Release Notes for Cisco 2650 and Cisco 2651 Routers for Cisco IOS Release 12.2(4)MB13c

November 2, 2005

Cisco IOS Release 12.2(4)MB13c

OL-1865-01 Rev. N2

These release notes for Cisco 2650, Cisco 2651, Cisco 2650XM, and Cisco 2651XM series routers describe the enhancements provided in Cisco IOS Release 12.2(4)MB13c. These release notes are updated as needed.

For a list of the software caveats that apply to Cisco IOS Release 12.2(4)MB13c, see the "Caveats for Cisco IOS Release 12.2 MB" section on page 12 and *Caveats for Cisco IOS Release 12.2*. The caveats document is updated for every maintenance release and is located on Cisco.com and the Documentation CD-ROM.

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

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

Contents

These release notes describe the following topics:

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

Introduction

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

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

System Requirements

This section describes the system requirements for Cisco IOS Release 12.2(4)MB13c:

Memory Recommendations

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

Feature Set	Software Image	Recommended Flash Memory	Recommended DRAM Memory	Runs From
IP Transfer Point (M3UA/SUA)	c2600-itp-mz	32 MB	128 MB	RAM
IP Transfer Point	c2600-itp-mz	32 MB	128 MB	RAM
ITP Map Gateway Base	c2600-itp-mz	32 MB	128 MB	RAM

Supported Hardware

Cisco IOS Release 12.2(4)MB13c supports the following Cisco 2600 series modular access routers:

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

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

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

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

Table 2 Supported Interfaces for Cisco 2600 Series Routers

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

Determining the Software Version

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

```
Router> show version

Cisco Internetwork Operating System Software
IOS (tm) 2600 Software (c2600-itp-mz), Version 12.2(4)MB13c, RELEASE SOFTWARE
```

Upgrading to a New Software Release

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

http://www.cisco.com/en/US/products/hw/routers/ps259/products_tech_note09186a00801fc986.shtml

Feature Set Tables

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

Cisco IOS Release 12.2(4)MB13c supports the feature set found in the Cisco IOS Release 12.2(4)T IP image.

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

Table 3 lists the features and feature sets supported by the Cisco 2600 series in Cisco IOS Release 12.2(4)MB13c and uses the following conventions:

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

Note These release notes list only features that are new to Cisco IOS Release 12.2(4)MB13c. The parent release for Cisco IOS Release 12.2(4)MB13c is Cisco IOS Release 12.2(4) T. For information about inherited features, refer to Cisco.com or Cisco Feature Navigator. For Cisco.com, go to http://www.cisco.com/univercd/home/index.htm, select the appropriate software release under **Cisco IOS Software**, and click **Release Notes**. If you have a Cisco.com login account, you can use the Cisco Feature Navigator tool at http://www.cisco.com/cgi-bin/Support/FeatureNav/FN.pl.

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

Features	Software Images by Feature Sets	
	In	IP Transfer Point (ITP)
ITP Instance Translation	(4)MB10	Yes
ITP M3UA/SUA Signaling Gateway	(4)MB5	Yes
ITP Multi-Layer Routing	(4)MB10	Yes
ITP Multiple Instances	(4)MB10	Yes
ITP SCCP/GTT	(4)MB1	Yes
ITP SS7 Offload	(1)MB1	Yes
SCCP Load Balancing Enhancements	(4)MB2	Yes

New and Changed Information

The following sections list the new hardware and software features supported by the Cisco 2600 series for Cisco IOS Release 12.2(4)MB13c.

New Hardware and Software Features in Cisco IOS Release 12.2(4)MB12 and Cisco IOS Release 12.2(4)MB13

No new hardware or software features are supported by the Cisco 2600 series routers for Cisco IOS Release 12.2(4)MB12 and Cisco IOS Release 12.2(4)MB13.

New Hardware Features in Cisco IOS Release 12.2(4) MB11

No new hardware features are supported in Cisco IOS Release 12.2(4) MB11.

New Software Features in Cisco IOS Release 12.2(4) MB11

ITP Packet Logging Facility

Cisco IOS Release 12.2(4)MB11 supports the ITP Packet Logging facility uses the Berkeley Standard Distribution (BSD) Syslog protocol (RFC 3164) to send selected Message Signal Units (MSUs) to a user-selected monitoring tool via the UDP connectionless protocol (RFC 768). You must select and install a monitoring tool to receive and decode messages that are sent by the ITP Packet Logging facility. We do not provide this monitoring tool.

New Hardware Features in Cisco IOS Release 12.2(4) MB10

No new hardware features are supported in Cisco IOS Release 12.2(4) MB10.

New Software Features in Cisco IOS Release 12.2(4) MB10

Multi-Layer Short Message Service Routing Feature

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

Multiple Instances Feature

The Multiple Instance feature enables multiple variant and network indicator combinations to run concurrently on one ITP. You can configure up to 8 instances.

Instance Translation Feature

The Instance Translation feature enables the conversion of packets between instances on the 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. Multiple Instance support is required if you configure the Instance Translation feature.

New Hardware Features from Cisco IOS Release 12.2(4) MB6 to Cisco IOS Release 12.2(4) MB9a

No new hardware features are supported from Cisco IOS Release 12.2(4) MB6 to Cisco IOS Release 12.2(4) MB9a.

New Software Features from Cisco IOS Release 12.2(4) MB6 to Cisco IOS Release 12.2(4) MB9a

No new software features are supported from Cisco IOS Release 12.2(4) MB6 to Cisco IOS Release 12.2(4) MB9a, except for the following new feature introduced in Cisco IOS Release 12.2(4)MB7.

Cisco IOS Release 12.2(4)MB7

Cisco IOS Release 12.2(4)MB7 adds the following capabilities to the IP Transfer Point (ITP) product: support for Set Initialization Mode (SIM) Authentication/Authorization for Cisco WLAN Solution Architecture for laboratory and demonstration purposes. This feature is not licensed on the Cisco 2600 series platform for production environments.

New Hardware Features in Cisco IOS Release 12.2(4) MB5

No new hardware features are supported in Cisco IOS Release 12.2(4) MB5.

New Software Features in Cisco IOS Release 12.2(4) MB5

ITP M3UA/SUA Signaling Gateway

Based on open industry standards, the Cisco IP Transfer Point (ITP) product is designed for transporting Signaling System 7 (SS7) traffic over IP (SS7oIP) networks. The ITP product's design provides significant cost efficiencies and scalability enhancements over legacy SS7 networks. Using the Internet Engineering Task Force (IETF) 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 (HSL) was added.

MTP3 User Adaptation (M3UA) and Signaling Connection Control Protocol (SCCP) User Adaptation (SUA) Signaling Gateway:

- Uses the ITP M3UA and SUA protocols.
- Adds signaling gateway functionality between legacy SS7 network and IP-enabled signaling endpoints (SEP) nodes.
- Introduces an additional switch option (China) for the **CS7 Variant** command.

Refer to *New Features in Release 12.2(4)MB5* for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122mb/1224mb5/index.htm

New Hardware Features in Cisco IOS Release 12.2(4) MB4

No new hardware features are supported in Cisco IOS Release 12.2(4) MB4.

New Software Features in Cisco IOS Release 12.2(4) MB4

MIB and Command Enhancements

The IP Transfer Point feature has been updated to include MIB and command changes. Refer to the document at the following location for information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122mb/1224mb4/index.htm

New Hardware and Software Features in Cisco IOS Release 12.2(4) MB3

No new hardware or software features are supported in Cisco IOS Release 12.2(4) MB3.

New Hardware Features in Cisco IOS Release 12.2(4) MB2

No new hardware features are supported in Cisco IOS Release 12.2(4) MB2.

New Software Features in Cisco IOS Release 12.2(4) MB2

The following new software enhancements have been made to the IP Transfer Point feature introduced in Cisco IOS Release 12.2(4) MB1:

- SS7 over ATM High-Speed Link (HSL) support

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

- SCCP enhancements that provide more granular control of SCCP load balancing than previous releases did.

  The SCCP Load Balancing enhancements include GTT address conversion, enhanced SCCP cost routing, and SCCP SLS loadsharing for Class 1 traffic.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122mb/122mb2/index.htm

New Hardware Features in Cisco IOS Release 12.2(4) MB1

No new hardware features are supported in Cisco IOS Release 12.2(4) MB1.

New Software Features in Cisco IOS Release 12.2(4) MB1

The following new features are supported in Cisco IOS Release 12.2(4) MB1:

GTT and SCCP Support

The following new software enhancements have been made to the IP Transfer Point (ITP) feature introduced in Cisco IOS Release 12.2(1) MB1:

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

- Enhanced QoS for 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 linksets. 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

New Hardware Features in Cisco IOS Release 12.2(1) MB1

No new hardware features are supported in Cisco IOS Release 12.2(1) MB1.

New Software Features in Cisco IOS Release 12.2(1) MB1

The following new feature is supported in Cisco IOS Release 12.2(1) MB1:

IP Transfer Point

Cisco IP Transfer Point (ITP) is an SS7oIP software solution. ITP provides a highly reliable, cost-effective medium for migrating Signaling System 7 (SS7) and the telecommunications network signaling technology to the mobile wireless industry IP environment.

Cisco has leveraged its leadership role in the high-end switch and router industry and has created a carrier class router with a transparent SS7oIP convergence solution. The result is a seamless solution that is managed identically to other Cisco devices in large wide-area networks and leverages existing Cisco skill sets within the service provider's organization. In many cases, the provisioning, management, and tools training are already in place.

Refer to *IP Transfer Point (ITP)* for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122mb/122mb1/itp.htm

MIBs

Current MIBs

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

http://tools.cisco.com/ITDIT/MIBS/servlet/index

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

To access Cisco MIB Locator, 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

Deprecated and Replacement MIBs

Old Cisco MIBs will be replaced in a future release. Currently, OLD-CISCO-* MIBs are being converted into more scalable MIBs without affecting existing Cisco IOS products or network management system (NMS) applications. You can update from deprecated MIBs to the replacement MIBs as shown in Table 4.

Table 4 Deprecated and Replacement MIBs

Deprecated MIB	Replacement
OLD-CISCO-APPLETALK-MIB	RFC1243-MIB
OLD-CISCO-CHASSIS-MIB	ENTITY-MIB
OLD-CISCO-CPUK-MIB	To be determined
OLD-CISCO-DECNET-MIB	To be determined
OLD-CISCO-ENV-MIB	CISCO-ENVMON-MIB
OLD-CISCO-FLASH-MIB	CISCO-FLASH-MIB
OLD-CISCO-INTERFACES-MIB	IF-MIB CISCO-QUEUE-MIB
OLD-CISCO-IP-MIB	To be determined
OLD-CISCO-MEMORY-MIB	CISCO-MEMORY-POOL-MIB
OLD-CISCO-NOVELL-MIB	NOVELL-IPX-MIB
OLD-CISCO-SYS-MIB	(Compilation of other OLD* MIBs)
OLD-CISCO-SYSTEM-MIB	CISCO-CONFIG-COPY-MIB
OLD-CISCO-TCP-MIB	CISCO-TCP-MIB
OLD-CISCO-TS-MIB	To be determined
OLD-CISCO-VINES-MIB	CISCO-VINES-MIB
OLD-CISCO-XNS-MIB	To be determined

Important Notes

The following information applies to Cisco IOS Release 12.2(4)MB13c.

Field Notices and Bulletins

For general information about the types of documents listed in this section, refer to the following document:

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

- Field Notices—Cisco recommends that you view the field notices for this release to see if your software or hardware platforms are affected. If you have an account on Cisco.com, you can find field notices at http://www.cisco.com/warp/customer/tech_tips/index/fn.html. If you do not have a Cisco.com login account, you can find field notices at http://www.cisco.com/warp/public/tech_tips/index/fn.html.
- Product Bulletins—If you have an account on Cisco.com, you can find product bulletins at http://www.cisco.com/warp/customer/cc/general/bulletin/index.shtml. If you do not have a Cisco.com login account, you can find product bulletins at http://www.cisco.com/warp/public/cc/general/bulletin/iosw/index.shtml.

- *What's Hot for IOS Releases: Cisco IOS 12.2—What's Hot for IOS Releases: Cisco IOS 12.2* provides information about caveats that are related to deferred software images for Cisco IOS Release 12.2. If you have an account with Cisco.com, you can access *What's Hot for IOS Releases: Cisco IOS 12.2* at http://www.cisco.com/kobayashi/sw-center/sw-ios.shtml or by logging in and selecting **Software Center**: **Cisco IOS Software**: **What's Hot for IOS Releases**: **Cisco IOS 12.2**.
- *What's New for IOS — What's New for IOS* lists recently posted Cisco IOS software releases and software releases that have been removed from Cisco.com. If you have an account with Cisco.com you can access *What's New for IOS* at http://www.cisco.com/kobayashi/sw-center/sw-ios.shtml or by logging in and selecting **Software Center: Cisco IOS Software**.

Modification of cs7 local-peer Command for Cisco 2600 Series Routers

The **cs7 local-peer** command is modified in Cisco IOS Release 12.2(4)MB8 for the range of valid port numbers. The previous range was 4096 to 32761. The new range is 1024 to 49151. Refer to the documents at the following URL for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122mb/1224mb8/index.htm

Addition of squeeze Command for Cisco 2600 Series Routers

The **squeeze** command, which is used to erase all files marked for deletion on a Flash file system, is now available on Cisco 2600 series routers.

Caveats for Cisco IOS Release 12.2 MB

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

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

All caveats in Cisco IOS Release 12.2 and Cisco IOS Release 12.2 T are also in Cisco IOS Release 12.2(4)MB13c.

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

For information on caveats in Cisco IOS Release 12.2 T, see *Caveats for Cisco IOS Release 12.2 T*, which lists severity 1 and 2 caveats and select severity 3 caveats and is located on Cisco.com and the Documentation CD-ROM.

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 & Support: Software Center: Cisco IOS Software: BUG TOOLKIT**. Another option is to go to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl.

Open Caveats—Cisco IOS Release 12.2(4) MB13c

There are no open caveats specific to Cisco IOS Release 12.2(4) MB13c that require documentation in the release notes.

Resolved Caveats—Cisco IOS Release 12.2(4) MB13c

- 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

- CSCei76358: cleanup of user interface data

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

Open Caveats—Cisco IOS Release 12.2(4) MB13b

There are no open caveats specific to Cisco IOS Release 12.2(4) MB13b that require documentation in the release notes.

Resolved Caveats—Cisco IOS Release 12.2(4) MB13b

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(4) MB13b. 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.

Caveat Advisory - Resolved Caveats Cisco IOS Release 12.2(4)MB13

- CSCsa81379: Deprecate NetFlow Feature Acceleration

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

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

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

Cisco Express Forwarding (CEF) 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(4) MB13

There are no open caveats specific to Cisco IOS Release 12.2(4) MB13 that require documentation in the release notes.

Resolved Caveats—Cisco IOS Release 12.2(4) MB13

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(4) MB13. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCeb54609 - ITP: Segmentation field lost during XUDT-->CLDT conversion

  Symptom: When the ITP SUA Signaling Gateway is converting an extended unitdata (XUDT) with segmentation information to the connectionless data transfer (CLDT) message, the gateway does not convert the segmentation information present in the XUDT message to the corresponding SUA field in the CLDT message.

  Condition: This defect only occurs when the ITP is configured for the ANSI variant.

  Workaround: There is no workaround.

- CSCeb57599- ITP: router crash during GTT to app-grp with congested member

  Symptom: The router (or Versatile Interface Processor (VIP) if MTP3 offload is configured) crashes during global title translation (GTT) processing.

  Condition: The crash only happens when GTT is performed and the result is a GTT application group containing at least 1 member (PC or PC/SSN) in the congested state.

  Workaround: Use GTT without using an Application-Group or use GTT with traffic rates that ensure no members get congested.

- CSCeb58198- ITP-R4:unexpected parsing error sctp dest addr change

  Symptom: Incorrectly formatted cSctpExtDestAddressStateChange notification occurs when SCTP association is offloaded to Versatile Interface Processor (VIP).

  Conditions: This problem occurs on a Cisco 2600 or 7500 series router that is running Cisco IOS 12.2(4)MB12.

  Workaround: Do not offload Signaling System 7 (SS7) links or disable notification.

  Further Problem Description: Use the following commands to configure the SS7 link that is running on VIP and enable the destination address notification.

```
cs7 local-peer 5002 offload 3
 local-ip 172.18.16.26
 local-ip 172.18.16.250
!
cs7 linkset to-STP 1.1.1
 link 0 sctp 172.18.16.27 5002 5002
!
snmp-server enable traps sctp dest-address
```

- CSCeb84186- Commit security changes to 12.2MB

  This DDTS integrates the security resolutions of caveats CSCdz71127 and CSCea02355 into the ITP software.

Open Caveats—Cisco IOS Release 12.2(4) MB12

There are no open caveats specific to Cisco IOS Release 12.2(4) MB12 that require documentation in the release notes.

Resolved Caveats—Cisco IOS Release 12.2(4) MB12

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(4) MB12. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdz71127 - corrupted packet can cause input queue wedge - reg to CSCdx02283

  Cisco routers and switches that are 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 that are 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 - rare ip packets may cause input queue wedge

  Cisco routers and switches that are 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 that are 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

- CSCeb15156 - ITP: Bus error after SCTP association termination

  Symptom: Traceback or system failure with mgd_timer_start in the traceback after termination of a locally multihomed SCTP association.

  Conditions: Occurs on Cisco 2600 or Cisco 7500 series routers that are running Cisco IOS Release 12.2(4)MB10 or Cisco IOS 12.2(4)MB11. Termination of a locally multihomed SCTP association with at least one other active association may trigger this system failure.

  Workaround: Disable local multihoming by configuring only a single IP address for local SCTP endpoints.

- CSCeb23816 - ITP: Memory leak on link test failure

  Symptom: Memory leak when cs7 link is mis-configured to incorrect variant or adjacent signalling point.

  Conditions: Occurs on Cisco 2600 or Cisco 7500 series routers that are running Cisco IOS 12.2(4)MB10 or Cisco IOS 12.2(4)MB11 release of the ITP product.

  Workaround: Correctly configure links.

- CSCeb39832 - ITP switch-over while viewing mtp3 route table

  Symptom: A Cisco ITP may switch over to the secondary processor if an x-listed route is removed while an operator views the route table using the **show cs7 route** command.

  Workaround: Do not page through the route table. Setting the terminal length to zero prevents this.

- CSCeb42215 - ITP: Processor memory corruption crash

  Symptom: System failure with block overrun of the redzone using SCTP bundling over IP interfaces that have a MTU size greater than 1500 bytes.

  Conditions: Occurs on Cisco 2600 or Cisco 7500 series routers that are running Cisco IOS 12.2(4)MB4-MB11. The IP interfaces with MTU sizes greater than 1500 bytes allows SCTP to bundle more than 1500 bytes into a 1500 byte buffer. Bundling more than 1500 bytes causes a memory overwrite of adjacent memory blocks, which then causes this system failure.

  Workaround: On IP interfaces with MTU sizes that are greater than 1500 bytes, reduce the MTU sizes to 1500 bytes.

- CSCeb46313 - ITP system failure when configuring removed port adapter

  Symptom: ITP system failure when configuring a port adapter that is removed from the system or is not properly seated after OIR.

  Workaround: Make sure that the port adapter is correctly seated within the Versatile Interface Processor (VIP). Do not attempt to configure hardware that is removed.

Open Caveats—Cisco IOS Release 12.2(4) MB11

No open caveats specific to Cisco IOS Release 12.2(4) MB11 require documentation in the release notes.

Resolved Caveats—Cisco IOS Release 12.2(4) MB11

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(4) MB11. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCea59369 - ITP R4: GTT MAP entries with summary routes don't come up

  Symptom: Global title translation (GTT) MAP entries have the PC in the unavail state even though the MTP3 route table has summary routes that match the MAP entry in the avail state.

  Conditions: The situation would occur whenever summary routes are used in conjunction with GTT MAP entries that match those summary routes.

  Workaround: Ensure that for each GTT entry a non summary route exists.

- CSCea65446 - ITP-R4 MB10: set plan-capacity-send only - sh link util causes crash

  Symptom: System failure can occur when link planning capacity is incorrectly configured.

  Conditions: On Cisco 7500 series routers that are running Cisco IOS Release 12.2(4)MB10, the following conditions produce the problem:

  – No global defaults are configured for plan capacity.
  – Receive planning capacity is specified on a link, but send planning capacity is not specified on any other link in the linkset.
  – Send planning capacity is specified on a link, but receive planning capacity is not specified on any other link in the linkset.
  – The **show cs7 linkset utilization** command is issued.

  The following is an example of an incorrect configuration:

```
conf t
cs7 instance 0 linkset to-STP1
    link 0 sctp 10.2.3.4 10.4.5.6 5000 5000
       plan-capacity-send 100000
```

  The following is an example of a correct configuration:

```
conf t
cs7 util-plan-capacity
```

  Or

```
conf t
cs7 instance 0 linkset to-STP1
    link 0 sctp 10.2.3.4 10.4.5.6 5000 5000
       plan-capacity-send 100000
       plan-capacity-rcvd 100000
```

  Workaround: Always specify a send and receive planning capacity or use the global default.

- CSCea72856 - RCP for nonexistent cluster but member configd must be responded

  Symptom: If an adjacent node sends the ITP an RCP (routeset cluster prohibited test) message or RCR, the ITP will not respond with a TCA or TCR. This occurs when the concerned cluster is not configured on the ITP, and there are one or more members within that cluster configured, and available or restricted on the ITP. As a result, the adjacent node will not be able to route messages for those members to the ITP.

  Conditions: This happens only in ANSI networks where cluster routes are in use. It occurs when a node adjacent to the ITP has cluster routes toward the ITP, and the ITP has only member routes configured within that cluster.

Since the ITP has no cluster route configured, it would not have sent a TCP or TCR in the first place to the adjacent node. The adjacent node is not expected to spontaneously send RCP or RCR without first receiving TCP or TCR. Therefore, the likelihood of the occurrence of this caveat is tied to the behavior of the adjacent node.

Workaround: There is no workaround.

- CSCea74594 - ITP R4: enhance nvgen of route/ls to output ls first

  Symptom: **show cs7 linkset** command displays linksets with adjacent pc 0.0.0 that are unexpected

  Conditions: When user modifies the startup_config file to include routes that reference linksets that are not listed in the startup_config file.

  Workaround: Modify the startup_config file to NOT include routes that reference linksets that are not listed in the startup_config. Reload the box after modifying the startup_config.

- CSCea74624 - ITP-R4: show cs7 acct does not display stats for all dest linksets

  Symptom: The **show cs7 accounting** commands when used with the point code filter display options do not show accounting data for all linksets.

  Workaround: Do not use the point code filter option when displaying the accounting data or, as an alternative, use the include filter option.

- CSCea76431 - Performance degradation of 2600 MTP2 links

  Symptom: Under high link utilization, Signaling System 7 (SS7) links may drop because of corruption in FISU/LSSU. This problem is particularly more prevalent on the 2600.

  Workaround: There is no workaround.

- CSCea79627 - Flapping Destination status causes memory loss and locked route tabl

  Symptom: The ITP can lose memory and the routing table will not allow changes when an adjacent destination changes status rapidly between Prohibited and Allowed or Restricted. For this to happen:

  - The direct linkset to the adjacent destination is unavailable, and
  - An alternate route to the destination is configures over an available linkset, and
  - The ITP receives a constant stream of TFP followed by TFR or TFA over the alternate route concerning the destination.

  Workaround: There is no workaround.

- CSCea79682 - Format error in %CS7MTP3-5-NONADJSIG message

  Symptom: A Cisco Internet Transfer Point may print the following malformatted message:

  ```
  %CS7MTP3-5-NONADJSIG: Received 3-4-1 message from non adjacent node OPC =
  ```

  The message should read as follows:

  ```
  %CS7MTP3-5-NONADJSIG: Received TFP message from non adjacent node OPC = 3-4-1
  ```

  Workaround: There is no workaround.

- CSCea79999 - Configuration inconsistencies

  Symptom: The following symptoms would occur if multiple instances are configured:

  - CLI does not enforce configuration of the local point code before configuration of linksets.
  - CLI allows removal of network-name while linkset is configured.
  - CLI allows removal of linkset from different instance.

  Workaround:

  - Do not try to configure linksets before local point code.
  - Do not try to remove network-name while linkset is configured.
  - Do not try to remove linkset from different instance.

- CSCea87000 - ITP: rsp crash when sending TFRs for more restrictive cluster member

  Symptom: ITPs that are running MB10 images are susceptible to a caveat if using ANSI cluster routing in situations in which a member of a cluster becomes restricted while the overall cluster remains available. The result of this caveat is a RSP software reload.

  Workaround: There is no workaround.

Open Caveats—Cisco IOS Release 12.2(4) MB10

No open caveats specific to Cisco IOS Release 12.2(4) MB10 require documentation in the release notes.

Resolved Caveats—Cisco IOS Release 12.2(4) MB10

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(4) MB10. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCea08661 - ITP sends TFx mgmt msg with wrong sls value (ITU only)

  Symptom: The IP Transfer Point (ITP) is inserting a random signalling link selector value into non link-related Message Transfer Part Level 3 (MTP3) management messages such as TFA, TFP, TFR, and TRA.

  ITU Q-704 requires such messages to be send with an SLS value of zero. However ANSI specifications do not require the use of an SLS value of zero for non link-related messages.

  This causes severe interoperability problems with Lucent DNCP and Comverse SMV. Both devices discard all TFx messages send by the ITP.

  Workaround: There is no workaround.

- CSCea08752 - TFA sent if RST is received immediately after broadcast TFP

  Symptom: If a Route-Set-Test (RST) message is received by the ITP shortly (less than two seconds) after the Transfer-Prohibited (TFP) message, then the ITP responds wrongly with a Transfer-Allowed (TFA) message.

  The ITP sends broadcast Transfer-Prohibited (TFP) messages when the destination become unavailable due to a signalling link failure. A signalling point receiving such messages will start a Route-Set-Test procedure as described in Q-704. Part of that procedure is an RST message from the signalling end point to the ITP to verify the status of the affected destination.

  Workaround: There is no workaround.

- CSCea35357 - ITP-R4: RSP crashes during heavy linkset flapping

  Symptom: A Cisco ITP reloads when a **shutdown** command is issued on an M2PA link while that link is in the process of connecting to the remote ITP. This problem is very rarely seen.

  Workaround: There is no workaround.

- CSCdz84201 - Missing route entries when walking cItpRouteTable using SNMP

  Symptom: When walking the cItpRouteTable in the CISCO-ITP-RT-MIB, routes may be missing in certain configurations.

The show **cs7 route detail** command displays the following output:

```
13/14            INACC     1 itp-d               UNAVAIL allowed UNAVAIL
14/14            INACC     1 sp-2a               UNAVAIL allowed UNAVAIL
14/14                       1 sp-a                 UNAVAIL allowed UNAVAIL
15/14            INACC     1 itp-d               UNAVAIL allowed UNAVAIL
```

The following is output from an SNMP walk of the ItpRouteTable in the CISCO-ITP-RT-MIB.my Management Information Base:

```
system : 13 : 16383 : 1 : itp-d : 2
                                    <== sp-a should here
system : 14 : 16383 : 1 : sp-2a : 4
system : 15 : 16383 : 1 : itp-d : 2
system : 15 : 16383 : 1 : stp-c : 2
```

Conditions: On Cisco 2600 series routers that are running Cisco IOS 12.2(4)MB5 release and Cisco IOS 12.2(4)MB9 release of the ITP product.

When routes with the same priority are specified using secondary point code, the route may be skipped during a walk of the cItpRouteTable.

Workaround: Reorder the configuration statements for the involved linkset or rename them to have equal length names. You can avoid the problem by renaming the "sp-a" linkset to "sp-1a" so that the names are the same length.

- CSCdz71361 - ITP: linkset stuck in available without active links

  Symptom: Concurrent transmission facility failures and SNMP polls can cause the ITP to report a linkset as available while no links in that linkset are active.

  Workaround: Performing a **shut** and **no shut** of linkset or links sometimes, but not always, recovers from this situation. If this occurs, then switching over to the secondary processor or a reload is necessary.

Open Caveats—Cisco IOS Release 12.2(4) MB9a

No open caveats specific to Cisco IOS Release 12.2(4) MB9a require documentation in the release notes.

Resolved Caveats—Cisco IOS Release 12.2(4) MB9a

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(4) MB9a. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdz71361

  Symptom: ITP: Linkset stuck in available without active links

  Concurrent transmission facility failures and SNMP polls can cause the ITP to report a linkset as available while no links in that linkset are active.

  Shut and **no shut** of linkset or links sometimes but not always recovers from this situation. If this occurs, then switching over to the secondary processor or a reload is necessary.

  Workaround: There is no workaround.

- CSCea03192

  Symptom: ITP: Links remain permanently in FAILED state

Under rare circumstances, a Signaling System 7 (SS7) link may get stuck in state FAILED.

Workaround: Perform a switch-over to a secondary processor or to reload the ITP.

- CSCea08661

  Symptom: ITP sends TFx mgmt msg with wrong SLS value (ITU only)

  The ITP is inserting a random signaling link selector (SLS) value into non link-related mtp3 management messages such as TFA, TFP, TFR, TRA. ITU Q-704 requires such messages to be sent with an SLS value of zero.

  ANSI specifications do not require using SLS zero for non link-related messages. Doing so causes severe interoperability problems with Lucent DNCP and Comverse SMV. Both devices discard all TFx messages sent by the ITP.

  Workaround: There is no workaround.

- CSCea08752

  Symptom: TFA sent if RST is received immediately after broadcast TFP

  The ITP sends broadcast Transfer-Prohibited (TFP) messages when the destination becomes unavailable due to a signaling link failure. A signaling point receiving such messages starts a Route-Set-Test (RST) procedure as described in ITU Q-704. Part of that procedure sends an RST message from the signaling end point to the ITP to verify the status of the affected destination.

  If the RST message is received by the ITP shortly (less than two seconds) after the TFP then the ITP responds wrongly with a Transfer-Allowed (TFA) message.

  Workaround: There is no workaround.

Open Caveats—Cisco IOS Release 12.2(4) MB9

No open caveats specific to Cisco IOS Release 12.2(4) MB9 require documentation in the release notes.

Resolved Caveats—Cisco IOS Release 12.2(4) MB9

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(4) MB9. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdz28216

  Symptom: When a remote process outage occurs at an adjacent node for a duration less than the ITP T1 timer defined for the link to the adjacent node, the link may stay unavailable indefinitely. If this occurs, the link will remain in this state until the link is shut down and restarted. This issue will only occur when the CS7 variant is configured for ITU.

  Workaround: There is no workaround.

- CSCdz30119

  On a Cisco 2600 or Cisco 7500 series router that is running Cisco IOS Release 12.2(4)MB4 or Cisco IOS Release 12.2(4)MB8 release of the ITP product, a MIB variable returns an incorrect value for the network indicator if the network indicator is not set to the default value of **national**.

```
cs7 network-indicator ?
  international  International network
  national       National network
  reserved       Reserved for national use
  spare          Spare (for international use only)
```

Workaround: Ignore the index value returned from the cItpSpPointCodeNi table and use the network indicator specified on the linkset (cItpSpLinksetNi).

- CSCdz37993

  Symptom: When the first link in the second linkset of a combined linkset is activated, a changeback declaration (CBD) MSU is erroneously sent on the link being activated. The erroneous CBD is causes the adjacent node to respond with a changeback acknowledgement (CBA) MSU which is correctly ignored by the ITP. This message exchange is harmless.

  Workaround: There is no workaround.

Open Caveats—Cisco IOS Release 12.2(4) MB8

No open caveats specific to Cisco IOS Release 12.2(4) MB8 require documentation in the release notes.

Resolved Caveats—Cisco IOS Release 12.2(4) MB8

No resolved caveats specific to Cisco IOS Release 12.2(4) MB8 require documentation in the release notes.

Open Caveats—Cisco IOS Release 12.2(4) MB7

This section documents possible unexpected behavior by Cisco IOS Release 12.2(4)MB7 and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdy13275

  Symptom: The ITP may send excessive transfer-prohibited messages to an adjacent node during an adjacent SP restart when both cluster routes and member routes exist to the same destination and use the same route.

  Workaround: Remove the member routes.

Resolved Caveats—Cisco IOS Release 12.2(4) MB7

No resolved caveats specific to Cisco IOS Release 12.2(4) MB7 require documentation in the release notes.

Open Caveats—Cisco IOS Release 12.2(4) MB6

No open caveats specific to Cisco IOS Release 12.2(4) MB6 require documentation in the release notes.

Resolved Caveats—Cisco IOS Release 12.2(4) MB6

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(4) MB6. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdx59699

  Under rare circumstances, it is possible for a linkset to remain unavailable, although the links in the linkset are available. This may occur if the adjacent node does not send a TRA in response to an adjacent SP restart, the ITP was not configured to disable adjacent SP restart for the adjacent node by using the **no adjacent-sp-restart** configuration command, and an alternate route to the adjacent node became available after the adjacent SP restart began.

  Workaround: Remove the linkset definition to the adjacent node, add it back again, and then activate the linkset.

- CSCdx70251

  When low-speed links are not aligned, MTP2 LSSU messages are constantly sent from the adjacent node. These are short messages and they constantly repeat on the wire/channel. The processing of these link proving messages can drive Versatile Interface Processor (VIP) CPU up and under extreme conditions can make it difficult for the VIP to service other low-speed links. Unless there are error conditions that cause eight or more low-speed links to be in the LSSU proving state at the same time, the VIP CPU is not a concern.

  Workaround: A software change allows the PA-MCX-8TE1-M to filter duplicate LSSU messages, thereby avoiding VIP CPU spikes.

- CSCdx83439

  An ambiguous error is displayed when running the **clear cs7 as** and **clear cs7 asroute** commands.

  Workaround: Use the **clear cs7 all** command.

- CSCdx83901

  The ITP's Global Title Address Conversion feature does not translate addresses correctly when the output address prefix is null (that is, **no out-address** parameter was specified on the **update** command in global title translation (GTT) address conversion submode). The absence of an output address prefix is intended to delete the input address prefix. Instead, the GTT address is corrupted and contains the characters "DEFA" in the first four digit positions.

  Workaround: Configure the translation feature in such a way that it can be accomplished with output address prefixes that are not null.

- CSCdx84452

  When ITP runs low of usable system memory, it is possible for a Signaling System 7 (SS7) route to buffer for controlled rerouting indefinitely. The symptom is that message signaling units queue towards the impacted destination will be lost, resulting in application timeouts.

  Workaround: Removing and re-adding the impacted route clears the problem.

- CSCdx86075

  Upon reconfiguration of ITP, including point-code and variant, global title translation (GTT) routing failures may occur. SCCP processing of the MTP3 restart did not completely update the status of MAP entries for newly restarted links.

- CSCdx87964

  Memory leak causing router to eventually fail. Occurs when traffic arrives via M3UA to be sent out on MTP3 linksets to route that cannot be accessed. This could occur because of remote congestion or no route in the routing table.

Workaround: If the conditions described occur, upgrade the software.

- CSCdx92630

  The ITP may reload when the global title translation (GTT) configuration is deleted after ITP variant changes. The following message is displayed before the system failure:

  ```
  %SYS-2-CHUNKFREE: Attempted to free nonchunk memory, chunk <address>, data <address>
  ```

  This may occur when GTT tables are configured and the ITP variant is changed by using the **cs7 variant** command. Another scenario involves deleting the ITP variant by using the **no cs7 variant** command and then issuing the **cs7 variant** command.

  Workaround: Delete the GTT configuration before changing the variant or deleting the variant.

- CSCdx94940

  The **clear cs7 all** command does not clear ITP access violation statistics.

  Workaround: These statistics can be cleared by issuing a **clear cs7 accounting access-violations** command.

Open Caveats—Cisco IOS Release 12.2(4) MB5

This section documents possible unexpected behavior by Cisco IOS Release 12.2(4)MB5 and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdx40164

  When **no IP routing** is entered and there are more than five links in the linkset, the links may flap.

  Workaround: Leave IP routing on as the default.

Resolved Caveats—Cisco IOS Release 12.2(4) MB5

No resolved caveats specific to Cisco IOS Release 12.2(4) MB5 require documentation in the release notes.

Open Caveats—Cisco IOS Release 12.2(4) MB4

No open caveats specific to Cisco IOS Release 12.2(4) MB4 require documentation in the release notes.

Resolved Caveats—Cisco IOS Release 12.2(4) MB4

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(4) MB4. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdt01449

  Under very heavy load, a Cisco 2600 series router that is running ITP software may drop Signaling System 7 (SS7) links if the commands **show running-config** or **write memory** are used.

- CSCdw69561

  The ITP waits during a full MTP3 restart for response from all adjacent Signaling System 7 (SS7) nodes. If an adjacent node does not support the MTP3 restart protocol, then the ITP waits as specified in timer T23 before putting any linkset into service.

  Using the "no adjacent-restart" linkset configuration also during full MTP3 restart decreases the waiting time for a full restart to finish. This also decreases the downtime after switchover between Route Switch Processors (RSPs).

- CSCdw82406

  The ITP does not provide measurements of how often mated applications have been used while performing global title translation.

- CSCdw88853

  When a QoS class becomes unavailable, SS7oIP traffic is discarded. The traffic should be reclassified as "best-effort" and use the default QoS class (class 0).

- CSCdw91492

  The **cs7 inhibit** and **uninhibit link** commands should not be allowed without entering enable mode first.

Open Caveats—Cisco IOS Release 12.2(4) MB3

No open caveats specific to Cisco IOS Release 12.2(4) MB3 require documentation in the release notes.

Resolved Caveats—Cisco IOS Release 12.2(4) MB3

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(4) MB3. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdw65903

  An error can occur with management protocol processing. Go to the following URL for further information:

  http://www.cisco.com/cgi-bin/bugtool/onebug.pl?bugid=CSCdw65903

Open Caveats—Cisco IOS Release 12.2(4)MB2

This section documents possible unexpected behavior by Cisco IOS Release 12.2(4)MB2 and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdv68797

  The ITP reports a route table successfully loaded from file, even if a previous error message indicates the file could not be accessed. This happens if a filename is spelled wrong, or file access through TFTP is not possible.

  Workaround: Load the route table from local Flash memory and use the correct spelling.

Resolved Caveats—Cisco IOS Release 12.2(4)MB2

No resolved caveats specific to Cisco IOS Release 12.2(4)MB2 require documentation in the release notes.

Open Caveats—Cisco IOS Release 12.2(1)MB1

This section documents possible unexpected behavior by Cisco IOS Release 12.2(4)MB2 and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdt01449

  Under a very heavy load, a Cisco 2600 series router that is running ITP software may drop Signaling System 7 (SS7) links if the commands **show running-config** or **write memory** are used.

Resolved Caveats—Cisco IOS Release 12.2(1)MB1

No resolved caveats specific to Cisco IOS Release 12.2(1)MB1 require documentation in the release notes.

Related Documentation

The following sections describe the documentation available for the Cisco 2600 series. 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 26
- Platform-Specific Documents, page 27
- Feature Modules, page 28
- Cisco Feature Navigator, page 28
- Cisco IOS Software Documentation Set, page 28

Release-Specific Documents

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

  On Cisco.com at:

  Technical Documents: **Cisco IOS Software**: **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

- The "Caveats for Cisco IOS Release 12.2 MB" section on page 12

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

  On Cisco.com at:

  Technical Documents: Cisco IOS Software: **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, **log in** to Cisco.com and click **Service & Support: Software Center: Cisco IOS Software: BUG TOOLKIT**. 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 2600 series on Cisco.com and the Documentation CD-ROM:

- *Cisco 2600 Series Modular Routers Quick Start Guide*
- Hardware installation documents for Cisco 2600 series
- Software configuration documents for Cisco 2600 series
- Regulatory compliance and safety documents for Cisco 2600 series

On Cisco.com at:

Technical Documents: Cisco Product Documentation: Access Servers and Access Routers: Modular Access Routers: Cisco 2600 Series Routers

On the Documentation CD-ROM at:

Cisco Product Documentation: Access Servers and Access Routers: Modular Access Routers: Cisco 2600 Series Routers

Feature Modules

Feature modules describe new features supported by Cisco IOS Release 12.2(4)MB13c 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: 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 Feature Navigator

Cisco IOS software is packaged in feature sets that are supported on specific platforms. To get updated information regarding platform support for this feature, access Cisco Feature Navigator. Cisco Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Cisco Feature Navigator is a web-based tool that enables you to quickly 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 release. Under the release section, you can compare releases side by side to display both the features unique to each software release and the features 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/cgi-bin/Support/FeatureNav/FN.pl

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: Cisco IOS Software: 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 5 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: Cisco IOS Software: Cisco IOS Release 12.2

On the Documentation CD-ROM at:

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

Table 5 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 Bridging and IBM Networking Configuration Guide* • *Cisco IOS Bridging and IBM Networking Command Reference, Volume 1 of 2* • *Cisco IOS Bridging and IBM Networking Command Reference, Volume 2 of 2*	Transparent Bridging SRB Token Ring Inter-Switch Link Token Ring Route Switch Module RSRB DLSW+ Serial Tunnel and Block Serial Tunnel LLC2 and SDLC IBM Network Media Translation SNA Frame Relay Access NCIA Client/Server Airline Product Set DSPU and SNA Service Point SNA Switching Services Cisco Transaction Connection Cisco Mainframe Channel Connection CLAW and TCP/IP Offload CSNA, CMPC, and CMPC+ TN3270 Server
• *Cisco IOS Dial Technologies Configuration Guide, Release 12.2* • *Cisco IOS Dial Technologies Command Reference, Release 12.2*	Dial Access Modem and Dial Shelf Configuration and Management ISDN Configuration Signaling Configuration Point-to-Point Protocols Dial-on-Demand Routing Dial Backup Dial Related Addressing Service Network Access Solutions Large-Scale Dial Solutions Cost-Control Solutions Internetworking Dial Access Scenarios
• *Cisco IOS Interface Configuration Guide* • *Cisco IOS Interface Command Reference*	LAN Interfaces Serial Interfaces Logical Interfaces
• *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 AppleTalk and Novell IPX Configuration Guide* • *Cisco IOS AppleTalk and Novell IPX Command Reference*	AppleTalk Novell IPX

Table 5 Cisco IOS Release 12.2 Documentation Set (continued)

Books	Major Topics
• *Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Configuration Guide* • *Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Command Reference*	Apollo Domain Banyan VINES DECnet ISO CLNS XNS
• *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
• *Cisco IOS Wide-Area Networking Configuration Guide* • *Cisco IOS Wide-Area Networking Command Reference*	ATM Frame Relay SMDS X.25 and LAPB
• *Cisco IOS Mobile Wireless Configuration Guide* • *Cisco IOS Mobile Wireless Command Reference*	General Packet Radio Service

Table 5 Cisco IOS Release 12.2 Documentation Set (continued)

Books	Major Topics
• *Cisco IOS Terminal Services Configuration Guide* • *Cisco IOS Terminal Services Command Reference*	ARA LAT NASI Telnet TN3270 XRemote X.28 PAD Protocol Translation
• *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 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 this 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

You can order Cisco documentation in these ways:

- Registered Cisco.com users (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 Systems Corporate Headquarters (California, U.S.A.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit comments electronically on Cisco.com. In the Cisco Documentation home page, click the **Fax** or **Email** option in the "Leave Feedback" section at the bottom of the page.

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

You can submit your comments by mail by using the response card behind the front cover of your document or by writing 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 online documentation, troubleshooting tips, and sample configurations from online tools by using the Cisco Technical Assistance Center (TAC) Web Site. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC Web Site.

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 with these tasks:

- 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

If you want to obtain customized information and service, you can self-register on Cisco.com. To access Cisco.com, go to this URL:

http://www.cisco.com

Technical Assistance Center

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

Cisco TAC inquiries 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, impacting 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.

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

Cisco TAC Web Site

You can use the Cisco TAC Web Site 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 this URL:

http://www.cisco.com/tac

All customers, partners, and resellers who have a valid Cisco service 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 this URL to register:

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

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

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

If you have Internet access, we recommend that you open P3 and P4 cases through the Cisco TAC Web Site.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses priority level 1 or priority level 2 issues. 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 automatically opens a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to this 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). When you call the center, 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 26.