version of the IP Transfer Point.

  Workaround 2: Within the client, right click on the link in the left hand panel of the client where it shows the SLC value and choose View->Real-time Data And Charts. This action will display the current utilization values in a panel that will update itself every 15 seconds.

- CSCsb02059

  The Hop Counter for Extended Unitdata (XUDT) messages is decremented twice when the Global Title Translation (GTT) result is an application server (AS).

  This condition occurs on a Cisco 7500 series router with Message Transfer Part, Level 3 (MTP3) offload configured, when Signaling Connection Control Part (SCCP) traffic using message type XUDT is GTT routed to an AS result.

  Workaround: Turn off MTP3 offload.

- CSCsb03447

  The Paklog debug feature is missing some message signaling units (MSUs).

  On a Cisco 7500 series router with Message Transfer Part, Level 3 (MTP3) offload configured, paklog will not log some MSUs that are locally originated on the Versatile Interface Processor (VIP).

  There are no known workarounds.

Open Caveats—Cisco IOS Release 12.2(25)SW2

This section documents possible unexpected behavior by Cisco IOS Release 12.2(25)SW2 and describes only severity 1 and 2 caveats and select severity 3 caveats.

There are no known open caveats for Cisco IOS Release 12.2(25)SW2.

Resolved Caveats—Cisco IOS Release 12.2(25)SW2

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(25)SW2. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCsa81379

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

  If your router configuration does not currently contain the **ip flow-cache feature-accelerate** command, 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) supersedes 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
```

Open Caveats—Cisco IOS Release 12.2(25)SW1

This section documents possible unexpected behavior by Cisco IOS Release 12.2(25)SW1 and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCeg83024

  The Standby Route/Switch Processor (RSP) of a Cisco 7500 IP Transfer Point (ITP) with the Non-Stop Operation (NSO) feature configured, is reloaded after a **cs7 as** command is entered.

  This condition occurs when Cisco IOS Release 12.2(25)SW is used.

  There are no known workarounds.

Resolved Caveats—Cisco IOS Release 12.2(25)SW1

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(25)SW1. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCeg01587

  Operation, Administration, and Maintenance (OAM) High Speed Link (HSL) Asynchronous Transfer Mode (ATM) loopback cell transmission is not working correctly. Typically, the Permanent Virtual Circuit (PVC) will display as “down” on one or both sides of the link and the IP Transfer Point (ITP) may show input errors on the ATM interface. The High Speed Link (HSL) will eventually fail due to a non responsive link test because the PVC is down and unable to pass traffic.

This caveat occurs on Cisco 7500 ITP images using HSLs when sending and receiving OAM cells on Enhanced Asynchronous Transfer Mode (ATM) Port Adapters.

This condition occurs on all Cisco 7500 based ITP images prior to Cisco IOS Release12.2(25)SW. 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 using the **oam-pvc** command under the interface.

Work around: Do not use OAM cells on the High Speed Signaling links or disable the PVC state from being tied to the acknowledgment of OAM cells.

- CSCeg08298

  If a link in a multilink linkset fails while it is congested, and the other links in the linkset are available and not congested, Global Title Translation (GTT) will treat destinations that use the linkset as still being congested, resulting in lost message signaling units (MSUs).

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

- CSCeg37718

  Incoming time-division multiplexing (TDM) traffic is evenly distributed among the links within the incoming TDM linkset. When the IP Transfer Point (ITP) is configured for Stream Control Transmission Protocol (SCTP) multihoming in configurations that balance 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.

  This condition occurs in Cisco IOS Release 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
```

  There are no known workarounds.

- CSCeg40188

  A Message Transfer Part Level 2 (MTP2) link does not recover when a T1 or E1 cable is disconnected and then reconnected to a IP Transfer Point (ITP). The ITP is running on a Cisco 7500 router and **cs7 offload mtp3** is configured.

  Workaround: Issue a **shutdown** command for the link followed by a **no shutdown** command to recover the link.

- CSCeg50304

  The Stream Control Transmission Protocol (SCTP) statistics for ordered and unordered chunks are reported higher than the number of chunks that were actually transmitted.

  This condition occurs in Cisco IOS Release 12.2 MB11 or higher.

  There are no known workarounds.

- CSCeg50319

  The Stream Control Transmission Protocol (SCTP) **show ip sctp association parameters** command reports the checksum type as negotiable (nego) after the association is established.

  This condition occurs in Cisco IOS Release 12.2 MB9 or higher.

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

- CSCeg72013

  Slips and errors are reported by the **show controller E1** command for interfaces supporting the Signaling System 7 (SS7) linkset.

  This condition occurs on all platforms supporting the PA-MCX-8TE1-M port adapter and running Cisco IOS Release 12.2(25)SW.

  There are no known workarounds.

- CSCsa42016

  Two issues occur with the IP Transfer Point (ITP) software only when using the Telecommunications Technology Committee (TTC) Signaling System 7 (SS7) variant.

  a. Transfer-prohibited (TFP) messages are broadcast when a link becomes available for all destinations in the Message Transfer Part, Level 3 (MTP3) routing table that are unavailable. The appropriate behavior for the Telecommunications Technology Committee (TTC) variant is not to broadcast the TFP in this circumstance.

  b. 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.

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

  There are no known workarounds.

- CSCsa42261

  A value of 0xF appears as the last nibble during instance conversion from ITU to ANSI when going from an odd to even number of digits.

  This condition occurs when performing E214 to E212 conversion between ITU and ANSI instances.

  There are no known workarounds.

- CSCsa45054

  Even though the Ethernet cable is pulled out, the state of the line protocol reports an UP state at the Route/Switch Processor (RSP) console. The actual sequence of events is that the line protocol will transition to down and the appropriate traps and console messages will be generated. When the offloaded MTP2-User Peer-to-Peer Adaptation Layer (M2PA)/Stream Control Transmission Protocol (SCTP) link fails, the line protocol on the RSP will show as “UP” but a console message will not be generated.

```
Router# show interfacce fastEthernet 0/0/0
FastEthernet0/0/0 is up, line protocol is up
```

However, the Versatile Interface Processor (VIP) console shows the correct states (UP and DOWN).

```
VIP-Slot0>show interface
 FastEthernet0/0 is up, line protocol is down
```

This condition appears to be a cosmetic issue of interface state because the Signaling System 7 (SS7) goes down correctly. However this is a critical issue from the perspective of network monitoring.

This condition occurs when an offloaded MTP2-User Peer-to-Peer Adaptation Layer (M2PA)/Stream Control Transmission Protocol (SCTP) link exists on the VIP in question, and an alternate path to the adjacent node exists and is available.

This issue occurs on Cisco 7507/7513 routers with a PA-2FE-TX port adapter and VIP6-80/VIP4-80 on Cisco IOS Releases 12.2(23)SW and 12.2(25)SW.

Workaround: The item is cosmetic on the RSP, but a trap is generated indicating the line protocol has come back up. The workaround is to issue a **shut/no shut** of the interface to correct the line protocol state on the RSP.

- CSCsa54632

  The IP Transfer Point (ITP) SCCP-User Adaptation (SUA) Signaling Gateway (SG) may leak buffers in the IP input process.

  This issue is observed when both of the following conditions occur:

  - The sending SUA Application Server Process (ASP) has sent a Connectionless Data (CLDT) message that is too large to fit into a single message signaling unit (MSU).
  - The Application Server Processor (ASP) has NOT indicated “return on error” in the SUA PROTOCOL_CLASS parameter.

  Workaround: Configure the ASPs to either not send messages that are too large to fit in a single MSU, or configure the ASPs to always indicate “return on error” within generated CLDT messages.

- CSCsa54864

  IP Transfer Points (ITPs) configured for the Telecommunications Technology Committee (TTC) variant may have difficulty bringing High Speed Links (HSLs) up due to SRTM/SRTA failures.

  This condition is only applicable for the TTC variant when the default link option “ttc-priority” is set so that the priority of the message is encoded before the routing label. This condition occurs when the attached node populates the spare bits of the priority byte.

  There are no known workarounds.

Open Caveats—Cisco IOS Release 12.2(25)SW

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

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

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.

- CSCee50294

  Cisco IOS® devices running branches of Cisco IOS version 12.2S that have Dynamic Host Configuration Protocol (DHCP) server or relay agent enabled, even if not configured, are vulnerable to a denial of service where the input queue becomes blocked when receiving specifically crafted DHCP packets. Cisco is providing free fixed software to address this issue. There are also workarounds to mitigate this vulnerability. This issue was introduced by the fix included in CSCdx46180 and is being tracked by Cisco Bug ID CSCee50294.

  This advisory is available at
  http://www.cisco.com/warp/public/707/cisco-sa-20041110-dhcp.html

- CSCef29094

  IP Transfer Point (ITP) may unexpectedly reload during a **sh cs7 gtt config** command.

  This unexpected reload occurs when a prompt is stuck at the automore state and then the Global Title Translation (GTT) database is modified. If the prompt is continued, there is a small chance of hitting a reload due to accessing freed memory.

  Workaround: Whenever the MORE prompt is seen during the display of a GTT config, type Q and re-enter the display command. Avoid executing **show** commands while bulk loading or provisioning data.

- CSCef31588

  When a summary route exists and the IP Transfer Point (ITP) receives a cluster poll message (route-set-test-cluster-prohibited (RCP) or route-set-test-cluster-restricted (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 transfer-cluster-allowed (TCA). This condition 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.

- CSCef38050

  Signaling Connection Control Part (SCCP) Calling and Called Party Addresses are truncated to 15 digits when sent to and received from an SCCP User Adaptation (SUA) application server (AS).

  For example:

```
Existing functionality-
Incoming SCCP CdPA = 12345678901234567890123456789
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 = 12345678901234567890123456789
ITP config: gta 123456789012345 pcssn 4601 pcssn
Outgoing SUA Source Address (CdPA) = 12345678901234567890123456789
```

This limitation exists in all IP Transfer Point (ITP) images supporting SUA.

There are no known workarounds. This behavior has been the base behavior on the ITP since the SUA Signaling Gateway (SG) function was released.

- CSCef69373

  If a **write mem** command is issued on an IP Transfer Point (ITP) router, a pause in the processing of data packets can occur, possibly leading to lost calls and failed links during times of otherwise high CPU utilization.

  This condition was introduced in Cisco IOS Release 12.2(23)SW.

  Workaround: Use Cisco IOS Release 12.2(21)SW, if possible.

  Alternative workaround: Avoid issuing the **write mem** or **copy running-config startup-config** commands except during a maintenance window or a period of low traffic volume.

- CSCef74580

  The CS7 monitor will stop working on High speed interfaces (Asynchronous Transfer Mode (ATM)) if IP Transfer Point (ITP) is loaded on Cisco IOS Release 12.2(23)SW1.

  This condition has been observed only on Cisco IOS Release 12.2(23)SW1.

  There are no known workarounds.

- CSCef85587

  An ASP-UP message from the MTP3 User Adaptation/SCCP User Adaptation (M3UA/SUA) Application Server Processor (ASP) is ignored until retried. Afterwards, two ASP-UP-ACK messages are returned by the IP Transfer Point (ITP).

  This condition occurs on an ITP with M3UA or SUA offloaded. ASP sends ASPUP immediately upon Steam Control Transmission Protocol (SCTP) association establishment.

  Workaround: Repeat the ASPUP message.

- CSCef95065

  During a Route or Global Title Translation (GTT) replace DB, or Route/GTT deployment using Signaling Gateway Manager (SGM), the processing time of Signaling System 7 (SS7) traffic is impacted, causing added delay.

  This condition occurs whenever the main Route Processor (RP) is responsible for both SS7 processing and GTT/Route DB management. (It does not occur during Versatile Interface Processor (VIP) forwarding.)

  Workaround: Perform GTT and route management during off peak hours.

  There are no known workarounds.

Open Caveats—Cisco IOS Release 12.2(23)SW1

This section documents possible unexpected behavior by Cisco IOS Release 12.2(23)SW1 and describes only severity 1 and 2 caveats and select severity 3 caveats.

There are no known open caveats for Cisco IOS Release 12.2(23)SW1.

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.

- CSCee36139

  When the IP Transfer Point (ITP) is configured with two source IP addresses under the local peer, only one of IP address will be used. This condition can cause trouble for the Stream Control Transmission Protocol (SCTP) link alignment when only one address is available.

  This condition occurs on 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
  ```
  There are no known workarounds.

- CSCee41388

  When configuring n Stream Control Transmission Protocol (SCTP) link on the IP Transfer Point (ITP), the INIT message is sent to only one destination address.

  This condition occurs when there are two destination addresses configured for the Stream Control Transmission Protocol (SCTP) link on the ITP, and the second address is lower than the first address. Thus, the INIT message is sent 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

  The IP Transfer Point (ITP) MAP Proxy application reports the following subsystem number (SSN) unequipped error:

  ```
  May  7 14:20:19.415 GMT: %CS7SCCP-5-UNEQUIPSS: SCCP received message for invalid or
  unequipped SSN.
  ```
  This condition occurs when an Extended Unitdata (XUDT) message is received carrying the response to the MAP Send Authentication Info message that was sent by ITP.

  Workaround: Disable sending the XUDT message type to the ITP in the Signaling System 7 (SS7) network.

- CSCee86829

  The IP Transfer Point (ITP) does not send Extended Unitdata (XUDT) messages into the Signaling System 7 (SS7) network for any non-segmented messages originated by SCCP User-Adaptation (SUA) application servers (AS).

  Workaround: There are no known workarounds for deployments requiring XUDTs and the SUA. Application Server Processors (ASPs) support sending either the hop counter or importance parameter.

- CSCee91201

  The cgspInstance table in the CISCO-ITP-GSP-MIB is always empty when the network-name is not specified. This condition can prevent network management applications like Signaling Gateway Manager (SGM) from properly discovering the device.

  This condition occurs on all platforms running Cisco IOS Release 12.2(23)SW.

  Workaround: Issue the following commands on all impacted and related devices:

  ```
  conf t
  cs7 network-name string
  ```

- CSCef08522

  The 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.

  This condition occurs when the full PC is down, the summary route used is instance 0 and in instance 0 there is a full PC route going back to instance 1. This creates a circular route within the ITP that 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, the destinations change status very rapidly (every couple of 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.

  This condition occurs because the default conversion is going from instance 1 to instance 0, and there is not a summary-routing-exception defined for instance 1.

  The condition does not occur with Cisco IOS Release 12.2(4)MB13, and does not occur in Cisco IOS Release 12.2(21)SW when a summary-routing-exception is configured in instance 1.

  Workaround: When configuring the default pc-conversion parameter, a summary- routing-exception should also be configured for the source instance.

  For example, whenever you configure:

  ```
  cs7 i x pc-conversion default y
  ```
  a summary route is entered in the instance y routing table.

  Then, a summary- routing-exception parameter should also be configured for instance y:

  ```
  cs7 i y summary-routing-exception
  ```
  This configuration ensures 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 message signaling unit (MSU) whose destination point code (DPC) does not match a full PC destination in the route table.

Open Caveats—Cisco IOS Release 12.2(23)SW

This section documents possible unexpected behavior by Cisco IOS Release 12.2(23)SW and describes only severity 1 and 2 caveats and select severity 3 caveats.

There are no known open caveats for Cisco IOS Release 12.2(23)SW.

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.

- CSCed67628

  During an initial boot of a Cisco 7301 router that has a PA-MC-8TE1+ or PA-MCX-8TE1-M port adapter in bay 0, an unexpected reload may occur.

  The condition only occurs during the initial boot of the platform and occurs regardless of whether a regular Cisco IOS software image or a boot software image is present in the bootflash file system.

  Workaround: Powercycle the Cisco 7301 router and reboot the platform.

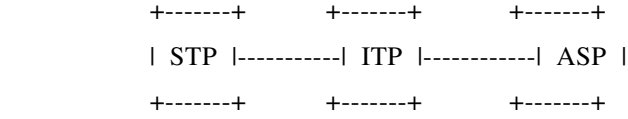
- CSCed82922

  When using the Multi-Layer Routing (MLR) feature 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 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.

- CSCee08792

  When an MTP3 User Adaptation (M3UA) application server (AS) shares the local point code (PC) 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 a Destination Restricted (DRST) message to the AS.

  Consider an M3UA AS that shares the local PC of the ITP as shown in the above figure.

  Issue 1: If the Signaling Transfer Point (STP) sends a TFR to the ITP for a concerned PC n.c.m (that is, 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 for a concerned cluster n.c.* (that is, 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. The ITP does send the DRST if the destination made a transition from Inaccessible to Restricted.

  There are no known workarounds.

- CSCee09009

  The IP Transfer Point (ITP) receives a transfer-cluster-prohibited (TCP) from the network but does not send a Destination Unavailable (DUNA) to an MTP3 User Adaptation (M3UA) application server (AS).

  This problem may occur under the following conditions:

  - The AS shares the ITP local point code.
  - The ITP has a cluster route configured that includes the local point code.
  - The concerned point code in the received TCP matches that cluster route.

  There are no known workarounds.

- CSCee11874

  Restart, link test, or link test ack messages may get dropped.

  This condition occurs only when the IP Transfer Point (ITP) initially reloads or is executing the RESTART procedure. The link test msg will be re-sent after 8 seconds and the RESTART after 12 seconds.

  There are no known workarounds.

Open Caveats—Cisco IOS Release 12.2(21)SW1

This section documents possible unexpected behavior by Cisco IOS Release 12.2(21)SW1 and describes only severity 1 and 2 caveats and select severity 3 caveats.

There are no known open caveats for Cisco IOS Release 12.2(21)SW1.

Resolved Caveats—Cisco IOS Release 12.2(21)SW1

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(21)SW1. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCed67628

  During the initial boot of a Cisco 7301 router with a PA-MC-8TE1+ or PA-MCX-8TE1-M port adapter in bay 0, an unexpected reload may occur. This reload occurs most prevalently when a full-featured IOS image is in bootflash, rather than a boot image.

  The condition occurs only during initial boot of the platform.

  Workaround: Powercycle the Cisco 7301 router and reboot the platform.

- CSCed82922

  When using the Multi-Layer Routing (MLR) feature 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: Use global title based routing prior to the ITP MLR routing

  Alternative Workaround: Have the originator use a global title address specified in the request's calling party address field.

Open Caveats—Cisco IOS Release 12.2(21)SW

This section documents possible unexpected behavior by Cisco IOS Release 12.2(21)SW and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCed08031

  If online insertion and removal (OIR) is performed on a Cisco 7500 router configured with an RSP16 running Cisco IOS Release 12.2(4)MB13, linksets may bounce and calls may be lost.

  There are no known workarounds.

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.

- 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

  Traffic coming from an M3UA Application Server Processor (ASP) is not handled properly.

  This condition occurs on IP Transfer Points (ITPs) configured for the Telecommunications Technology Committee (TTC) variant.

  There are no known workarounds.

Open Caveats—Cisco IOS Release 12.2(20)SW

This section documents possible unexpected behavior by Cisco IOS Release 12.2(20)SW and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCed08031

  If online insertion and removal is performed on a Cisco 7500 router configured with an RSP16 running Cisco IOS Release 12.2(4)MB13, linksets may bounce and calls may be lost.

  There are no known workarounds.

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.

- CSCec61182

  A Cisco RSP8, running Cisco IOS Release 12.2(4)MB12, reports 100% CPU usage in the Virtual Exec process, after typing the **privilege configure level 7 cs7** command in a telnet session.

  There are no known workarounds.

- CSCec62567

  Sent link utilization is incorrect in certain configurations. The cgspLinkL2BytesSent(CISCO-ITP-GSP-MIB.my) and cItpSpLinkL2BytesSent (CISCO-ITP-SP-MIB.my) objects may provide incorrect values in these situations.This condition can result in incorrect information for [send erlang values] in Signaling Gateway Manager (SGM).

  This condition occurs with routers running Cisco IOS Release 12.2(4)MB10-MB13, 12.2(18)SW, or 12.2(19)SW.

  There are no known workarounds.

- CSCec69259

  After a reboot of the event table in the CISCO-ITP-GSP2.my MIB, entering a **getmany** command can produce traceback.

  This condition occurs when the Simple Network Management Protocol (SNMP) is configured without cs7 configured, and when running the following IP Transfer Point (ITP) images: Cisco IOS Release 12.2(4)MB6, Cisco IOS Release 12.2(4)MB13,Cisco IOS Release 12.2(18)SW, or Cisco IOS Release 12.2(19)SW.

  There are no known workarounds.

- CSCec79617

  The **sh cs7 gtt map stat** command shows Global Title Translation (GTT) maps stuck in a congested state and the Signaling Connection Control Part (SCCP) does not choose alternates of congested point-codes.

  This condition occurs when summary or cluster routes are used and GTT is translated to point-codes for which a full route does not exist.

  Workaround: Ensure there is a full route to the destination for all point-codes that GTT translates.

- CSCed01515

  IP Transfer Point (ITP) does not remove Message Transfer Part, Level 3 (MTP3) routes from the Versatile Interface Processor (VIP) using the CLI when MTP3 offload is configured. This condition results in indeterministic traffic routing when an attempt to delete Signaling System 7 (SS7) routes occurs.

  Workaround: Do not enable MTP3 offload for affected versions of the ITP software.

- CSCed20020

  IP Transfer Point (ITP) sends Global Title Translation (GTT) traffic to an unavailable subsystem.

  This condition occurs when using GTT application groups under the following scenario:

  - Item(s) in group are point codes (PCs) without subsystem numbers (SSNs)
  - RI=PCSSN
  - The message signaling unit's (MSU's) Signaling Connection Control Part (SCCP) Called Party (CDPA) contains SSN=X
  - PC/SSN=X exists in GTT map table and SSN is prohibited

  Workaround: Specify an explicit SSN in the application group entry, such as HLR, MSC, VLR.

Open Caveats—Cisco IOS Release 12.2(19)SW

This section documents possible unexpected behavior by Cisco IOS Release 12.2(19)SW and describes only severity 1 and 2 caveats and select severity 3 caveats.

There are no known open caveats for Cisco IOS Release 12.2(19)SW.

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.

- CSCec44189

  Nodes receiving subsystem status from the IP Transfer Point (ITP) may ignore the status because the ITP sources the SCCP Management (SCMG) messages from the primary local point code only.

  Workaround: Have nodes either expect all SCMG messages from the primary ITP point code, or disable the sending preliminary subsystem status test (SST) messages to the ITP destined for a point code (PC) other than the primary local PC.

- CSCec45088

  A rapid memory leak occurs on a Versatile Interface Processor (VIP).

  This condition occurs when Message Transfer Part, Level 3 (MTP3) offload is configured and traffic has to be entered and forwarded on the same VIP on an High Speed Link (HSL) IMA port adapter (PA).

  Workaround: Disable the MTP3 offload feature, or avoid traffic entering and exiting the same VIP.

Open Caveats—Cisco IOS Release 12.2(18)SW

This section documents possible unexpected behavior by Cisco IOS Release 12.2(18)SW and describes only severity 1 and 2 caveats and select severity 3 caveats.

There are no known open caveats for Cisco IOS Release 12.2(18)SW.

Resolved Caveats—Cisco IOS Release 12.2(18)SW

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(18)SW. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdu53656

  A Cisco device running IOS and enabled for the Border Gateway Protocol (BGP) is vulnerable to a Denial of Service (DOS) attack from a malformed BGP packet. The BGP protocol is not enabled by default, and must be configured in order to accept traffic from an explicitly defined peer. Unless the malicious traffic appears to be sourced from a configured, trusted peer, it would be difficult to inject a malformed packet. BGP MD5 is a valid workaround for this problem.

  Cisco has made free software available to address this problem. For more details, please refer to this advisory, available at http://www.cisco.com/warp/public/707/cisco-sa-20040616-bgp.shtml.

- CSCdz71127

  Cisco routers and switches running Cisco IOS software and configured to process Internet Protocol version 4 (IPv4) packets are vulnerable to a Denial of Service (DoS) attack. A rare sequence of crafted IPv4 packets sent directly to the device may cause the input interface to stop processing traffic once the input queue is full. No authentication is required to process the inbound packet. Processing of IPv4 packets is enabled by default. Devices running only IP version 6 (IPv6) are not affected. A workaround is available.

  Cisco has made software available, free of charge, to correct the problem.

  This advisory is available at

  http://www.cisco.com/warp/public/707/cisco-sa-20030717-blocked.shtml

- CSCea02355

  Cisco routers and switches running Cisco IOS software and configured to process Internet Protocol version 4 (IPv4) packets are vulnerable to a Denial of Service (DoS) attack. A rare sequence of crafted IPv4 packets sent directly to the device may cause the input interface to stop processing traffic once the input queue is full. No authentication is required to process the inbound packet. Processing of IPv4 packets is enabled by default. Devices running only IP version 6 (IPv6) are not affected. A workaround is available.

  Cisco has made software available, free of charge, to correct the problem.

  This advisory is available at

  http://www.cisco.com/warp/public/707/cisco-sa-20030717-blocked.shtml

- CSCea28131

  A Cisco device running IOS and enabled for the Border Gateway Protocol (BGP) is vulnerable to a Denial of Service (DOS) attack from a malformed BGP packet. The BGP protocol is not enabled by default, and must be configured in order to accept traffic from an explicitly defined peer. Unless the malicious traffic appears to be sourced from a configured, trusted peer, it would be difficult to inject a malformed packet. BGP MD5 is a valid workaround for this problem.

  Cisco has made free software available to address this problem. For more details, please refer to this advisory, available at http://www.cisco.com/warp/public/707/cisco-sa-20040616-bgp.shtml.

Related Documentation

The following sections describe the documentation available for the Cisco 7000 family. These documents consist of hardware and software installation guides, Cisco IOS configuration guides 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 and the Documentation CD-ROM.

Use these release notes with these documents:

- Release-Specific Documents, page 72
- Platform-Specific Documents, page 73
- Feature Modules, page 73
- Cisco IOS Software Documentation Set, page 73

Release-Specific Documents

The following documents are specific to Cisco IOS Release 12.2 and are located on Cisco.com and the Documentation CD-ROM:

- *Cross-Platform Release Notes for Cisco IOS Release 12.2*

  On Cisco.com at:

  Technical Documents: **Cisco IOS Software Configuration**: **Cisco IOS Release 12.2: Release Notes: Cross-Platform Release Notes**

  On the Documentation CD-ROM at:

  Cisco Product Documentation: Cisco IOS Software Configuration: **Cisco IOS Release 12.2: Release Notes**: **Cross-Platform Release Notes**

- Product bulletins, field notices, and other release-specific documents on Cisco.com at:

  Technical Documents

- *Caveats for Cisco IOS Release 12.2*

  As a supplement to the caveats listed in "Caveats for Cisco IOS Release 12.2 SW" in these release notes, see *Caveats for Cisco IOS Release 12.2* which contains caveats applicable to all platforms for all maintenance releases of Cisco IOS Release 12.2.

  On Cisco.com at:

  Technical Documents: **Cisco IOS Software Configuration**: **Cisco IOS Release 12.2**: **Release Notes**: **Caveats**

On the Documentation CD-ROM at:

Cisco Product Documentation: Cisco IOS Software Configuration: **Cisco IOS Release 12.2**: **Caveats**

Note If you have an account with Cisco.com, you can also use the Bug Toolkit to find select caveats of any severity. To reach the Bug Toolkit, l**og 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.

Platform-Specific Documents

These documents are available for the Cisco 7000 family of routers on Cisco.com and the Documentation CD-ROM:

- *Cisco 7000 User Guide*
- *Cisco 7000 Hardware Installation and Maintenance*

  On Cisco.com at:

  Technical Documents: **Documentation Home Page**: **Core/High-End Routers**

  On the Documentation CD-ROM at:

  Cisco Product Documentation: **Core/High-End Routers**

Feature Modules

Feature modules describe new features supported by Cisco IOS Release 12.2(25)SW 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. Feature module information is incorporated in the next printing of the Cisco IOS documentation set.

On Cisco.com at:

Technical Documents: Cisco IOS Software Configuration: **Cisco IOS Release 12.2**: **New Feature Documentation**

On the Documentation CD-ROM at:

Cisco Product Documentation: Cisco IOS Software Configuration: **Cisco IOS Release 12.2**: **New Feature Documentation**

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. The Cisco IOS software documentation set is shipped with your order in electronic form on the Documentation CD-ROM—unless you specifically ordered the printed versions.

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.

On Cisco.com at:

Technical Documents: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 12.2: Configuration Guides and Command References

On the Documentation CD-ROM at:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.2: Configuration Guides and Command References

Cisco IOS Release 12.2 Documentation Set Contents

Table 21 lists the contents of the Cisco IOS Release 12.2 software documentation set, which is available in electronic form and in printed form if ordered.

Note You can find the most current Cisco IOS documentation on Cisco.com and the Documentation CD-ROM.

On Cisco.com at:

Technical Documents: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 12.2

On the Documentation CD-ROM at:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.2

Table 21 Cisco IOS Release 12.2 Documentation Set

Books	Major Topics
• *Cisco IOS Configuration Fundamentals Configuration Guide* • *Cisco IOS Configuration Fundamentals Command Reference*	Cisco IOS User Interfaces File Management System Management
• *Cisco IOS Interface Configuration Guide* • *Cisco IOS Interface Command Reference*	LAN Interfaces Serial Interfaces Logical Interfaces

Table 21 Cisco IOS Release 12.2 Documentation Set (continued)

Books	Major Topics
• *Cisco IOS IP Configuration Guide* • *Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services* • *Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols* • *Cisco IOS IP Command Reference, Volume 3 of 3: Multicast*	IP Addressing IP Services IP Routing Protocols IP Multicast
• *Cisco IOS Voice, Video, and Fax Configuration Guide* • *Cisco IOS Voice, Video, and Fax Command Reference*	Voice over IP Call Control Signaling Voice over Frame Relay Voice over ATM Telephony Applications Trunk Management Fax, Video, and Modem Support
• *Cisco IOS Quality of Service Solutions Configuration Guide* • *Cisco IOS Quality of Service Solutions Command Reference*	Packet Classification Congestion Management Congestion Avoidance Policing and Shaping Signaling Link Efficiency Mechanisms
• *Cisco IOS Security Configuration Guide* • *Cisco IOS Security Command Reference*	AAA Security Services Security Server Protocols Traffic Filtering and Firewalls IP Security and Encryption Passwords and Privileges Neighbor Router Authentication IP Security Options Supported AV Pairs
• *Cisco IOS Switching Services Configuration Guide* • *Cisco IOS Switching Services Command Reference*	Cisco IOS Switching Paths NetFlow Switching Multiprotocol Label Switching Multilayer Switching Multicast Distributed Switching Virtual LANs LAN Emulation

Table 21 Cisco IOS Release 12.2 Documentation Set (continued)

Books	Major Topics
• *Cisco IOS Wide-Area Networking Configuration Guide* • *Cisco IOS Wide-Area Networking Command Reference*	ATM Frame Relay SMDS X.25 and LAPB
• *Cisco IOS Configuration Guide Master Index* • *Cisco IOS Command Reference Master Index* • *Cisco IOS Debug Command Reference* • *Cisco IOS Software System Error Messages* • *New Features in 12.2-Based Limited Lifetime Releases* • New Features in Release 12.2 T • Release Notes (Release note and caveat documentation for 12.2-based releases and various platforms)	

Obtaining Documentation

The following sections explain how to obtain documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at the following URL:

http://www.cisco.com

Translated documentation is available at the following URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which is shipped with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual subscription.

Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/cgi-bin/order/order_root.pl

- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:

  http://www.cisco.com/go/subscription

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

If you are reading Cisco product documentation on Cisco.com, you can submit technical comments electronically. Click **Leave Feedback** at the bottom of the Cisco Documentation home page. After you complete the form, print it out and fax it to Cisco at 408 527-0730.

You can e-mail your comments to bug-doc@cisco.com.

To submit your comments by mail, use the response card behind the front cover of your document, or write to the following address:

Cisco Systems
Attn: Document Resource Connection
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

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

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com is a highly integrated Internet application and a powerful, easy-to-use tool that provides a broad range of features and services to help you to

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

You can self-register on Cisco.com to obtain customized information and service. To access Cisco.com, go to the following URL:

http://www.cisco.com

Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two types of support are available through the Cisco TAC: the Cisco TAC Web Site and the Cisco TAC Escalation Center.

Inquiries to Cisco TAC are categorized according to the urgency of the issue:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

Which Cisco TAC resource you choose is based on the priority of the problem and the conditions of service contracts, when applicable.

Cisco TAC Web Site

The Cisco TAC Web Site allows you to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC Web Site, go to the following URL:

http://www.cisco.com/tac

All customers, partners, and resellers who have a valid Cisco services contract have complete access to the technical support resources on the Cisco TAC Web Site. The Cisco TAC Web Site requires a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to the following URL to register:

http://www.cisco.com/register/

If you cannot resolve your technical issues by using the Cisco TAC Web Site, and you are a Cisco.com registered user, you can open a case online by using the TAC Case Open tool at the following URL:

http://www.cisco.com/tac/caseopen

If you have Internet access, it is recommended that you open P3 and P4 cases through the Cisco TAC Web Site.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses issues that are classified as priority level 1 or priority level 2; these classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer will automatically open a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to the following URL:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled; for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). In addition, please have available your service agreement number and your product serial number.

This document is to be used in conjunction with the documents listed in the "Related Documentation" section on page 72.