



Release Notes for IP Transfer Point (ITP) for Cisco IOS Release 12.4(15)SW

March 2009

Cisco IOS Release 12.4(15)SW3

These release notes describe the enhancements provided in Cisco IOS Release 12.4(15)SW3 and earlier. These release notes are updated as needed.

For a list of the software caveats that apply to Cisco IOS Release 12.4(15)SW, see the [“Caveats for Cisco IOS Release 12.4\(15\)SW”](#) section on page 11.

Contents

These release notes include the following topics:

- [System Requirements, page 1](#)
- [New and Changed Information, page 4](#)
- [Caveats for Cisco IOS Release 12.4\(15\)SW, page 15](#)

System Requirements

This section describes the system requirements for Cisco IOS Release 12.4(15)SW and includes the following sections:

[Supported Platforms and Memory Requirements, page 2](#)



Corporate Headquarters:

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

© 2006 Cisco Systems, Inc. All rights reserved.

[Determining the Software Version, page 2](#)

Supported Platforms and Memory Requirements

Table 1 Recommended Memory for Cisco IOS Release 12.4(15)SW

Platform	Feature Set	Image	Flash Memory	DRAM
Cisco 7200 G1/G2	IP Transfer Point	c7200-itpk9-mz	128/256 MB	256 MB/1GB
Cisco 7301	IP Transfer Point	c7301-itpk9-mz	128 MB	256 MB
Cisco 2811	IP Transfer Point	c2800nm-itpk9-mz	32 MB	256 MB
	IP Transfer Point (SLT)	c2800nm-ipss7-mz	32 MB	256 MB
	IP Transfer Point (SLT)	c2800nm-ipss7k9-mz	32 MB	256 MB

Determining the Software Version

To determine the version of Cisco IOS software running on your Cisco ITP, use the **show version EXEC** command.

New and Changed Information

The following sections list the new hardware and software features supported.

New Hardware Features in Release 12.4(15)SW3

No new hardware features are supported.

New Software Features in Release 12.4(15)SW3

The following new software features are supported:

- [Probeless Monitoring](#)
- [ASP Binding Enhancement](#)
- [Enhanced SCTP Monitoring](#)
- [Support of 32 ASPs per AS](#)
- [CgPA Checking of the MO-SMS Messages](#)
- [GCP \(H.248\) Support](#)
- [Large MSU Support on M2PA and M3UA Associations](#)
- [Increased Local Port Numbers](#)

Probeless Monitoring

Probeless Monitoring enables the ITP to send packets to an external server. The packets sent to this server contain copies of any MSUs received or sent by the ITP. The MSU copies in the packets are carried in an encapsulated, propriety, probeless monitoring protocol (PMP) stacked on top of the UDP protocol and transmitted over a non-reliable IP stream. This feature does not affect normal ITP performance.

ASP Binding Enhancement

This feature enhances ASP binding functionality by eliminating the dynamic creation and maintenance of a unique data structure per ASP binding. This greatly reduces the ITP CPU load, SGMP management traffic, and SUP/LC updates in ITPs forwarding M3UA/SUA traffic with large CIC or SLS ranges using loadshare bindings traffic mode. Instead, ASP bindings are loadshared using a deterministic ranking of ASPs in the AS combined with local and remote ASP state.

Enhanced SCTP Monitoring

This feature provides detection of abnormal SCTP conditions that have not caused the association to fail.

Support of 32 ASPs per AS

This feature provides support for up to 32 ASPs per AS for M3UA and SUA.

CgPA Checking of the MO-SMS Messages

This feature checks the originating MSC/VLR address (SCCP CgPA) of a MO-SMS message against the response of the SRI-SM from the HLR. This prevents SMS MO spoofing and only applies to MO Proxy.

GCP (H.248) Support

This feature adds ITP support for the Gateway Control Protocol (GCP), also known as H.248.1 and Megaco, to be carried over M2PA and M3UA. It also allows the configuration of GCP, BISUP, AAL2 and Satellite ISUP as SI in M3UA AS. It also allows DPC and DPC+SI based M3UA routing.

Large MSU Support on M2PA and M3UA Associations

This feature enables the M2PA and M3UA associations to carry signaling messages with payload sizes of up to 4096 octets. Currently, HSL is the only SS7 link type in ITP that supports sending of 4096 bytes.

Increased Local Port Numbers

This feature increases the number of SCTP ports supported by the platform from 100 to 1,000. This range matches the number of SCTP associations supported by the total platform. The restrictions of 100 SCTP associations and ports per a single processor remains.

New Hardware Features in Release 12.4(15)SW2

No new hardware features are supported.

New Software Features in Release 12.4(15)SW2

The following new software features are supported:

- [Support for Applying ANSI SLS Rotation to MSUs from M3UA/SUA ASPs](#)
- [MLR Concatenated SMS Option](#)
- [MLR MAP Error Return](#)
- [GSM MAP Version Check In](#)
- [MLR Update Location for IMSI Blacklist](#)
- [MLR Instance Conversion](#)
- [Circular Route Detection](#)
- [Support for the cs7 xua-err-diag-fmt Command](#)

Support for Applying ANSI SLS Rotation to MSUs from M3UA/SUA ASPs

This feature adds a configurable option per M3UA/SUA Application Server (AS) to perform ANSI rotation on incoming MSUs. This feature may significantly improve distribution of data messages originating from M3UA and SUA ASPs with a non-distributed SLS range.

In ANSI networks, a node performs SLS rotation before transmitting an MSU over MTP3 links by modifying the SLS field in the MSU. The modification shifts the lower 5 bits to the right and moves the first bit to the fifth bit. This is described in GR-246, Section T1.115.1 Chapter 7.

For example, the SLS value X7 X6 X5 X4 X3 X2 X1 X0 is changed to X7 X6 X5 X0 X4 X3 X2 X1

Some M3UA and SUA ASPs may not perform SLS rotation prior to sending an MSU to an ITP Signalling Gateway (SG), and may use their own schemes for loadsharing between multiple SG associations.

This enhancement adds a configurable option per AS to perform ANSI rotation on incoming messages before outgoing link and linkset selection.

The option is available to shift the SLS by more than 1 bit position. For example, if "rotate-sls 4" is selected, then the ITP will shift the SLS link this:

X7 X6 X5 X4 X3 X2 X1 X0 is changed to X7 X6 X5 X3 X3 X1 X0 X4

Note that unlike the sls-shift option in ITU, this option actually changes the field in the MSU that will be transmitted.

MLR Concatenated SMS Option

MLR supports directly routing SMS-MO messages that are concatenated at the SMS layer.

MLR MAP Error Return

MLR supports the option of returning a MAP error, instead of silently discarding an MSU message when a block rule is matched. You can configure a specific return cause with the MLR rule.

GSM MAP Version Check In

MLR supports checking the GSM MAP version of the MSU and deciding whether it matches the MAP version specified in a triggered MLR rule. You can specify one or several MAP versions in the MLR rule.

MLR Update Location for IMSI Blacklist

MLR supports performing specific actions, such as returning a MAP error, for UpdateLocation MSUs from specific subscribers. These specific subscribers are identified by the originator IMSI. This feature can be used to block fraudulent activity.

MLR Instance Conversion

MLR converts an MSU instance to another instance.

Circular Route Detection

Circular Route Detection (CRD) detects circular routing and disables problematic routes. Circular routing is when an MSU flows through an SS7 network and ends up back at the originating point code (OPC). Circular routes can quickly lead to congestion of links and degrade network performance.

Support for the `cs7 xua-err-diag-fmt` Command

The `cs7 xua-err-diag-fmt` command modifies the format of the diagnostic info parameter in outbound M3UA and SUA ERR messages.

New Hardware Features in Release 12.4(15)SW1

No new hardware features are supported by the Cisco IOS Release 12.4(15)SW1.

New Software Features in Release 12.4(15)SW1

The following new software features are supported in Cisco IOS Release 12.4(15)SW1:

- [Accounting Support for xUA and Virtual Linkset](#)
- [Support for 16 Application Server Processes \(ASPs\) per Application Server \(AS\)](#)
- [Support for GTT Inter-Instance](#)
- [Support for the `cs7 mtp3 rct-opc-from-tfc` Command](#)
- [Support for TTC Variant Conversion](#)

Accounting Support for xUA and Virtual Linkset

In Cisco IOS 12.4(15)SW1 and later releases, Cisco ITP supports accounting for the combination of M3UA and SUA functionality (xUA). This feature applies the existing linkset-based accounting to xUA AS use. Accounting is also provided for virtual linksets between instances.

Support for 16 Application Server Processes (ASPs) per Application Server (AS)

In Cisco IOS 12.4(15)SW1 and later releases, Cisco ITP supports 16 ASPs per AS.

Support for GTT Inter-Instance

In Cisco IOS 12.4(15)SW1 and later releases, Global Title Translation (GTT) Inter-Instance support enhances Cisco ITP's capability of routing MSU inter-instance based on global title when configuring instance conversion after GTT. This allows Cisco ITP to use the GTT process on an MSU in one instance and send it to another instance for subsequent GTT processing. The feature also addresses inter-instance looping prevention.

Support for the `cs7 mtp3 rct-opc-from-tfc` Command

In Cisco IOS 12.4(15)SW1 and later releases, Cisco ITP provides the ability to configure the operation of sending Rangeset Congestion Test (RCT) messages to use the destination point code (DPC) found on the last received TFC as the source for the Origin Point Code (OPC) on the next RCT procedure. By default, Cisco ITP uses its local point code as the OPC parameter on an RCT.

Support for TTC Variant Conversion

In Cisco IOS 12.4(15)SW1 and later releases, Cisco ITP provides MTP3/SCCP conversion ability between TTC and ANSI/ITU variants. A similar conversion between ITU and ANSI is already supported.

New Hardware Features in Release 12.4(15)SW

There are no new hardware features supported in Cisco IOS Release 12.4(15)SW.

New Software Features in Release 12.4(15)SW

The following new software features are supported by the Cisco 7200 and Cisco 7301 series routers for Cisco IOS Release 12.4(15)SW:

- [Enhanced MLR Modification CdPA \(and CgPA\)](#)
- [Enhancing GTT Address Conversion Flexibility](#)
- [Extending the Application Group to 64 Entries per Group](#)
- [Extending the Application Group to 64 Entries per Group](#)
- [Saving, Loading, and Non-Disruptive Replacement of a GWS Configuration or GWS Table to a Remote or Local File](#)

- [Saving, Loading, and Non-Disruptive Replacement of an MLR Configuration to a Remote or Local File](#)
- [Translation Type \(TT\) Modification within an Application Group](#)
- [TTMAP support for xUA AS](#)

Enhanced MLR Modification CdPA (and CgPA)

This feature allows Multi Layer Routing (MLR) to modify the Signaling Connection Control Part (SCCP) called party address (CdPA) global title (GT) selector and digits prior to routing to the specified result. MLR modifies the SCCP CdPA PC and subsystem number (SSN) using a modification profile. MLR modifies the SCCP CdPA via modify-profile for all MAP-based operations. MLR expands its SCCP calling party address (CgPA) modification to be applied to all MAP-based operations

Enhancing GTT Address Conversion Flexibility

Global title translation (GTT) address conversion allows the operator to specify the number of digits removed from the original address prefix when the in-address prefix is matched. GTT address-conversion supports 0 digits for the update in-address parameter. The supported range today is between 1 and 15 digits. The range of digits removed may be between 0 and 15 digits, and has no relation to the number of digits specified in the in-address parameter.

Extending the Application Group to 64 Entries per Group

This feature extends the limit of eight global title translation (GTT) application group members per application group to 64 application group members. The composition of the application group supports the range of 64 members with the same cost value and 64 members with unique cost values.

MLR Routing to M3UA AS without Modifying the DPC

This feature gives Multi Layer Routing (MLR) the ability to route a received packet to an MTP3 User Adaptation Layer (M3UA) application server (AS) without modifying the Destination Point Code (DPC). This is not a message signal unit (MSU) copy feature, but a modification to the routing of the received MSU.

Saving, Loading, and Non-Disruptive Replacement of a GWS Configuration or GWS Table to a Remote or Local File

In Cisco IOS Release 12.4(15)SW and later releases, you can save a Gateway Screening (GWS) table or a general GWS configuration to a local or remote file system, load the general configuration from a local or remote file system, and non-disruptively replace the running GWS configuration or GWS table on an operational system.

The GWS table file is made up of a number of table entries. The general GWS configuration file is made up of action sets, table sub mode commands, linkset table, AS table and global table.

Saving, Loading, and Non-Disruptive Replacement of an MLR Configuration to a Remote or Local File

In Cisco IOS Release 12.4(15)SW and later releases, you can save the general Multi Layer Routing (MLR) configuration to a local or remote file system, load the general configuration from a local or remote file system, and non-disruptively replace the running MLR configuration on an operational system.

The general MLR configuration file includes MLR global result groups, loading MLR address table command, MLR rule sets, MLR modify profiles, routing tables. Individual MLR address tables may still be saved to separate files, but the load statements are included in the general MLR configuration file.

Translation Type (TT) Modification within an Application Group

Global title translation (GTT) currently allows post-translation modification of the TT on a per-global title address (GTA) basis, unless the result type is an application group. This feature allows post-translation modification of the TT on a per application group member basis.

TTMAP support for xUA AS

Mapping the called party address (CdPA) TT to a configured value is supported for all message signal units (MSUs) being sent or received over a particular linkset. This feature extends configured CdPA TT modification to all MSUs being sent or received over a particular MTP3 User Adaptation Layer (M3UA) or SCCP User Adaptation (SUA) application server (AS).

New Hardware Features in Release 12.4(11)SW3

There are no new hardware features supported in Cisco IOS Release 12.4(11)SW3.

New Software Features in Release 12.4(11)SW3

There are no new software features supported in Cisco IOS Release 12.4(11)SW3.

New Hardware Features in Release 12.4(11)SW2

There are no new hardware features supported in Cisco IOS Release 12.4(11)SW2.

New Software Features in Release 12.4(11)SW2

The following new software features are supported by the Cisco 7200 and Cisco 7301 series routers for Cisco IOS Release 12.4(11)SW2:

- [Enhanced Loadsharing](#)
- [Integrated GWS and MLR Triggers](#)

Enhanced Loadsharing

The Enhanced Loadsharing feature creates a 3-bit hash from a subset of bits (6 each) taken from the Originating Point Code (OPC) and Destination Point Code (DPC). Concatenating this hash with the SLS yields a 7-bit value that is then used to select a link (SLC) from a 128 entry SLS->SLC mapping table. This results in a much more even load distribution among available links.

The feature also allows flexibility in choosing the subset of bits from the OPC and DPC using the `opc-shift` and `dpc-shift` parameters and simultaneous configuration of `sls-shift`, at the global and/or linkset level.

Integrated GWS and MLR Triggers

In Cisco IOS 12.4(11)SW2 and later releases, Multi Layer Routing (MLR) triggers and Gateway Screening (GWS) are integrated. GWS determines which packets are intercepted by MLR. You can configure MLR triggers using the GWS infrastructure, GWS tables, and MLR variables.

New Hardware Features in Release 12.4(11)SW1

There are no new hardware features supported in Cisco IOS Release 12.4(11)SW1.

New Software Features in Release 12.4(11)SW1

There are no new software features supported in Cisco IOS Release 12.4(11)SW1.

New Hardware Features in Release 12.4(11)SW

There are no new hardware features supported in Cisco IOS Release 12.4(11)SW.

New Software Features in Release 12.4(11)SW

The following new software features are supported by the Cisco 7200 and Cisco 7301 series routers for Cisco IOS Release 12.4(11)SW:

- [C-Link Backup Routing of M3UA/SUA Traffic](#)
- [GWS SCCP Error Return](#)
- [MLR SCCP Error Return](#)
- [Multiple HSL PVCs per Physical ATM interface](#)
- [SCCP/MAP Address Modification for SRI-SM Messages](#)

C-Link Backup Routing of M3UA/SUA Traffic

Cisco IOS Release 12.4(11)SW supports a C-link Backup Routing feature that provides backup routing to MTP3 User Adaptation Layer (M3UA) and SCCP User Adaptation (SUA) application servers (ASs). It uses a Message Transfer Part Level 3 (MTP3)/M2PA linkset to a remote signaling gateway (SG) serving the same ASs over Stream Control Transmission Protocol (SCTP)/IP. This configurable software

feature is available to any IP Transfer Point (ITP) running a sigtran protocol (M3UA and/or SUA) and offloaded MTP3. The remote SG that is reachable through the C-link may be another ITP, or any SG serving the same ASs.

GWS SCCP Error Return

Cisco IOS Release 12.4(11)SW allows you to configure Gateway Screening (GWS) to return a unitdata service (UDTS) to the source of the Signaling Connection Control Part (SCCP) packet when the SCCP packet is dropped. You configure a return UDTS when you define the gateway screening action set in enhanced GWS.

MLR SCCP Error Return

Cisco IOS Release 12.4(11)SW allows you to configure Multi Layer Routing (MLR) to return a unitdata service (UDTS) to the source of the Signaling Connection Control Part (SCCP) packet when the SCCP packet is blocked. You configure this by specifying an optional `sccp-error` parameter on block results in MLR rules and MLR address tables.

Multiple HSL PVCs per Physical ATM interface

Cisco IOS Release 12.4(11)SW allows multiple High Speed Link (HSL) permanent virtual circuits (PVCs) per physical Asynchronous Transfer Mode (ATM) interface. This is done through the support of subinterface configuration on the ATM link. Prior to Cisco IOS Release 12.4(11)SW, you could only configure the ATM interface, not any subinterfaces. The ability to create additional subinterfaces allows for more qssals, since only one qssal is allowed per interface or subinterface.

SCCP/MAP Address Modification for SRI-SM Messages

Cisco IOS Release 12.4(11)SW permits Signaling Connection Control Part (SCCP) and MAP address modification using a Multi-Layer Routing (MLR) **modify-profile**. MLR currently supports modifying only the service center address (`orig-smsc`) and the calling party address (`CgPA`) for SRI-SM messages.

With Cisco IOS Release 12.4(11)SW, the user can also now optionally configure the desired action for failed modifications using the **modify-failure** command within the MLR options submode. A user can also configure the **preserve-opc** function within the global MLR options submode. The **preserve-opc** function retains the original Originating Point Code (OPC). The user may configure MLR to return a unitdata service (UDTS) to the source of the SCCP packet when the SCCP packet is blocked by specifying an optional **sccp-error** parameter on block results.

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

Caveats for Cisco IOS Release 12.4(15)SW

Caveats describe unexpected behavior in Cisco IOS software releases.



Note

If you have an account with Cisco.com, you can also use the Bug Toolkit to find select caveats of any severity. To reach the Bug Toolkit, **log in** to Cisco.com and click **Service and Support: Technical Assistance Center: Select & Download Software: Jump to a software resource: Software Bug Toolkit/Bug Watcher**. Another option is to go to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl.

Open Caveats—Cisco IOS Release 12.4(15)SW3

This section documents possible unexpected behavior by Cisco IOS Release 12.4(15)SW3 and organizes caveats by the level of severity.

Moderate

- CSCsy73811

Symptom The following two issues occur on ITP which is configured with AS and C-link:

- When C-link and AS are both available, the C-link route status is displayed as restricted. The expected C-link status is available.
- When the AS becomes active/inactive, the C-link route status can not be updated.

Conditions These issues occur, when ITP is configured with AS and C-link, and **national-options TFR** is configured.

Workaround There is no known workaround.

Resolved Caveats—Cisco IOS Release 12.4(15)SW3

All the caveats listed in this section are resolved in Cisco IOS Release 12.4(15)SW3. Caveats are organized by the level of severity

Severe

- CSCsv49949

Symptom An ITP Signaling Gateway may reload due to an invalid memory address:

Address Error (load or instruction fetch) exception, CPU signal 10, PC = 0x41DD69B0

Conditions An ITP reload occurs in the following scenario:

- cs7 is configured with mapua clients.
- SMPP sends unbind message to MAPUA while HLR return message. ITP will free the SMPP client data structure immediately without freeing the HLR transaction until a timer (1second) process is called. MAPUA will use the transaction to refer the invalid SMPP client, then ITP reloads.

Workaround There is no known workaround.

Moderate

- CSCsq31776

Cisco devices running affected versions of Cisco IOS Software are vulnerable to a denial of service (DoS) attack if configured for IP tunnels and Cisco Express Forwarding. Cisco has released free software updates that address this vulnerability. This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20090923-tunnels.shtml>.

- CSCsv95510

Symptom ITP eventually reloads when the SCTP local receive window for an association decreases to zero.

Conditions If ITP is forced to hold packets in its receive queue because of out of order packets, the local receive window decreases for each packet that is held. If the remote node continues to send new packets instead of the missing packets (which is causing the ITP to hold packets), the local receive window will eventually decrease to zero. Once the ITP local receive window decreases to zero and the remote node continues to send new packets, the ITP tries to handle the newly arrived packets and eventually crashes.

Workaround There is no known workaround.

- CSCsw20012

Symptom Packet loss may occur during an M2PA link changeover, even at low MSU rates.

Conditions An M2PA link fails that is part of a multi-link linkset, for which normal MTP3 changeover should succeed. The MSU rate of traffic carried over the failed link does not exceed 40% of the maximum supported data rate given the protocol, processor, release and supported features such as GTT, MLR, GWS, etc.

Workaround There is no known workaround.

- CSCsw20980

Symptom The following MIB issues were found for HSL, M2PA link types:

- Link level MIB measurements are pulled from incorrect memory locations for HSL and M2PA link types.
- The following link level measurements are not implemented for HSL link type.
 - rx_cong_onset (rx congestion onset count)
 - tx_cong_level1 (tx congestion level1 count)
 - tx_cong_level2 (tx congestion level2 count)
 - tx_cong_level3 (tx congestion level3 count)
 - tx_cong_level4 (tx congestion level4 count)
 - retx_pkts_count (retransmit packet count)
 - retx_byte_count (retransmit packet byte count)
 - align_proving_fail_cnt (total alignment and proving failure count)
 - proving_fail_cnt (proving failure count (T2 timeout))
 - tx_pkts_retrieved (tx packet retrieved during changeover)
 - MTP2 link level retransmission MIB counts were incorrect.
- MTP2 clear commands also cleared bytes, msus, lssus etc.
- Retransmission mib measurements were not preserved after a clear command.

Conditions These issues apply to ITP usage with HSL MTP2 link types.

Workaround There is no known workaround.

- CSCsw23706

Symptom ITP sent incorrect AS traffic-mode parameters in the SNMP data to the SNMP server.

Conditions In AS submode, if the end user configures traffic-mode as the following value, then incorrect traffic-mode value is sent to the SNMP server via the SNMP data:

- traffic-mode loadshare bindings CIC
- traffic-mode loadshare bindings SLS
- traffic-mode loadshare bindings redistribute-active
- traffic-mode loadshare bindings CIC redistribute-active
- traffic-mode loadshare bindings SLS redistribute-active

Workaround There is no known workaround.

- CSCsw31173

Symptom ITP routes the MSU back to the same linkset when receiving TFP from XUA point code.

Conditions When the ITP begins routing to a destination over a linkset, it sends a TFP concerning that destination over the linkset to prevent circular routing. If the adjacent node ignores the TFP and sends traffic for that destination to the ITP over that linkset, the ITP should drop the MSUs instead of routing them back out the same linkset.

If the OPC is an XUA point code, the ITP does not drop the MSU but routes it back out the same linkset.

Workaround There is no known workaround.

- CSCsx71762

Symptom The `cs7 gtt map sp available` command is not applicable for changing the M3UA/SUA point code state.

Conditions N/A

Workaround Disable this command from M3UA/SUA to avoid the confusion from user.

- CSCsy31047

Symptom C-link is configured between ITPA and ITPB. ITPA and ITPB both configure AS point to the same SP1.

- Shutdown AS for SP1 in ITPA, ITPA send TFP to ITPB over C-link to indicate the Restriction of C-link
- After ITPB T10 expires, ITPB sends RST to ITPA.
- ITPA returns TFA to ITPB, hence in ITPB, route status to SP1 via c-link is available.

This behavior is not correct, according to the ITU Q.704 section:13.5.4. ITPA should not return any message to ITPB for RST because ITPA has no other available route to SP1 except via C-link.

Conditions The issue occurs when the c-link is configured between two ITPs and the `cs7 instance X national-options TFR` is enabled.

Workaround The TFA against RST in C-link is disabled with the command `cs7 instance X national-options TFR`

Open Caveats—Cisco IOS Release 12.4(15)SW2

This section documents possible unexpected behavior and organizes caveats by the level of severity.

There are no new open caveats.

Resolved Caveats—Cisco IOS Release 12.4(15)SW2

All the caveats listed in this section are resolved in this release. Caveats are organized by the level of severity

Severe

- CSCso92582

Symptom When configuring the ATM IMA E1 port adapter, the **national reserve** command is not effective after a Line Card reload or OIR.

Conditions This issue only occurs for the **national reserve** command when the linecard is reloaded or OIR.

Workaround The **national reserve** command becomes effective by removing the **national reserve** command and then reconfiguring the **national reserve** command.

- CSCsq34722

Symptom An ITP Signaling Gateway may reload due to the following watchdog event:

```
%SYS-2-WATCHDOG: Process aborted on watchdog timeout, process = CS7 SCCP Process.
```

Conditions ITP is configured as a Signalling Gateway with active M3UA or SUA ASPs, and one or more ASP's SCTP associations are changing state. The probability for hitting the reload increases with the increase of ASP SCTP association state transitions, but the reload scenario is extremely rare.

Workaround There is no known workaround.

- CSCsr54357

Symptom A memory leak on the ingress linecard for M3UA/sua traffic is caused by closing the SGMP association.

Conditions This occurs with the following conditions:

- ITP is forwarding offloaded M3UA/sua traffic to AS's configured with traffic mode = loadshare bindings.
- SGMP is enabled.
- The concerned ITP is not the ASP binding manager.

Workaround You can prevent the problem with one of the following actions:

- Stop all the M3UA/SUA traffic before closing the SGMP association.
- Disable the SGMP.
- Change the AS traffic mode to loadshare roundrobin.

- CSCsu22093

Symptom MTP2 links fail and do not recover.

Conditions At least one MTP2 link is configured on a T1 controller, but the controller state is down and link(s) are not shutdown. In addition, some number of MTP2 links must also be configured on the same PA, active on another T1 controller and running traffic at 50% link occupancy. Link failures began after about 1 hour, and links do not recover.

Workaround There is no known workaround.

Moderate

- CSCso05935

Symptom ITP PA-MCX-8TE1-M and PA-MCX-4TE1-Q E1 controller ports configured with clock source bits primary are in the down state following a reload on the Cisco 7600 platform.

Conditions After a reload, the **show controller** output for the affected E1 controller ports indicates 'Receiver has remote alarm'. The state of the remote controller ports on the remote device is in the up state with no alarm indication.

Workaround Execute the **shut** command on the affected controller, followed by the **no shut** command or remove and insert the cable connected to the affected port.

- CSCso13465

Symptom MLR may not route an MSU to the specified point code (PC) destination when using a post GTT trigger. For PostGTT MLR, If the matched rule is result to PC, mlr won't be able route the packet to that pc, instead MLR will change the dpc in the packet to that pc and use gtt table route the packet out.

Conditions When MLR is configured to trigger in a post GTT gateway screening table and the expected MLR result is a PC, the MSU will not be routed properly if one of these two conditions also exist:

- The GTT translation specified an M3UA or SUA AS name as the destination.
- The GTT translation performed instance conversion.

Workaround Change the configuration to allow MLR to trigger before the GTT translation is performed.

- CSCso39717

Symptom Traceback occurs when sending SCCP MSUs to a broadcast Application Server (AS) on a Cisco 2600 platform.

%CS7MTP3-7-INTERR: Internal Software Error

Conditions When sending SCCP MSUs to an AS, which is configured with broadcast traffic mode, there is a traceback.

Workaround There is no known workaround.

- CSCso85835

Symptom Global Title Translation (GTT) tries to route packets to an Application Server (AS) Point Code (PC) that should not have been used since the M3UA/SUA AS is unavailable. The following GTT error messages are seen in the log and indicate that the routing to the PC failed.

```
%CS7SCCP-5-SCCPGNRL: SCCP error sending via M3UA/SUA.
```

Conditions The issue occurs if a virtual summary route exists via another instance which matches the PC of the AS routing key. In this case, the SCCP audit sets the GTT map state of the PC to available since a summary route exists. However, routing will not allow the use of summary routes when using an XUA pc routing key.

Workaround Configure the GTT directly routed to the AS name rather than the PC.

- CSCsq02307

Symptom The **show gws linkset** command fails and gives the following error message:

```
%Error: Linkset Name can not exceed length of 19
```

Workaround Reduce the length of the linkset name to under 19 characters.

- CSCsq14771

Symptom The ITP attempts to route messages after GTT to an unavailable AS PC. GTT error messages similar to the following are observed on the console:

```
*May 7 20:10:46.671 MSK: %CS7SCCP-5-SCCPGNRL: May 7 2008 20:10:46 : SCCP error sending via M3UA/SUA. Instance: 0 MsgType udt LS: VirtualLS7-6 OPC: 0.0.18 CgPA: tt 9 gta 99881234 ssn 32 DPC: 0.62.71 CdPA: tt 1 gta 12345670 ssn 32
```

Conditions The problem can occur if all of the following conditions hold:

- The GTT to an AS PC is configured.
- The AS PC is unavailable.
- A default route is configured where the AS PC is a member of the default route.

Workaround Update the GTT configuration to route to the AS name rather than the AS PC.

- CSCsq26326

Symptom When using the Multi-Layer Routing (MLR) feature of the ITP, routing toward selected Point Code (PC) members of an MLR result group may occur when the destination PC is congested.

Conditions - MLR result group PC member is selected and congested to a level where MSUs should be dropped when routing toward the MSU.

This problem is more likely to occur on a single processor router platform, such as the Cisco 2811, Cisco 7301, or Cisco 7200 series.

Workaround There is no known workaround.

- CSCsq77114

Symptom The **cs7 save mlr all** command cannot save the updated MLR address-tables to a slave disk.

Workaround Manually save the address table instead of using **cs7 save mlr all** command.

- CSCsq84291

Symptom ITP failed to transmit an XUDT message and displayed the following error message:

SCCP encoding error, badly formatted or unsupported part

Conditions The received XUDT message's optional portion is placed before the data portion, and the total XUDT message length is larger than 273 bytes.

Workaround Reduce the XUDT message data portion length to less than 255 bytes.

- CSCsr01623

Symptom The MTP2 links remain shutdown after a **shutdown** and then a **no shutdown** was issued for the linkset.

Conditions On a Cisco 2811 platform, a **shut** is issued on a linkset that has MTP2 links. Then the Cisco 2811 reloads and a **no shut** is issued on the linkset. MTP2 links do not come up because the serial interfaces are still down.

On any ITP supported platform, a **shut** is issued on a linkset that has MTP2 links and an existing MTP2 link is deleted. The deleted link is added to the down linkset then a **no shut** is issued on the linkset. The link does not come up because the serial interface is still down.

Workaround The link can be put back into service after a **no shut** is issued for the serial interface

- CSCsr09619

Symptom After a reload of ITP, a series of TFP/TFA messages are exchanged between two ITPs over an xUA C-link regarding an unavailable AS PC.

Conditions This occurs with the following conditions:

- The Japan TTC variant is configured.

- An xUA C-link route is configured on both ITPs.
- The AS is unavailable on both ITPs.

Workaround There is no known workaround.

- CSCsr58145

Symptom For up to several minutes after an SGMP SCTP association fails, the 7600 Supervisor CPU is processing at almost 100% capacity.

Conditions The problem occurs under the following conditions:

- SGMP is configured between two ITPs.
- A loadshare bindings AS is configured on both ITPs.
- Over a thousand ASP bindings exist on the ITPs.

Workaround There are two possible workarounds:

- Use xUA C-link routes rather than SGMP for redundancy.
- Configure **loadshare roundrobin** rather than **loadshare bindings** for the AS traffic-mode.

Minor

- CSCsr25825

Symptom An M3UA/SUA PC is incorrectly displayed as active after the reload of an ITP in a mated pair configuration.

Conditions The problem occurs under the following conditions:

- A variant that does not support TFR messages is configured.
- An M3UA/SUA AS is configured on two ITPs and is not active on either ITP.
- A C-link route for the M3UA/SUA AS PC is configured on both ITPs.
- Both ITP nodes are isolated (i.e. no links except for the C-link are available on both ITPs). After reloading one of the ITPs in the mated-pair, the M3UA/SUA AS PC is incorrectly displayed as active on both ITPs.

Workaround You can work around the problem by configuring the cs7 national-options TFR command and ensuring that at least one of the ITPs is not isolated. For example, the ITP has an available link other than the C-link.

Open Caveats—Cisco IOS Release 12.4(15)SW1

This section documents possible unexpected behavior by Cisco IOS Release 12.4(15)SW1 and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCsk60020

The Secure Shell server (SSH) implementation in Cisco IOS contains multiple vulnerabilities that allow unauthenticated users the ability to generate a spurious memory access error or, in certain cases, reload the device.

The IOS SSH server is an optional service that is disabled by default, but its use is highly recommended as a security best practice for management of Cisco IOS devices. SSH can be configured as part of the AutoSecure feature in the initial configuration of IOS devices, AutoSecure run after initial configuration, or manually. Devices that are not configured to accept SSH connections are not affected by these vulnerabilities.

Common Vulnerabilities and Exposures (CVE) identifier CVE-2008-1159 has been assigned to this bug.

The Security Advisory for this issue is posted at

<http://www.cisco.com/warp/public/707/cisco-sa-20080521-ssh.shtml>.

- CSCso00287

The SUP processor on a distributed Cisco ITP platform or the Route Processor (RP) on a single processor Cisco ITP platform exceeds the normal CPU operating range even with light traffic.

This problem occurs when the Enhanced Gateway Screening (GWS) console logging is turned on for all received/sent packets.

Workaround: Turn off GWS console logging. File logging may be used as an alternative.

- CSCso01412

An ATM IMA port link may not activate after a reload.

```
Router#show cs7 linkset msc-server
lsn=msc-server apc=16258 state=avail avail/links=1/2
SLC Interface Service PeerState Inhib
00 ATM13/1/7 avail -----
*01 ATM13/1/2 FAILED -----
```

This problem occurs when an ATM link does not activate after reload.

Workaround: Execute the **shut** and **no shut** commands, or unplug and plug in the cable. The link should come up.

Resolved Caveats—Cisco IOS Release 12.4(15)SW1

All the caveats listed in this section are resolved in Cisco IOS Release 12.4(15)SW1. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCsg58153

The port adapter (PA) has crashed and is unresponsive

This problem occurs because bad circuits on uplink links cause all the SS7 links to go down and flap continuously.

Workaround: Bring the PA up after it has crashed.

- CSCsk79377

The **remove** option specified in a global title translation (GTT) address conversion table is not applied when performing GTT address conversion.

This problem only occurs when the GTT address conversion table is used for Signaling Connection Control Part (SCCP) conversion across instances when cs7 multi-instance is configured.

There are no known workarounds.

- CSCs108358

SCCP User Adaptation (SUA) Application Server Processes (ASPs) may reject SCCP segmented messages from an ITP SUA Signaling Gateway (SG).

This problem occurs because the segmentation parameter in SUA CLDT messages is populated incorrectly when the sequence delivery option is set to '1'b (Class 1) in the received SCCP XUDT segmentation parameter. In this case, bit 7 within the first/remain field of the SUA segmentation parameter is also set, which may cause the ASP to interpret the number of remaining segments to be greater than 15.

There are no known workarounds.

- CSCs159128

Cisco ITP does not reject m3ua/sua messages without a Routing Context parameter when the ASP is active in multiple AS's.

This problem occurs when the sending ASP is active in multiple AS's.

There are no known workarounds.

- CSCs193462

No linkUp and linkDown Simple Network Management Protocol (SNMP) traps are generated when the remote end is down for the controller. No linkUp trap generated when the controller is brought up by **no shutdown** command.

This problem is specific to the PA-MCX-8TE1-M and PA-MCX-4TE1-Q port adapters.

There are no known workarounds.

- CSCsm76092

If the default conversion is removed with the real and alias instance swapped in the **cs7 instance** command, then reentered, the FlexWan is not updated, and the PC is not converted.

For example:

```
Router(config)#cs7 instance 1 pc-conversion default 0
Router(config)#no cs7 instance 0 pc-conversion default 1
Router(config)#cs7 instance 0 pc-conversion default 1
%Error: Default conversion already defined for instance 0
```

```
Rrouter(config)#cs7 instance 1 pc-conversion default 0
%Error: Alias PC 0.0.0:0 already in use
```

This problem occurs when ITP has multiple instances configured and default instance conversion configured.

Workaround: Enter the default conversion with the **no-route** option:

```
Router(config)#cs7 instance 0 pc-conversion default 1 no-route
```

- CSCso12698

When a set of links are quickly shut and then removed, as with a cut and paste of a prepared script into the console terminal, the ITP software can crash. The crash traceback is not predictable or fixed.

A cut and paste of a script similar to the one below can result in a crash:

```
Router(config)#cs7 linkset linksetname
Router(config-cs7-ls)#link 1
Router(config-cs7-ls-link)#shut
Router(config-cs7-ls-link)#no link 1
Router(config-cs7-ls-link)#link 2
```

```

Router(config-cs7-ls-link)#shut
Router(config-cs7-ls-link)#no link 2
...
Router(config-cs7-ls-link)#end

```

Workaround: Do not remove links using a cut and paste of a script. Wait 4 to 5 seconds after shutting a link before issuing the **no link** command.

Open Caveats—Cisco IOS Release 12.4(15)SW

This section documents possible unexpected behavior by Cisco IOS Release 12.4(15)SW and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCsd34549

An unexpected config_state value is seen during reload or switchover.

This issue is seen after an IMA card reloads or switches over.

There are no known workarounds
- CSCsd73254

If a specific software error on the active Route Processor (RP) causes the active RP to fail, the standby SUP may not detect the failure. Instead, the active SUP may reload the ITP to restore ITP manageability.

This issue has only been observed in specific lab tests that force a specific software failure on the active RP.

There are no known workarounds.
- CSCsh35975

A Bad VCD message occurs when the following actions are performed:

 - Shut the main interface and its subinterfaces that are used in links
 - No shut the main interface, but keep the subinterfaces shut

Traffic on the other links and subinterfaces does not seem to be affected.

There are no known workarounds.

Resolved Caveats—Cisco IOS Release 12.4(15)SW

All the caveats listed in this section are resolved in Cisco IOS Release 12.4(15)SW. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCek63758

Message signal unit (MSU) rates spike after clearing counters.

This problem occurs on all ITP platforms

There are no known workarounds.
- CSCse11887

An IPCALLOCFAIL error occurs during online insertion and removal (OIR) of a FlexWAN module.

This issue occurs intermittently during FlexWAN OIR.

- There are no known workarounds.
- CSCsf10777

An ATMPA-3-CMDFAIL can occur when you extract the FlexWAN module from the chassis. This issue only occurs when the FlexWAN module contains an E1 IMA PA and the FlexWAN module is extracted from the chassis. Once the FlexWAN module is reinserted, no additional symptoms occur.

There are no known workarounds if the FlexWAN module is extracted.
 - CSCsg27676

The Signaling Gateway Mate Protocol (SGMP) link between ITP mates flaps when an Application Server Process (ASP) becomes active.

This problem occurs on all ITP platforms.

There are no known workarounds.
 - CSCsg58153

The PA crashes and is unresponsive.

This issue occurs because bad circuits on uplink links cause all the SS7 links to go down and flap continuously.

Workaround: Bring the PA up after it has crashed.
 - CSCsh33248

Traceback similar to the following is observed:

```
%FIB-4-FIBNULLIDB: Missing idb for fibidb ATM4/1/0.1 (if_number 76).
-Traceback= 40603CD0 413473C8 4134867C 40C9CFB0 40CA08FC 40CA177C
%FIB-4-FIBNULLIDB: Missing idb for fibidb ATM4/1/0.1 (if_number 76).
-Traceback= 40603CD0 4133485C 41334990 4132A58C 4132AB68 4132E490 4132C5FC
%FIB-SP-STDBY-4-FIBXDRINV: Invalid format. invalid if_number
%CEF: fibidb ATM4/1/0.1(76) has no idb
```

This issue occurs in a multi-PVC configuration after a switchover, and may be caused by configuration of a non-existent subinterface.

Workaround: Do not unconfigure a non-existent subinterface.
 - CSCsh69956

Syslog messages and Simple Network Management Protocol (SNMP) traps are not generated for clock transitions on the PA-A3-8T1IMA

This problem occurs on all ITP platforms

There are no known workarounds.
 - CSCsi34398

When unconfiguring and reconfiguring OC3 ATM interfaces and associated linksets with the multi-PVC feature, including a subinterface and IP protocol, the system may reload unexpectedly.

Some conditions that can cause this problem include configuring and unconfiguring subinterfaces, the IP protocol, and ATM NNI.

Workaround: Avoid configuring and unconfiguring the OC3 ATM interface multiple times. Once the system is configured, it remains stable.
 - CSCsi40918

The Route Switch Processor (RSP) crashes causing a switchover to the standby RSP.

This crash occurs during normal router operations.

There are no known workarounds.

- CSCsi60319

The Multimedia Message Service Center (MMSC) gateway feature of the ITP is not returning the responding Home Location Register (HLR) E.164 address to the Short Message Peer-to-Peer (SMPP) client when the HLR responds with an ERROR or REJECT component.

This problem only affects the MMSC gateway feature when clients submit a GetIMSI request and an HLR responds with an error.

There are no known workarounds.

- CSCsi64297

A Versatile Interface Processor (VIP) crashes while processing global title translation (GTT) traffic.

This issue occurs when Message Transfer Part Level 3 (MTP3) offload is enabled with a VIP performing GTT on both UDT and XUDT SCCP messages.

There are no known workarounds.

- CSCsi68966

The Signaling Connection Control Part (SCCP) fails to route messages to XUA PCs even though they are available.

This problem is timing related and only occurs on a reboot of the entire system or card.

Workaround: The global title address (GTA) entered in the configuration should point to application server (AS) name directly instead of a PC.

- CSCsi79035

The MTP3 User Adaptation Layer (M3UA) Application Server Process (ASP) multi-homing test fails when one interface is disconnected even though there are multiple local-ip addresses configured on multiple interfaces. The output of the **show ip sctp instance** shows only one local-ip address when it should show two.

This issue occurs when M3UA ASPs have local-ip addresses from different FlexWANs, and only one IP address is used by the Stream Control Transmission Protocol (SCTP) instance.

Workaround: Perform a **shutdown** and **no shutdown** of the affected M3UA instance to clear the problem. The output of the **show ip sctp instance** command should now show two local-ip addresses.

- CSCsi98081

A buffer leak occurs because of a large quantity of Simple Network Management Protocol (SNMP) traps.

This problem occurs on all ITP platforms.

There are no known workarounds.

- CSCsj36934

The router crashes with the following bus error: *System returned to ROM by bus error at PC 0x4107D360 TLB (load or instruction fetch) exception, CPU signal 10, PC = 0x4107D360*

This issue occurs during normal operations.

There are no known workarounds.

- CSCsj60899

FlexWAN crashes while processing outbound MTP3 User Adaptation Layer (M3UA) Signaling Connection Control Part (SCCP) message signal unit (MSU) Extended Unitdata (XUDT).

ITP may experience a LC crash while processing an XUDT SCCP message that is routed to an M3UA destination. The XUDT must contain the optional importance parameter.

There are no known workarounds.

- CSCsj99422

A new Application Server Process (ASP) binding during a Non-Stop Operation (NSO) bulk sync causes a SYNCERR.

This issue occurs during an NSO switchover on an ITP running MTP3 User Adaptation Layer (M3UA)/SCCP User Adaptation (SUA) traffic.

There are no known workarounds.

- CSCsk15118

ITP crashes while performing Signaling Connection Control Part (SCCP) instance address conversion.

This issue occurs when the following three conditions occur:

- SCCP instance conversion where address conversion is used between instances
- A message signal unit (MSU) with more than 16 digits is in the received called party address
- The called party address does not match an entry in the selected prefix conversion table

Workaround: Ensure that all prefix conversion tables have default entries that match all possible addresses.

For example:

```
cs7 instance 0 gtt address-conversion E164toE164 ...
update in-address 0 out-address 0 update
in-address 1 out-address 1 update
in-address 2 out-address 2 update
in-address 3 out-address 3 update
in-address 4 out-address 4 update
in-address 5 out-address 5 update
in-address 6 out-address 6 update
in-address 7 out-address 7 update
in-address 8 out-address 8 update
in-address 9 out-address 9
```

- CSCsk25247

An ITP MTP2-User Peer-to-Peer Adaptation Layer (M2PA) link stops processing received messages and eventually fails after receiving a Stream Control Transmission Protocol (SCTP) DATA chunk that is 300 bytes or more.

This issue occurs because the DATA chunk is larger than the maximum message signal unit (MSU) size allowed on the link and is discarded as an invalid message before the Forward Sequence Number (FSN) in the M2PA header is updated for the link. As a result, all subsequent messages received over the link will be dropped due to an invalid FSN. The link will eventually fail if a Signaling Link Test Message (SLTM)/Signaling Link Test Acknowledgement (SLTA) is dropped, or when the remote peer can no longer buffer forwarded messages.

Either the **show cs7 m2pa statistics** or the **show cs7 m2pa state** command may be used to identify that this problem is occurring. The **show cs7 m2pa statistics** command will show an elevated number of Unexpected FSN_rcvd errors; the **show cs7 m2pa state** command will show that the 'bsnr' field is not incrementing despite data chunks being received over the association.

Workaround:

- Identify the source of the invalid MSU and prevent it from forwarding the MSU to the ITP.
- Shut/no shut the linkset to recover the affected links. This action, however, will not prevent the problem from re-occurring.

- CSCsk50308

When configuring a Message Transfer Part Level 3 (MTP3) route to an MTP3 User Adaptation Layer (M3UA)/SCCP User Adaptation (SUA) point code, the initial route status is "available" even though the M3UA/SUA point code is locally inactive.

This issue occurs only upon initial route configuration.

Workaround: Perform one of the following actions:

- Bring the M3UA/SUA point code active to match the route availability.
- Execute an MTP3 restart.

- CSCsk56500

The removal of a card leaves the controller configuration intact.

This issue occurs on ITPs only when the **no card type** *tl* or *el* command is issued. The controller configuration remains in the show running-configuration output.

Workaround: Do not issue a **no card type** command. A reload is required to change the card type on all ITP systems.

Open Caveats—Cisco IOS Release 12.4(11)SW3

This section documents possible unexpected behavior by Cisco IOS Release 12.4(11)SW3 and describes only severity 1 and 2 caveats and select severity 3 caveats.

There are no known open caveats for Cisco IOS Release 12.4(11)SW3.

Resolved Caveats—Cisco IOS Release 12.4(11)SW3

All the caveats listed in this section are resolved in Cisco IOS Release 12.4(11)SW3. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCsi68841

After configuring a cs7 group, ITP crashes during normal traffic processing.

There are no known workarounds.

- CSCsj44081

Improper use of data structures occurs in Cisco IOS. The Cisco IOS software has been enhanced with the introduction of additional software checks to signal the improper use of data structures. The %DATACORRUPTION-1-DATAINCONSISTENCY error message is now preceded by a timestamp, and the error message is then followed by a traceback.

There are no known workarounds.

- CSCsj53415

When traffic goes through global title translation (GTT), which results in the traffic going to an xUA application server (AS), but the traffic is blocked by outbound Gateway Screening (GWS), the buffer is lost. Eventually all buffers are exhausted, and the links fail and do not recover. The **show buffers** command displays an extremely large number of cs7 buffers and an extremely large number of misses in the global pool. The cs7 buffers keep increasing until the links fail.

Workaround: To prevent the problem, remove the outbound GWS rule. If the links fail, you must reload the individual line card that contains the inbound links, or reload the entire router.

Open Caveats—Cisco IOS Release 12.4(11)SW2

This section documents possible unexpected behavior by Cisco IOS Release 12.4(11)SW2 and describes only severity 1 and 2 caveats and select severity 3 caveats.

There are no known open caveats for Cisco IOS Release 12.4(11)SW2.

Resolved Caveats—Cisco IOS Release 12.4(11)SW2

All the caveats listed in this section are resolved in Cisco IOS Release 12.4(11)SW2. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCsg11686

ITP sends an SIE instead of an SIN when a failed link is reactivating.

This issue occurs when a linkset has two links and one of the links is brought out of service (for example, as a result of a remote disconnect). Although the linkset status remains "available" when the failed link is re-activated, the ITP sends an SIE instead of an SIN (as shown by the increase of the OMLSSU_XMIT_SIECount by 1 for the failed link in the output of **show cs7 mtp2 statistics** command). Because one link is still available, an SIN should be sent instead of an SIE.

There are no known workarounds.

- CSCsg27676

The Signaling Gateway Mate Protocol (SGMP) link between ITP mates may fail when an Application Server Process (ASP) becomes active.

This issue occurs when an ASP configured for a loadshare bindings Application Server (AS) becomes active, and thousands of ASP bindings exist on the ITP.

There are no known workarounds.

- CSCsh59560

Cisco IP Transfer Point (ITP) running Cisco IOS Release 12.4(11)SW reports the Message Transfer Part Level 3 (MTP3) route as Avail, but the destination is reported as INACC.

This issue occurs during a system boot while processing a large route table because the MTP3 restart may not complete before the mtp3 timers expire. As a result, the system may be in an intermediate state where routes are available but the destination is inaccessible.

Workaround: Reduce the number of routes to 8000 total routes/4000 destinations.

- CSCsh69956

Syslog messages and Simple Network Management Protocol (SNMP) traps are not generated for clock transitions on the Inverse Multiplexing over ATM (IMA) port adapter.

There are no known workarounds.

- CSCsi60319

The responding Home Location Register (HLR) E.164 address is not returned to the Short Message Peer-to-Peer (SMPP) client when handling error responses from an HLR.

This issue only affects the Multimedia Message Service Center (MMSC) gateway feature when clients submit a GetIMSI request and an HLR responds with an error.

There are no known workarounds.

Open Caveats—Cisco IOS Release 12.4(11)SW1

This section documents possible unexpected behavior by Cisco IOS Release 12.4(11)SW1 and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCsh59560

Cisco IP Transfer Point (ITP) running Cisco IOS Release 12.4(11)SW reports the Message Transfer Part Level 3 (MTP3) route as Avail, but the destination is reported as INACC.

This issue occurs during a system boot while processing a large route table because the MTP3 restart may not complete before the mtp3 timers expire. As a result, the system may be in an intermediate state where routes are available but the destination is inaccessible.

Workaround: Reduce the number of routes 8000 total routes/4000 destinations.

Resolved Caveats—Cisco IOS Release 12.4(11)SW1

All the caveats listed in this section are resolved in Cisco IOS Release 12.4(11)SW1. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCec12299

Devices running Cisco IOS versions 12.0S, 12.2, 12.3 or 12.4 and configured for Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs) or VPN Routing and Forwarding Lite (VRF Lite) and using Border Gateway Protocol (BGP) between Customer Edge (CE) and Provider Edge (PE) devices may permit information to propagate between VPNs.

Workarounds are available to help mitigate this vulnerability.

This issue is triggered by a logic error when processing extended communities on the PE device.

This issue cannot be deterministically exploited by an attacker.

Cisco has released free software updates that address these vulnerabilities. Workarounds that mitigate these vulnerabilities are available.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20080924-vpn.shtml>.

- CSCsd85587

A vulnerability has been discovered in a third party cryptographic library which is used by a number of Cisco products. This vulnerability may be triggered when a malformed Abstract Syntax Notation One (ASN.1) object is parsed. Due to the nature of the vulnerability it may be possible, in some cases, to trigger this vulnerability without a valid certificate or valid application-layer credentials (such as a valid username or password).

Successful repeated exploitation of any of these vulnerabilities may lead to a sustained Denial-of-Service (DoS); however, vulnerabilities are not known to compromise either the confidentiality or integrity of the data or the device. These vulnerabilities are not believed to allow an attacker will not be able to decrypt any previously encrypted information.

The vulnerable cryptographic library is used in the following Cisco products:

- Cisco IOS, documented as Cisco bug ID CSCsd85587
- Cisco IOS XR, documented as Cisco bug ID CSCsg41084
- Cisco PIX and ASA Security Appliances, documented as Cisco bug ID CSCse91999
- Cisco Unified CallManager, documented as Cisco bug ID CSCsg44348
- Cisco Firewall Service Module (FWSM)

This vulnerability is also being tracked by CERT/CC as VU#754281.

Cisco has made free software available to address this vulnerability for affected customers. There are no workarounds available to mitigate the effects of the vulnerability.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20070522-crypto.shtml>.



Note

Another related advisory is posted together with this Advisory. It also describes vulnerabilities related to cryptography that affect Cisco IOS. A combined software table for Cisco IOS only is available at <http://www.cisco.com/warp/public/707/cisco-sa-20070522-cry-bundle.shtml> and can be used to choose a software release which fixes all security vulnerabilities published as of May 22, 2007. The related advisory is published at <http://www.cisco.com/warp/public/707/cisco-sa-20070522-SSL.shtml>.

Open Caveats—Cisco IOS Release 12.4(11)SW

This section documents possible unexpected behavior by Cisco IOS Release 12.4(11)SW and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCsh59560

Cisco IP Transfer Point (ITP) running Cisco IOS Release 12.4(11)SW reports the Message Transfer Part Level 3 (MTP3) route as Avail, but the destination is reported as INACC.

This issue occurs during a system boot while processing a large route table because the MTP3 restart may not complete before the mtp3 timers expire. As a result, the system may be in an intermediate state where routes are available but the destination is inaccessible.

Workaround: Reduce the number of routes 8000 total routes/4000 destinations.

Resolved Caveats—Cisco IOS Release 12.4(11)SW

All the caveats listed in this section are resolved in Cisco IOS Release 12.4(11)SW. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

There are no known resolved caveats for Cisco IOS Release 12.4(11)SW.

