Release Notes for Cisco 7000 Family for Cisco IOS Release 12.2 MB

November 12, 2005

Cisco IOS Release 12.2(4)MB13c

78-13338-17

These release notes for the Cisco 7000 Family 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 "Important Notes" section on page 20 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.

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://www.cisco.com/warp/public/732/docsurvey/rtg/ to give us your feedback .

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

Copyright © 2002-2005. Cisco Systems, Inc. All rights reserved.

Contents

These release notes describe the following topics:

System Requirements

This section describes the system requirements for Cisco IOS Release 12.2 MB and includes the following sections:

Memory Recommendations

Table 1 Memory Recommendations for Cisco IOS Release 12.2(4)MB13c

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

Table 2 Memory Recommendations for Cisco IOS Release 12.2(4)MB13b

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

Table 3 Memory Recommendations for Cisco IOS Release 12.2(4)MB13a

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

Table 4 Memory Recommendations for Cisco IOS Release 12.2(4)MB13

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

Table 5 Memory Recommendations for Cisco IOS Release 12.2(4)MB12

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

0

Table 6 Memory Recommendations for Cisco IOS Release 12.2(4)MB11

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

Table 7 Memory Recommendations for Cisco IOS Release 12.2(4)MB10

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

Table 8 Memory Recommendations for Cisco IOS Release 12.2(4)MB9a

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 7500	IP Standard Feature Set	IP Transfer Point	rsp-itpv-mz	32 MB Flash	128 MB DRAM	FLASH

Table 9 Memory Recommendations for Cisco IOS Release 12.2(4)MB9

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 7500	IP Standard Feature Set	IP Transfer Point	rsp-itpv-mz	32 MB Flash	128 MB DRAM	FLASH

Table 10 Memory Recommendations for Cisco IOS Release 12.2(4)MB8

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

Table 11 Memory Recommendations for Cisco IOS Release 12.2(4)MB7

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

Table 12 Memory Recommendations for Cisco IOS Release 12.2(4)MB6

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

Table 13 Memory Recommendations for Cisco IOS Release 12.2(4)MB5

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

Table 14 Memory Recommendations for Cisco IOS Release 12.2(4)MB4

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

Table 15 Memory Recommendations for Cisco IOS Release 12.2(4)MB3

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

Table 16 Memory Recommendations for Cisco IOS Release 12.2(4)MB2

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

Table 17 Memory Recommendations for Cisco IOS Release 12.2(4)MB1

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

Supported Hardware

Cisco IOS Release 12.2(4)MB13c supports the following Cisco 7000 family platforms:

- Cisco 7200 series routers
- Cisco 7500 series routers

For detailed descriptions of the new hardware features, see the "New and Changed Information" section on page 9.

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) 12.2 MB Software (rsp-itpv-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 *Upgrading the Cisco IOS Software Release in Cisco Routers and Modems* located at:

http://www.cisco.com/warp/public/620/6.html

Feature Set Tables

The Cisco IOS software is packaged in feature sets consisting of software images—depending on the platform. Each feature set contains a specific set of Cisco IOS features.

Cisco IOS Release 12.2(4)MB13csupports the same feature sets as Cisco IOS Release 12.2, but Cisco IOS Release 12.2(4)MB13c include new features supported by the Cisco 7000 Family.

Table 18 through Table 19 lists the features and feature sets supported by the Cisco 7000 family 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)MB means a feature was introduced in 12.2(1)MB.

Note This table might not be cumulative or list all the features in each image. You can find the most current Cisco IOS documentation on Cisco.com. These electronic documents may contain updates and modifications made after the hard-copy documents were printed.

Table 18 Feature List by Feature Set for the Cisco 7200 Series

Features	In	Software Images by Feature Sets			
		IP Transfer Point			
CS7 Monitor	(4)MB12	Yes			
ITP Instance Translation	(4)MB10	Yes			
ITP Multi-Layer Short Message Service Routing	(4)MB10	Yes			
ITP Multiple Instances	(4)MB10	Yes			
ITP Packet Logging Facility	(4)MB11	Yes			

Table 19 Feature List by Feature Set for the Cisco 7500 Series

Features	In	Software Images by Feature Sets			
		IP Transfer Point			
CS7 Monitor	(4)MB12	Yes			
ITP Instance Translation	(4)MB10	Yes			
ITP M3UA/SUA Signalling Gateway	(4)MB5	Yes			
ITP Multi-Layer Short Message Service Routing	(4)MB10	Yes			
ITP Multiple Instances	(4)MB10	Yes			
ITP Packet Logging Facility	(4)MB11	Yes			
ITP RPR+	(4)MB3	Yes			
ITP SCCP/GTT	(4)MB1	Yes			
ITP Support on 7204/6 VXR	(4)MB8	Yes			
MTP3 Offload	(4)MB12	Yes			
SCCP Load Balancing Enhancements	(4)MB2	Yes			
xUA SCTP VIP Offload	(4)MB13				
SIM Authentication and Authorization for Cisco WLAN Solution	(4)MB7	Yes			
SS7 over ATM High Speed Link (HSL) Support	(4)MB2	Yes			
Support for VIP680 and RSP16	(4)MB7	Yes			

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 MB.

New Hardware Features in Cisco IOS Release 12.2(4)MB13c

There are no new hardware features supported by the Cisco 7000 family for Cisco IOS Release 12.2(4)MB13c.

New Software Features in Cisco IOS Release 12.2(4)MB13c

There are no new software features supported by the Cisco 7000 family for Cisco IOS Release 12.2(4)MB13c.

New Hardware Features in Cisco IOS Release 12.2(4)MB13b

There are no new hardware features supported by the Cisco 7000 family for Cisco IOS Release 12.2(4)MB13b.

New Software Features in Cisco IOS Release 12.2(4)MB13b

There are no new software features supported by the Cisco 7000 family for Cisco IOS Release 12.2(4)MB13b.

New Hardware Features in Cisco IOS Release 12.2(4)MB13a

There are no new hardware features supported by the Cisco 7000 family for Cisco IOS Release 12.2(4)MB13a.

New Software Features in Cisco IOS Release 12.2(4)MB13a

There are no new software features supported by the Cisco 7000 family for Cisco IOS Release 12.2(4)MB13a.

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

There are no new hardware features supported by the Cisco 7000 family for Cisco IOS Release 12.2(4)MB13.

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

The following new software feature is supported by the Cisco 7000 family for Cisco IOS Release 12.2(4)MB13:

xUA SCTP VIP Offload

Platforms: Cisco 7500 series routers

The xUA SCTP VIP Offload feature enables the ITP to perform SCTP message processing on the distributed processors of the VIPs, resulting in overall increased SUA/M3UA (SIGTRAN protocols) message/sec processing capacity on the main RSP processors. The net effect is an increased SUA/M3UA processing capacity of 20% on the 7500-based ITP. Reference the ITP datasheet for detailed performance specifications.

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

There are no new hardware features supported by the Cisco 7000 family for Cisco IOS Release 12.2(4)MB12.

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

The following new software feature is supported by the Cisco 7000 family for Cisco IOS Release 12.2(4)MB12:

CS7 Monitor

Platforms: Cisco 7204VXR routers, Cisco 7206VXR routers, and Cisco 7500 series routers

The CS7 monitor feature allows the ITP to monitor SS7/HSL ports and send the MSUs (via TCP) to a server for collection/storage. This feature is available on the 7200 and 7500 platforms only.

MTP3 Offload

Platforms: Cisco 7500 series routers.

The MTP3 Offload feature enables the ITP to perform MTP3 message forwarding and Global Title Translation on the VIP on the 7500 platform. This feature effectively doubles the MTP3 forwarding performance. This feature is only available on the 7500 platform.

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

There are no new hardware features supported by the Cisco 7000 family for Cisco IOS Release 12.2(4)MB11.

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

The following new software feature is supported by the Cisco 7000 family for Cisco IOS Release 12.2(4)MB11:

ITP Packet Logging Facility

Platforms: Cisco 7204VXR routers, Cisco 7206VXR routers, and Cisco 7500 series routers

The ITP Packet Logging facility uses the BSD Syslog protocol (RFC 3164) to send selected MSUs to a user-selected monitoring tool via the 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.

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

There are no new hardware features supported by the Cisco 7000 family for Cisco IOS Release 12.2(4)MB10.

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

The following new software feature is supported by the Cisco 7000 family for Cisco IOS Release 12.2(4)MB10:

ITP Multi-Layer Short Message Service Routing

Platforms: Cisco 7204VXR routers, Cisco 7206VXR routers, and Cisco 7500 series routers

The ITP Multi-Layer Routing (MLR) feature enables intelligent routing of SMS 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 TCAP, MAP, and MAP-user layers.

ITP Multiple Instances

Platforms: Cisco 7204VXR routers, Cisco 7206VXR routers, and Cisco 7500 series routers

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

ITP Instance Translation

Platforms: Cisco 7204VXR routers, Cisco 7206VXR routers, and Cisco 7500 series routers

The ITP 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.

New Hardware Features in Cisco IOS Release 12.2(4)MB9a

There are no new hardware features supported by the Cisco 7000 family for Cisco IOS Release 12.2(4)MB9a.

New Software Features in Cisco IOS Release 12.2(4)MB9a

There are no new software features supported by the Cisco 7000 family for Cisco IOS Release 12.2(4)MB9a.

New Hardware Features in Cisco IOS Release 12.2(4)MB9

There are no new hardware features supported by the Cisco 7000 family for Cisco IOS Release 12.2(4)MB9.

New Software Features in Cisco IOS Release 12.2(4)MB9

There are no new software features supported by the Cisco 7000 family for Cisco IOS Release 12.2(4)MB9.

New Hardware Features in Cisco IOS Release 12.2(4)MB8

There are no new hardware features supported by the Cisco 7000 family for Cisco IOS Release 12.2(4)MB8.

New Software Features in Cisco IOS Release 12.2(4)MB8

The following new software feature is supported by the Cisco 7000 family for Cisco IOS Release 12.2(4)MB8:

ITP Support on 7204/6 VXR

Platforms: Cisco 7204VXR routers, Cisco 7206VXR routers, and Cisco 7500 series routers

This feature now supports Cisco 7204VXR routers and Cisco 7206VXR routers.

New Hardware Features in Cisco IOS Release 12.2(4)MB7

There are no new hardware features supported by the Cisco 7000 family for Cisco IOS Release 12.2(4)MB7.

New Software Features in Cisco IOS Release 12.2(4)MB7

The following new software feature is supported by the Cisco 7000 family for Cisco IOS Release 12.2(4)MB7:

SIM Authentication and Authorization for Cisco WLAN Solution

Platforms: Cisco 7204VXR routers, Cisco 7206VXR routers, and Cisco 7500 series routers

Cisco IOS Release 12.2(4)MB7 adds support for SIM Authentication/Authorization for Cisco WLAN Solution Architecture to the IP Transfer Point (ITP) product.

Support for VIP680 and RSP16

Platforms: Cisco 7204VXR routers, Cisco 7206VXR routers, and Cisco 7500 series routers

Cisco IOS Release 12.2(4)MB7 adds support for the new Route Switch Processor 16 (RSP16) card and support for the new Versatile Interface Processor 6-80 (VIP6-80) line card for the ITP 7500 platform.

New Hardware Features in Cisco IOS Release 12.2(4)MB6

There are no new hardware features supported by the Cisco 7000 family for Cisco IOS Release 12.2(4)MB6.

New Software Features in Cisco IOS Release 12.2(4)MB6

There are no new software features supported by the Cisco 7000 family for Cisco IOS Release 12.2(4)MB6.

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

There are no new hardware features supported by the Cisco 7000 family for Cisco IOS Release 12.2(4)MB5.

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

The following new software feature is supported by the Cisco 7000 family for Cisco IOS Release 12.2(4)MB5:

ITP M3UA/SUA Signalling Gateway

Platforms: Cisco 7500 series routers

Based on open industry standards, Cisco's IP Transfer Point (ITP) product is designed for transporting SS7 traffic over IP (SS7oIP) networks. Its design provides significant cost efficiencies and scalability enhancements over legacy SS7 networks. Using the IETF's M2PA and SCTP protocols, the initial release of the ITP product provided the base functionality to offload SS7 traffic to IP. Subsequent releases provided the full functionality found in typical legacy signalling transfer point (STP) nodes, such as global title translation (GTT), gateway screening and ISUP transport. In addition, support for high speed links (HSL) was added. Using the M3UA and SUA protocols, this latest release of the ITP provides signalling gateway functionality between legacy SS7 network and IP-enabled signalling end points (SEP) nodes.

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

There are no new hardware features supported by the Cisco 7000 family for Cisco IOS Release 12.2(4)MB4.

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

There are no new software features supported by the Cisco 7000 family for Cisco IOS Release 12.2(4)MB4.

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

The following new hardware feature is supported by the Cisco 7000 family for Cisco IOS Release 12.2(4)MB3:

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

Platforms: Cisco 7500 series routers

The 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 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% MSU per second performance improvement on the VIP under typical conditions.

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

The following new software feature is supported by the Cisco 7000 family for Cisco IOS Release 12.2(4)MB3:

ITP RPR+

Platforms: Cisco 7500 series routers

The IP Transfer Point Route Processor Redundancy (ITP RPR+) feature increases the availability of the 7500 system by limiting potential downtime due to a primary Route-Switch Processor (RSP) software fault. Specifically, this release allows a backup RSP to recover faster from a primary RSP failure. RPR+ for the ITP requires no new hardware and provides greater ITP system availability. Enhancements to RPR+ address the following ITP scenarios:

- Unplanned RSP Outage. ITP RPR+ enables a quicker switchover between an active and a standby RSP in the event of a hardware or software fault on the active RSP. When you configure ITP RPR+, the standby RSP loads a Cisco IOS image on bootup and initializes itself in standby mode. When you configure ITP RPR+ you must also issue the hw-module secondary-cpu reset command to boot the standby RSP. In the event of a fatal error on the active RSP, the system switches to the standby RSP, which reinitializes itself as the active RSP, reloads all of the line cards, and performs an MTP3 restart of the SS7 links. During the failover recovery process, downtime of SS7 links typically will be less than 10 seconds during a clean MTP3 restart and should be no longer than 30 seconds during MTP3 restart error cases.
- Planned Software Upgrade. The Fast Software Upgrade (FSU) feature uses ITP RPR+ to enable the administrator to configure the system to switch over to a standby RSP that is preloaded with an upgraded Cisco IOS software image.

For more information about configuring RPR+, RPR, and FSU, refer to the following URLs:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120st/120st19/st_rpr2.htm#xtocid2882313

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120st/120st16/st_rpr7x.htm

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

There are no new hardware features supported by the Cisco 7000 family for Cisco IOS Release 12.2(4)MB2.

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

The following new software features are supported by the Cisco 7000 family for Cisco IOS Release 12.2(4)MB2:

SCCP Load Balancing Enhancements

Platforms: Cisco 7500 series routers

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

SS7 over ATM High Speed Link (HSL) Support

Platforms: Cisco 7500 series routers

HSL allows full bandwidth utilization of a 1.55Mbps T1 or a 2.048 Mbps E1 for a single 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 Hardware Features in Cisco IOS Release 12.2(4)MB1

There are no new hardware features supported by the Cisco 7000 family for Cisco IOS Release 12.2(4)MB1.

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

The following new software features are supported by the Cisco 7000 family for Cisco IOS Release 12.2(4)MB1:

ITP SCCP/GTT

Platforms: Cisco 7500 series 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 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 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

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

There are no new hardware features supported by the Cisco 7000 family for Cisco IOS Release 12.2(1)MB1.

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

The following new software features are supported by the Cisco 7000 family for Cisco IOS Release 12.2(1)MB1:

ITP SS7 Offload

Platforms: Cisco 7500 series routers

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

The Cisco ITP provides the following benefits:

- Lower incremental investment via cost effective IP network
- Reduced number of links
- Reduced STP ports
- Reduced processor occupancy for STP
- Support for the full suite of Cisco routing protocols and QoS technologies
- Non-intrusive and transparent to SS7 network end point devices
- Full set of high-end routing protocols and IP media
- Integrated SS7 and IP management using IP-based industry standard tools

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.

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 20.

Table 20 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-XNS-MIB	To be determined

Important Notes

IP Transfer Point Phase Two Software Enhancements for Cisco IOS Release 12.2(4)MB4

The following new software enhancements have been made to the IP Transfer Point Phase Two feature since in Cisco IOS Release 12.2(4) MB2:

- **New MIB** CISCO-ITP-SP2-MIB.my provides Quality of Service information for ITP environment event history for SS7 events. (need url to doc)
- **MIB enhancements** New notifications for link utilization have been added to CISCO-ITP-SP-MIB. (need url to doc)
- **Command Line Interface (CLI) changes and additions** (see http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122mb/1224mb4/itp20_4/itpcmds.htm)
  - The new keyword **link-utilization** has been added to **snmp-server enable traps cs7**
  - Integer range sample time is now in seconds for **.sgm-75-72a(config)#cs7 util-sample-interval ? <60-3600>**
  - Integer range utilization threshold is now in percentages for **sgm-75-72a(config)#cs7 util-threshold ? <25-100>** and **sgm-75-72a(config)#cs7 util-abate-deltat ? <0-40>**
  - Planned capacity is now in bits **per second for sgm-75-72(config-cs7-ls-link)# plan-capacity-rcvd ? <56000-2147483647>** and **sgm-75-72(config-cs7-ls-link)# plan-capacity-send ? <56000-2147483647>**

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 use Bug Navigator II to find caveats of any severity for any release. To reach Bug Navigator II, l**og in** to Cisco.com and click **Software Center: Cisco IOS Software: Bug Toolkit: Bug Navigator II**. Another option is to go to http://www.cisco.com/support/bugtools/.

Because Cisco IOS Release 12.2(4)MB1 is the initial base release, there are no resolved caveats. For a list of the resolved caveats, refer to the next set of release notes for this release version.

Table 21 Caveats Reference for Cisco IOS Release 12.2 MB

DDTS Number	Open in Release	Resolved in Release
CSCdu03364	12.2(1)MB1	
CSCdv68797	12.2(4)MB2	
CSCdv74582	12.2(4)MB2	
CSCdw65903		12.2(4)MB3
CSCdw67218		12.2(4)MB4
CSCdw69561		12.2(4)MB4
CSCdw82359		12.2(4)MB4
CSCdw82406		12.2(4)MB4
CSCdw88853		12.2(4)MB4
CSCdw91492		12.2(4)MB4
CSCdx03928		12.2(4)MB4
CSCdx11140		12.2(4)MB4
CSCdx19832		12.2(4)MB4
CSCdx40164	12.2(4)MB5	
CSCdx59699		12.2(4)MB6
CSCdx67742		12.2(4)MB6
CSCdx70251		12.2(4)MB6
CSCdx72410		12.2(4)MB6
CSCdx77249		12.2(4)MB6
CSCdx83901		12.2(4)MB6
CSCdx84452		12.2(4)MB6
CSCdx84529		12.2(4)MB6
CSCdx86075		12.2(4)MB6
CSCdx87964		12.2(4)MB6
CSCdx94940		12.2(4)MB6
CSCdy02518		12.2(4)MB6
CSCdy07277		12.2(4)MB6
CSCdy12418		12.2(4)MB7
CSCdy13275	12.2(4)MB7	
CSCdy14611		12.2(4)MB7
CSCdy17013		12.2(4)MB7
CSCdy20372	12.2(4)MB7	
CSCdy22523		12.2(4)MB7
CSCdy27526		12.2(4)MB7
CSCdy28759		12.2(4)MB7
CSCdy30056		12.2(4)MB7

Table 21 Caveats Reference for Cisco IOS Release 12.2 MB (continued)

CSCdy35364	12.2(4)MB7	
CSCdy35742		12.2(4)MB7
CSCdy61277	12.2(4)MB7	
CSCdy63482		12.2(4)MB13
CSCdy64394	12.2(4)MB7	
CSCdy76083		12.2(4)MB9
CSCdz15806		12.2(4)MB9
CSCdz19623	12.2(4)MB10	
CSCdz28216		12.2(4)MB9
CSCdz30119		12.2(4)MB9
CSCdz34943		12.2(4)MB9
CSCdz37993		12.2(4)MB9
CSCdz38810		12.2(4)MB9
CSCdz48659		12.2(4)MB9
CSCdz53204		12.2(4)MB9
CSCdz54486		12.2(4)MB9
CSCdz56008		12.2(4)MB9
CSCdz58624		12.2(4)MB9
CSCdz71127		12.2(4)MB12
CSCdz71361		12.2(4)MB9a, 12.2(4)MB10
CSCdz84201		12.2(4)MB10
CSCea02355		12.2(4)MB12
CSCea08661		12.2(4)MB9a, 12.2(4)MB10
CSCea08752		12.2(4)MB9a, 12.2(4)MB10
CSCea35357		12.2(4)MB10
CSCea59369		12.2(4)MB11
CSCea64225		12.2(4)MB11
CSCea65446		12.2(4)MB11
CSCea72856		12.2(4)MB11
CSCea74594		12.2(4)MB11
CSCea74624		12.2(4)MB11
CSCea76431		12.2(4)MB11
CSCea79627		12.2(4)MB11
CSCea79682		12.2(4)MB11
CSCea79999		12.2(4)MB11
CSCea87000		12.2(4)MB11
CSCeb15156		12.2(4)MB12

Table 21 Caveats Reference for Cisco IOS Release 12.2 MB (continued)

CSCeb23816		12.2(4)MB12
CSCeb39832		12.2(4)MB12
CSCeb42215		12.2(4)MB12
CSCeb46313		12.2(4)MB12
CSCeb54609		12.2(4)MB13
CSCeb57599		12.2(4)MB13
CSCeb58198		12.2(4)MB13
CSCeb73047		12.2(4)MB13
CSCeb84186		12.2(4)MB13
CSCef68324		12.2(4)MB13b
CSCei61732		12.2(4)MB13c
CSCei76358		12.2(4)MB13c
CSCsa81379		12.2(4)MB13a

Open Caveats—Cisco IOS Release 12.2(4)MB13c

This section documents possible unexpected behavior by Cisco IOS Release 12.2(4)MB13c 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(4)MB13c.

Resolved Caveats—Cisco IOS Release 12.2(4)MB13c

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(4)MB13c. 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.

- 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(4)MB13b

This section documents possible unexpected behavior by Cisco IOS Release 12.2(4)MB13b 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(4)MB13b.

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.

Open Caveats—Cisco IOS Release 12.2(4)MB13a

This section documents possible unexpected behavior by Cisco IOS Release 12.2(4)MB13a 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(4)MB13a.

Resolved Caveats—Cisco IOS Release 12.2(4)MB13a

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(4)MB13a. 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 command **ip flow-cache feature-accelerate** will no longer be recognized in any IOS configuration.

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

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

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

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

```
cnfFeatureAcceleration         1.3.6.1.4.1.9.9.99999.1.3
cnfFeatureAccelerationEnable   1.3.6.1.4.1.9.9.99999.1.3.1
cnfFeatureAvailableSlot        1.3.6.1.4.1.9.9.99999.1.3.2
cnfFeatureActiveSlot           1.3.6.1.4.1.9.9.99999.1.3.3
```

```
cnfFeatureTable              1.3.6.1.4.1.9.9.99999.1.3.4
cnfFeatureEntry              1.3.6.1.4.1.9.9.99999.1.3.4.1
cnfFeatureType               1.3.6.1.4.1.9.9.99999.1.3.4.1.1
cnfFeatureSlot               1.3.6.1.4.1.9.9.99999.1.3.4.1.2
cnfFeatureActive             1.3.6.1.4.1.9.9.99999.1.3.4.1.3
cnfFeatureAttaches           1.3.6.1.4.1.9.9.99999.1.3.4.1.4
cnfFeatureDetaches           1.3.6.1.4.1.9.9.99999.1.3.4.1.5
cnfFeatureConfigChanges      1.3.6.1.4.1.9.9.99999.1.3.4.1.6
```

Open Caveats—Cisco IOS Release 12.2(4)MB13

This section documents possible unexpected behavior by Cisco IOS Release 12.2(4)MB13 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(4)MB13.

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.

- CSCdy63482

  Associations missing from the CISCO-IETF-SCTP-MIB and CISCO-IETF-SCTP-MIB MIBs.

  This problem occurs on a Cisco 7500 series routers running Cisco IOS 12.2(4)MB4- or Cisco IOS 12.2(4)MB7 releases of the ITP product.

  If SS7 links based on Stream Transmission Control Protocol(SCTP) are configured and have been offloaded to the VIP then information on the associations will not appear in the CISCO-IETF-SCTP-MIB and CISCO-IETF-SCTP-MIB MIBs.

  Workaround: Do not enable associations to be offloaded to VIP.

- CSCeb54609

  When the ITP SUA Signaling Gateway is converting an XUDT (with segmentation info) to the CLDT message, it does not convert the segmentation info present in the XUDT message to the corresponding SUA field in the CLDT message.

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

  There are no known workarounds.

- CSCeb57599

  The router (or vip if MTP3 offload is configured) will crash during GTT processing.

  The crash will only happen 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

  Incorrectly formatted cSctpExtDestAddressStateChange notification when SCTP association offloaded to VIP.

  This problem occurs on a Cisco 2600 or 7500 series routers running Cisco IOS 12.2(4)MB12.

  Workaround: Do not offload SS7 links or disable notification.

- CSCeb73047

  The cgrtInstLoadStatus object in the CISCO-ITP-GRT-MIB.my can incorrectly indicate an error occurred during the load of route table.

  This problem occurs on a Cisco 2600 or 7500 series routers running Cisco IOS 12.2(4)MB10 to Cisco IOS 12.2(4)MB12 releases of the ITP product.

  Workaround: Verify status of load by looking a SYSLOG messages.

- CSCeb84186

  This ddts integrates security fixes CSCdz71127 and CSCea02355 into ITP software.

Open Caveats—Cisco IOS Release 12.2(4)MB12

This section documents possible unexpected behavior by Cisco IOS Release 12.2(4)MB12 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(4)MB12.

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

  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

- CSCeb15156

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

  This problem may occur on Cisco 2600 or Cisco 7500 series routers 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

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

  This problem may occur on Cisco 2600 or Cisco 7500 series routers running Cisco IOS 12.2(4)MB10 or Cisco IOS 12.2(4)MB11 release of the ITP product.

  Workaround: Correctly configure links.

- CSCeb39832

  A Cisco ITP may switchover to the secondary processor if a 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 will prevent this.

- CSCeb42215

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

  This problem may occur on a Cisco 2600 or 7500 series routers 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 causing this crash.

  Workaround: Reduce the MTU sizes on the IP interfaces that are greater than 1500 bytes to 1500 bytes.

- CSCeb46313

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

  Workaround: Make sure that port adapters are correctly seated within the VIP. Do not attempt to configure hardware that is removed.

Open Caveats—Cisco IOS Release 12.2(4)MB11

This section documents possible unexpected behavior by Cisco IOS Release 12.2(4)MB11 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(4)MB11.

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

  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.

  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.

- CSCea64225

  A Fast Ethernet interface stops forwarding or receiving IP traffic.

  A Fast Ethernet interface might stop working after failover if ALL if the following are true:

  – The Fast Ethernet port is on a VIP with M2PA offloaded local-peers.

  – There is an alternate IP route available over this Fast Ethernet interface.

  – There has been a redundancy switchover performed since power up (due to user-force switchover, unexpected system reload, or software upgrade).

  Workaround: Do not mix Fast Ethernet ports used for m2pa offloaded local-peers with other Fast Ethernet ports on the same VIP.

- CSCea65446

  A crash may occur when the link planning capacity is incorrectly configured.

  On a Cisco 7500 series routers running Cisco IOS 12.2(4)MB10, the following conditions produce this 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 global default.

- CSCea72856

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

  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 occurrence of this bug is tied to the behavior of the adjacent node.

  There are no known workarounds.

- CSCea74594

  The **show cs7 linkset** command displays linksets with adjacent pc 0.0.0 that are unexpected.

  This problem occurs when modifications to the startup_config include routes which reference linksets that are not listed in startup_config.

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

- CSCea74624

  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.

  Alternative workaround: Use the include filter option as an alternative.

- CSCea76431

  Under high link utilization, SS7 links may drop because of corruption in FISU/LSSU. This problem is particularly more prevalent on the 2600.

  There are no known workarounds.

- CSCea79627

  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.

  There are no known workarounds.

- CSCea79682

  A Cisco Internet Transfer Point may print a malformatted message:

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

  The message should read:

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

  There are no known workarounds.

- CSCea79999

  CLI does not enforce to CONFIGURATION OF THE local point code before CONFIGURATION OF linksets. CLI allows the user to remove network-name while linkset is configured. CLI allows the user to remove linkset from different instance.

  These symptoms would occur if multiple instances are configured.

  Workaround: Do not try to configure linksets before local point code.

  Alternative workaround 1: Do not try to remove network-name while linkset is configured.

  Alternative workaround 2: Do not try to remove linkset from different instance.

- CSCea87000

  ITPs 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.

  There are no known workarounds for this caveat beyond avoiding this configuration.

Open Caveats—Cisco IOS Release 12.2(4)MB10

This section documents possible unexpected behavior by Cisco IOS Release 12.2(4)MB10 and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdz19623

  The insertion of a VIP, following removal, may cause links to drop.

  This is an intermittent problem that does not always occur on every VIP insertion.

  Workaround: Avoid OIR of VIP when links are active with traffic.

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.

- CSCdz71361

  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/no shut of linkset or links will sometimes but not always recover from this situation. If this is the case then a switch-over to the secondary processor or a reload is necessary.

  There are no known workarounds.

- CSCdz84201

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

  The following is output form a show **cs7 route detail** command:

```
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 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
```

  This problem occurs on a Cisco 2600 or 7500 series routers running Cisco IOS 12.2(4)MB5 and Cisco IOS 12.2(4)MB9 releases 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.

  The problem can be avoided by renaming the “sp-a” linkset to “sp-1a” so that the names are the same length.

  Workaround: Reorder the configuration statements for the involved linkset or rename them to have equal length names.

- CSCea08661

  The ITP is inserting random signalling link selector value into non link-related mtp3 management messages such as TFA, TFP, TFR, TRA. ITU Q-704 requires such messages to be send with a sls value of zero.

  ANSI specifications do not require to use sls 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.

  There are no known workarounds.

- CSCea08752

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

  There are no known workarounds.

- CSCea35357

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

  There are no known workarounds.

Open Caveats—Cisco IOS Release 12.2(4)MB9a

This section documents possible unexpected behavior by Cisco IOS Release 12.2(4)MB9a 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(4)MB9a.

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

  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/no shut of linkset or links will sometimes but not always recover from this situation. If this is the case then a switch-over to the secondary processor or a reload is necessary.

  There are no known workarounds.

- CSCea08661

  The ITP is inserting random signalling link selector value into non link-related mtp3 management messages such as TFA, TFP, TFR, TRA. ITU Q-704 requires such messages to be send with a sls value of zero.

  ANSI specifications do not require to use sls 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.

  There are no known workarounds.

- CSCea08752

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

  There are no known workarounds.

Open Caveats—Cisco IOS Release 12.2(4)MB9

This section documents possible unexpected behavior by Cisco IOS Release 12.2(4)MB9 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(4)MB9.

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.

- CSCdy76083

  Upon receipt of a TFP or adjacent PC linkset failure, the ITP SUA signaling gateway sends two identical SUA DUNA messages to the ASPs reporting the outage. The duplication causes no adverse effect.

  There are no known workarounds.

- CSCdz15806

  In a dual RSP system configured for RPR+, an OIR of a VIP may cause the slave RSP to reload.

  The following message may be output on the slave RSP prior to reload:

  ```
  %HA_3_SYNC_ERROR: SNMP IDB not found/SNMP sync failed
  ```

  There are no known workarounds.

- CSCdz28216

  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 shutdown and restarted. This issue will only occur when the CS7 variant is configured for ITU.

  There are no known workarounds.

- CSCdz30119

  On a Cisco 2600 or 7500 series router running Cisco IOS 12.2(4)MB4 or Cisco IOS 12.2(4)MB8 release of the ITP product, a MIB variable returns an incorrect value for the network indictor if the network indicator is not set to the default, 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 cItpSpPointCodeNi table and use network indicator specified on the linkset (cItpSpLinksetNi).

- CSCdz34943

  Update configuration manuals to include TUP in the set of valid Service Indicator (SI) values in an M3UA routing key.

  Old syntax:

```
havelock(config-cs7-as)#routing-key 1 1.2.3 si ?
  isup  ISUP service indicator (M3UA only)
  sccp  SCCP service indicator
```

  New syntax:

```
havelock(config-cs7-as)#routing-key 1 1.2.3 si ?
  isup  ISUP service indicator (M3UA only)
  sccp  SCCP service indicator
  tup   TUP service indicator (M3UA only)
```

- CSCdz37993

  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 causes the adjacent node to respond with a changeback acknowledgement (CBA) MSU which is correctly ignored by the ITP. This message exchange is harmless.

  There are no known workarounds.

- CSCdz38810

  Retrieve BSNT times out or fails which could lead to packet loss.

  In rare situations MTP3 could request BSN from HSL prior to HSL knowing the link is going down. At present this flow is not addressed in the HSL specs and therefore was not addressed in the code until now.

  There are no known workarounds.

- CSCdz48659

  Packets sourced from SUA ASPs via the ITP SUA SG may be rejected due to a non-standard setting of the national indicator in the SCCP Calling and Called Party address indicator field.

  There are no known workarounds.

- CSCdz53204

  SS7 SCCP class 1 traffic is not distributed correctly when using GGT application groups. A configured cost factor is ignored and the traffic is forwarded to all available subsystems instead of using only those with lowest cost.

  There are no known workarounds.

- CSCdz54486

  Using the **connect** command to create a "drop and insert" connection causes the VIP on which the connection is made to reload and the connection will be in the invalid state after reload finishes.

  This problem will most likely occur if using the "D&I" feature on the 2nd bay of a vip EI or T1 PA.

  Workaround: Ensure that the E1/T1 PA is in bay 0 of the VIP.

- CSCdz56008

  The 7500 router may crash if the **card type** command is issued for a VIP that has been removed from the system.

  There are no known workarounds.

- CSCdz58624

  Use of the **do** command in a configuration submode on the ITP running on the 7500 series using RPR+ can cause the secondary RSP to reload.

  The **do** command will only cause the secondary to reload if the output of the **do** command prints several pages to the console such as a **show** command.

  Workaround: Do not use the **do** command in a configuration submode. The best solution is to leave configuration mode, issue the command, and then re-enter the configuration mode.

Open Caveats—Cisco IOS Release 12.2(4)MB8

This section documents possible unexpected behavior by Cisco IOS Release 12.2(4)MB8 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(4)MB8.

Resolved Caveats—Cisco IOS Release 12.2(4)MB8

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(4)MB8. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

There are no known resolved caveats for Cisco IOS Release 12.2(4)MB8.

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

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

  Workaround: Remove the member routes.

- CSCdy20372

  The **show cs7 linkset util** command can show traffic for links that have been marked unavailable.

  This problem is encountered on SS7 links based on Stream Transmission Control Protocol (SCTP). This problem occurs on Cisco 2600 or 7500 series routers running Cisco IOS 12.2(4)MB5 or Cisco IOS 12.2(4)MB6 release of the ITP product.

  Workaround: Ignore output from **show cs7 linkset util** command for link not in the active state. These types of links are configured in the following manners.

  ```
  cs7 linkset STP01-STP10F 1.1.1
   accounting
   link 0 sctp 172.18.16.27 8000 6000
   route all table system
  !
  ```

- CSCdy35364

  While running moderate traffic the CPU usage can spike periodically. The CPU usage rises for 40-60 seconds and then return to normal levels with roughly 3 minutes between spikes.

  This problem is encountered on SS7 links based on Stream Transmission Control Protocol (SCTP). This problem occurs on Cisco 2600 or 7500 series routers running Cisco IOS 12.2(4)MB5 or Cisco IOS 12.2(4)MB6 release of the ITP product.

  Workaround: The rise is CPU usage does not have a direct impact on the routers ability to transport traffic. These types of links are configured in the following manners.

  ```
  cs7 linkset STP01-STP10F 1.1.1
   accounting
   link 0 sctp 172.18.16.27 8000 6000
   route all table system
  ```

- CSCdy61277

  A CPUHOG message can occur during RPR switchover with different IOS software release when having ATM IMA interfaces in the ITP.

  There is no other functional impact except the additional time spent for the switchover as mentioned in the CPUHOPG message.

  There are no known workarounds.

- CSCdy64394

  A memory leak occurs on the ITP when M2PA associations are configured but none of the local-peers ip addresses for an association is available. The is the case when ip interfaces are down.

Resolved Caveats—Cisco IOS Release 12.2(4)MB7

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(4)MB7. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdy12418

  Out of sequence packets are received when a changeover is forced on an mtp2 link.

  There are no known workarounds.

- CSCdy14611

  When using ITP software, if a Routeset Test Cluster Probibited (RCP) or Routeset Test Cluster Restricted (RCR) message is received for the cluster of which the ITP's local point code is a member, ITP should respond with a Transfer Cluster Accessible (TCA) message. Before the fix for this problem, ITP responded based on route status of the cluster only, without considering that it is a member of the cluster.

  There are no known workarounds.

- CSCdy17013

  On the Cisco 2600 or 7500 series routers running Cisco IOS 12.2(4)MB4 or Cisco IOS 12.2(4)MB5 or Cisco IOS 12.2(4)MB6 release of the ITP product.

  The **show cs7 linkset utilization** command can produce incorrect link utilization when routing traffic that is mostly composed of small packets.

  In addition, the number mib objects will be incorrect when routing traffic that is mostly composed of small packets.

  ```
  cItpSpLinkUtilizationRcvd
  cItpSpLinkL2BytesRcvd
  cItpSpLinkUtilizationSent
  cItpSpLinkL2BytesSent
  ```

- CSCdy22523

  When running in rpr-plus mode, no output is displayed from the following commands:

  ```
  show slavebootflash:
  show slaveslot0:
  show slaveslot1:
  show slavedisk0:
  show slavedisk1:
  ```

  Workaround: Use 'dir slavebootflash:' etc.

- CSCdy27526

  When a remote processor outage is detected, the ITP will perform a sequenced changeover instead of a timed diversion changeover.

  There are no known workarounds.

- CSCdy28759

  Configuring **cs7 fast-restart** may cause the ITP to discontinue sending broadcast TFPs if the ITP has been isolated for longer than 3 seconds.

  There are no known workarounds.

- CSCdy30056

  The ITP does not enforce ANSI timer T27 after the node has become isolated. Instead, the ITP will perform a full MTP3 restart immediately after the first link becomes available without waiting for T27 to expire.

  There are no known workarounds.

- CSCdy35742

  If the user configures “encap mtp2” on an interface before configuring “cs7 variant”, the “encap” command will fail as follows:

```
router(config-if)# encap mtp2
Error in encaps setup.  Encapsulation not changed.
%CS7MTP2-3-NOVARIANT: Must configure CS7 variant before MTP2 encap on the interface

After the "encap mtp2" failure,
the "cs7 variant" command will also fail as follows:

router(config-if)#cs7 variant ansi
%Error: cannot change variant while interfaces are configured with MTP2 encap
```

  There are no known workarounds.

Open Caveats—Cisco IOS Release 12.2(4)MB6

This section documents possible unexpected behavior by Cisco IOS Release 12.2(4)MB6 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(4)MB6.

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 even though 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 and the ITP was not configured to disable adjacent SP restart for the adjacent node 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, then activate the linkset.

- CSCdx67742

  SS7 link goes OOS and fails to re-align

  ITP SS7 low-speed links may not align when the adjacent node sends the MTP2 SIO message before the MTP2 protocol on the ITP is initialized and ready. This problem has been fixed this problem in "CSCdx54149: Telcordia MTP2: T2 expires when SIO received" and will be integrated into the 12.2(4)MB6 release.

  This ddts remains open due to the fact the link does not recover from this ignored SIO as it should. One of the following must be happening...

  – MTP2 SIO/SIOS are not really sent by ITP once MTP2 is initialized (waiting for a line trace to verify)

  – ITP sends MTP2 SIO/SIOS on the wire and for some reason they are ignored by the end-node. End-node is an Ericsson MSC. This is a valid possibility since this situation is only seen when new MSC links are put into service. Once the links come up, they may be recycled without incident.

  To debug link alignment errors, please get a line trace for Cisco to evaluate.

- 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 VIP CPU up and under extreme conditions can make it difficult for the VIP to service other low-speed links.

  Workaround: Unless there are error conditions that cause 8 or more low-speed links to be in the LSSU proving state at the same time, the VIP CPU is not a concern.

- CSCdx72410

  SNMP-3-BADOID: Attempt to generate an invalid object identifier.

  There are no known workarounds.

- CSCdx77249

  The ITP may display error messages '%MCSS7-1-RPTFAIL' upon reload. The message indicates that a VIP failed to report a status change to the RSP.

  There are no known workarounds.

- CSCdx83901

  The ITP's Global Title Address Conversion feature does not translate addresses correctly when the output address prefix is null (i.e. no *out-address* parameter was specified on the **update** command in 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 an SS7 route to buffer for controlled rerouting indefinitely. The symptom is that message signaling units queue towards the affected destination will be lost resulting in application timeouts.

  Workaround: Removing and re-adding the affected route will clear the problem.

- CSCdx84529

  RSP Restart while reading input from VIP console.

  There are no known workarounds.

- CSCdx86075

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

  There are no known workarounds.

- CSCdx87964

  Memory leak causing router to eventually reload.

  Occurs when traffic arrives via M3UA to be sent out on MTP3 linksets to route that can not be accessed. This could be because of remote congestion or no route in the routing table.

  There are no known workarounds.

- CSCdx94940

  The **clear cs7 all** command does not clear ITP access violation statistics. These statistics can be cleared by issuing a clear **cs7 accounting access-violations** command.

  There are no known workarounds.

- CSCdy02518

  The ITP may fail to expand the accounting table when receiving a MSU destined to the ITP itself. This results in a %SYS-3-INVMEMINT followed by a %SYS-2-MALLOCFAIL error message.

  The defect does not cause a data loss as the offending MSU is processed by the ITP. However, there will be no accounting record for this MSU.

  There are no known workarounds.

- CSCdy07277

  Traditionally t1/e1 PAs in IOS default to Line clocking. This enlacement initializes the t1/e1 ports on the Topsail PA to Internal clocking. Once the end user configures clocking on a t1/e1 port, the new configured value will take effect. This is intended to prevent unconfigured but connected ports to become clock source for the PA.

  There are no known workarounds.

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

  Ip routing is turned on by default and when “no IP routing” is entered and if there are more than 5 links in the linkset then the links may flap.

  Workaround: Leave IP routing on as the default

Resolved Caveats—Cisco IOS Release 12.2(4)MB5

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(4)MB5. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

There are no known resolved caveats for Cisco IOS Release 12.2(4)MB5.

Open Caveats—Cisco IOS Release 12.2(4)MB4

This section documents possible unexpected behavior by Cisco IOS Release 12.2(4)MB4 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(4)MB4.

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.

- CSCdw67218

  A Cisco router de-configuring an MTP2 channelized interface may cause the VIP to reload unexpectedly.

  There are no known workarounds.

- CSCdw69561

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

  Using the “no adjacent-restart” linkset configuration also during full mtp3 restart will decrease the time waiting for a full restart to finish. This also decrease the downtime after switchover between RSPs.

- CSCdw82359

  HSL link will not activate following an error during proving.

  Following a SSCOP protocol error during proving, the HSL link may not activate again.

  Workaround: The link will recover if the user shut/no shut the link or linkset with the HSL link.

- CSCdw82406

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

  There are no known workarounds.

- CSCdw88853

  When a QOS class becomes unavailable SS7oIP traffic is discarded. The traffic should be re-classified as “best-effort” and use the default QOS class (class 0).

  There are no known workarounds.

- CSCdw91492

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

  There are no known workarounds.

- CSCdx03928

  When running RPR+ the standby RSP loads route and gtt table from flash before eventually a switchover occurs. Any errors loading those tables are not reported on the active RSP.

  There are no known workarounds.

- CSCdx11140

  LINKED error messages and/or VIP crash.

  During stress a link may fail due to repeated retransmissions. During failover retrieval HSL may requeue and free packet buffers which can cause LINKED error messages and/or VIP crash.

  There are no known workarounds.

- CSCdx19832

  In rare situations a VIP card is disabled after online insertion reporting an error CBUS-3-CCBPTIMEOUT.

  Workaround: Remove the VIP card and insert it again.

Open Caveats—Cisco IOS Release 12.2(4)MB3

This section documents possible unexpected behavior by Cisco IOS Release 12.2(4)MB3 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(4)MB3.

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. Please use 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

  On a Cisco router, the ITP reports a route table successfully loaded from file even if a previous error message indicate the file couldn't be accessed. This will happen if the filename is spelled wrong or file access through tftp isn't possible.

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

- CSCdv74582

  On a Cisco 7500 series router, a Packet loss can occur if the cable is pulled during moderate or high traffic rates on HSL using ATM-IMA T1 interfaces. This problem only occurs on HSL using T1 interfaces, E1s do not exhibit the problem.

  Workaround: Shut the link or reduce the traffic rate prior to removing the cable.

Open Caveats—Cisco IOS Release 12.2(4)MB1

This section documents possible unexpected behavior by Cisco IOS Release 12.2(4)MB1 and describes only severity 1 and 2 caveats and select severity 3 caveats.

There are no new caveats for Cisco IOS Release 12.2(4)MB1.

Open Caveats—Cisco IOS Release 12.2(1)MB1

This section documents possible unexpected behavior by Cisco IOS Release 12.2(1)MB1 and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdu03364

  A Cisco 7500 series router running IP Transfer Point (ITP) software may, in rare situations, report a T1 controller hang after booting IOS.

  Workaround: Use the **shut**/**no shut** command on the controller.

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 44
- Platform-Specific Documents, page 45
- Feature Modules, page 45
- Cisco IOS Software Documentation Set, page 45

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 "Important Notes" 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**

- *Caveats for Cisco IOS Release 12.2 T*

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

  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 use Bug Navigator II to find caveats of any severity for any release. To reach Bug Navigator II, log in to Cisco.com and click **Software Center: Cisco IOS Software: Bug Toolkit: Bug Navigator II**. Another option is to go to http://www.cisco.com/support/bugtools/bugtool.shtml.

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(4)MB9 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 22 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. These electronic documents may contain updates and modifications made after the hard-copy documents were printed.

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 22 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
• 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

Table 22 Cisco IOS Release 12.2 Documentation Set (continued)

Books	Major Topics
• 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 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 provide sources for obtaining documentation from Cisco Systems.

World Wide Web

The most current Cisco documentation is available on the World Wide Web at http://www.cisco.com. Translated documentation can be accessed at http://www.cisco.com/public/countries_languages.shtml.

Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which ships 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 as 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, in North America, by calling 800 553-NETS(6387).

Documentation Feedback

If you are reading Cisco products documentation on the World Wide Web, you can submit technical comments electronically. Click **Feedback** in the toolbar and select **Documentation**. After you complete the form, click **Submit** to send it to Cisco.

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

For your convenience, many documents contain a response card behind the front cover for submitting your comments by mail. Otherwise, you can mail your comments to the following address:

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

We appreciate your comments.

Obtaining Technical Assistance

The following sections provide sources for obtaining technical assistance from Cisco Systems.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at anytime, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

Cisco.com provides a broad range of features and services to help customers and partners streamline business processes and improve productivity. Through Cisco.com, you can find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online technical support, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on Cisco.com to obtain additional personalized information and services. Registered users can order products, check on the status of an order, access technical support, and view benefits specific to their relationships with Cisco.

To access Cisco.com, go to the following website:

http://www.cisco.com

Technical Assistance Center

The Cisco TAC website is available to all customers who need technical assistance with a Cisco product or technology that is under warranty or covered by a maintenance contract.

Contacting TAC by Using the Cisco TAC Website

If you have a priority level 3 (P3) or priority level 4 (P4) problem, contact TAC by going to the TAC website:

http://www.cisco.com/tac

P3 and P4 level problems are defined as follows:

- P3—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- P4—You need information or assistance on Cisco product capabilities, product installation, or basic product configuration.

In each of the above cases, use the Cisco TAC website to quickly find answers to your questions.

To register for Cisco.com, go to the following website:

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

Cisco.com registered users who cannot resolve a technical issue by using the TAC online resource can open a case online by using the TAC Case Open tool at the following website:

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

Contacting TAC by Telephone

If you have a priority level 1(P1) or priority level 2 (P2) problem, contact TAC by telephone and immediately open a case. To obtain a directory of toll-free numbers for your country, go to the following website:

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

P1 and P2 level problems are defined as follows:

- P1—Your production network is down, causing a critical impact to business operations if service is not restored quickly. No workaround is available.
- P2—Your production network is severely degraded, affecting significant aspects of your business operations. No workaround is available.

This document is to be used in conjunction with the documents listed in the "Related Documentation" section on page 43.

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, TeleRouter, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0502R)

Copyright © 2001-2005
Cisco Systems, Inc.
All rights reserved.