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

Current Release—12.4(15)SW9

These release notes describe the enhancements provided in Cisco IOS Release 12.4(15)SW9 and earlier. These release notes are updated as needed. Refer to the Document Revision History. 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 17.

Document Revision History

The following table lists the major changes made to this document during the current release.

Date	Current Release 12.4(15)SW9 Change Summary
16 July 2012	Revision 1.4—Updated resolved caveats
8 November 2011	Revision 1.3—Updated resolved caveats
4 November 2011	Revision 1.2—Updated open caveats
18 October 2011	Revision 1.0

Contents

These release notes include the following topics:

CISCO SYSTEMS

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
- Determining the Software Version, page 2

Supported Platforms and Memory Requirements

Refer to the Cisco ITP data sheet:
https://www.cisco.com/en/US/prod/collateral/wireless/wirelssw/ps1862/product_data_sheet09186a008 00925b1.html

Determining the Software Version

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

New and Changed Information

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

New Hardware Features in Release 12.4(15)SW9

No new hardware features are supported in this release.

New Software Features in Release 12.4(15)SW9

The following new software features are supported:

- Conversion between XUDT/XUDTS and UDT/UDTS, page 2
- ASP Binding Algorithm Enhanced for SCCP Class 2 Traffic, page 3
- Enhanced CLI Statistics and Debugging for EAP-SIM, page 3
- Enhanced MLR "default-rule", page 3
- CLI to Trigger On-Demand Circular Route Detection, page 3

Conversion between XUDT/XUDTS and UDT/UDTS

This feature allows you to modify the SCCP packet header between XUDT/XUDTS and UDT/UDTS per end node requirements. This feature can be enabled and disabled at GTT and instance levels. Segmentation and reassembly of SCCP messages is not supported.

ASP Binding Algorithm Enhanced for SCCP Class 2 Traffic

Prior to this release, ASP binding occured for only SCCP Class 0 and Class 1 packets. SCCP Class 2 packets were sent through all ASPs in a particular AS. The enhancement in this release binds SCCP Class 2 packets as well. ASP binding occurs for packets routed at the MTP3 level only, since Class 2 traffic is not supported at the SCCP level.

Enhanced CLI Statistics and Debugging for EAP-SIM

EAP-SIM is an Extensible Authentication Protocol (EAP) mechanism for authentication and session key distribution using the Subscriber Identity Module (SIM) from the Global System for Mobile Communications (GSM). This enhancement adds additional CLI statistics and debugging information for EAP-SIM.

- Error code for last error occurred
- Unsuccessful decode of access request
- Invalid length of RADIUS packet

Enhanced MLR ″default-rule″

Prior to the IRI release, while MLR processing a packet, if no valid MAP operation code is found in the packet, then MLR processing discontinues and the packet is routed using SCCP/MTP3. This enhancement provides an option for specifying a "default-rule" in a MLR ruleset. The "default-rule" is applied to TCAP packets that satisfy the following conditions:

- ITP receives a TCAP-BEGIN, TCAP-CONTINUE, or TCAP-END message having no opcode in the component portion or a TCAP-ABORT message.
- The component portion of TCAP-BEGIN, TCAP-CONTINUE, or TCAP-END message received by ITP does not have a valid MAP operation code.

Note Note: Invalid means invalid in terms of length (less than 1 or greater than 4). Any unknown operation code is treated as a positive scenario and will not match the default rule.

- The attempt to extract Originating Transaction Id or Destination Transaction Id from component portion of received TCAP-BEGIN, TCAP-CONTINUE, or TCAP-END message fails at ITP.
- The MAP operation code defined in component portion of the received TCAP message is SMS-MO or SMS-NOTIFY and no other rule matches.

CLI to Trigger On-Demand Circular Route Detection

In prior releases, a Circular Route Detection (CRD) test gets triggered upon detection of congestion. This meant you had to create a congestion scenario in order to check for a loop in the network topology. This feature provides a CLI option to trigger an on-demand CRD test to help detect network loops more easily.

New Hardware Features in Release 12.4(15)SW8

No new hardware feaures are supported in this release.

New Software Features in Release 12.4(15)SW8

The following new software features are supported:

SCCP Class-1 Load Balancing Within Application Group

This feature provides a CLI option with which SCCP Class-1 traffic can be evenly distributed within an application group for multiplicity share, cost, and wrr. SCCP Class-1 traffic can be load balanced among a maximum of 64 destinations based on various algorithms using a GTT application group.

xUA Error Handling

This feature provides a CLI option with which ITP can tear off SCTP association for an ASP when a configured number of error messages are received in a configured interval of time. The error codes on which error handling occurs are configurable.

SNMP Traps for 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. In this current release, SNMP alarm traps can be triggered when a circular route is detected. These SNMP alarm traps can be cleared when the circular route is resolved.

New Hardware Features in Release 12.4(15)SW7

No new hardware feaures are supported in this release.

New Software Features in Release 12.4(15)SW7

The following new software features are supported:

Egress Traffic Rate Limit

The egress traffic rate limit provides a mechanism to throttle outgoing traffic at the linkset or AS level. It measures the traffic on each linkset against a configured threshold. Excess traffic is silently discarded. . An alarm is raised when the threshold reaches a configurable limit and cleared when the traffic rate over the next time window stays below the abate limit.

Load Balancing Across up to Four Routes

The support for configuring up to four routes with the same priority provides a mechanism to load balance across up to four routes. With load balancing disabled, traffic is distributed among all the links of a combined linkset. With load balancing enabled, traffic is equally distributed among all the linksets of a combined linkset.

USSD Filtering

The USSD filtering feature enables ITP to filter mobile-initiated GSM-MAP messages based on USSD string and route the messages to the USSD server. USSD reponse messages are then routed back to the same MSC. If the USSD string does not match, the messages can be discarded.

MSU Peak Rate Reset

This enhancement provides a CLI option with which ITP can reset high water mark variables cimrMsuTrafficMaxRate and cimrMsuTrafficMaxTimestamp without sacrificing rest of the MSU report counters and variables in the CISCO-ITP-MSU-RATES-MIB.

Resync of DPC Status

This enhancement automatically updates the access or inaccess status of the route correctly and when a new route is included for a destination in the route table.

Additionally, it is required to update the route status of the affected remote XUA destinations correctly when the linkset (in shutdown state) used for defining the route becomes available as a result of performing a **no shutdown** on it.

New Hardware Features in Release 12.4(15)SW6

No new hardware features are supported in this release.

New Software Features in Release 12.4(15)SW6

The following new software features are supported:

- Ingress Traffic Rate Limit, page 6
- Inter-Carrier SMS Accounting, page 6
- Q.704 Load Balancing, page 6
- TestSPRPInbandPing, page 6

Ingress Traffic Rate Limit

The Ingress Traffic Rate Limit provides a mechanism to throttle incoming traffic at the linkset or AS level. It measures the traffic on each linkset against a configured threshold. Users can configure the option of either silently dropping the excess traffic or rejecting the excess traffic with an appropriate SCCP message.

Inter-Carrier SMS Accounting

Cisco ITP generates a large amount of statistical and accounting information from its signaling network. Inter-Carrier Accounting allows the user to tailor this information for use in billing and settlement. In earlier releases, Inter-Carrier Accounting operated only with MTP3 and SCCP messages. Cisco ITP software release 12.4(15)SW6 add SMS message support to this feature.

Q.704 Load Balancing

Cisco ITP load balancing adds the ITU Q.704 standard linkset load sharing scheme to the distributed traffic loadsharing options. This scheme equally divides traffic between the linksets. It then divides the allocated linkset traffic among the links that comprise the linkset. The user can configure their preferred load balancing scheme.

TestSPRPInbandPing

The TestSPRPInbandPing is a runtime diagnostic that detects most runtime software driver and hardware problems on a supervisor engines. It tests the Layer 2, Layer 3 and 4 forwarding engine, and the replication engine on the path from the switch processor to the route processor. On Cisco ITP, TestSPRPInbandPing packet failures result in resetting the active supervisor engine.

TestSPRPInbandPing is part of the Cisco GOLD (Generic OnLineDiagnostics). GOLD is a platform independent distributed framework that provides a common CLI and scheduling for runtime diagnostics

New Hardware Features in Release 12.4(15)SW5

No new hardware features were introduced.

New Software Features in Release 12.4(15)SW5

The following new software features are supported:

- Packet Address Modification (PAM), page 7
- Default Next Table in GTT, page 7
- SCTP Compliance with the United Kingdom Interconnect Parameters, page 7
- SCTP RFC 4960 Compliance Phase Two, page 7

Packet Address Modification (PAM)

The PAM feature allows the operator to modify the MTP and SCCP header fields for both TDM and SIGTRAN links. Among the fields that you can modify include: Originating Point Code (OPC), Destination Point Code (DPC), Calling Party Address (CgPA), and Called Party Address (CdPA).

Default Next Table in GTT

The Default Next Table in GTT feature allows the default GTT entry in a GTT table to point to another (next-table) GTT table in the same or different instance. Using this feature allows a user to maintain only a master table instead of having to maintain redundant GTA entries for the master tables and other tables.

SCTP Compliance with the United Kingdom Interconnect Parameters

The UK authorities have requested changes in SCTP parameters in order to allow UK interconnect. This feature modifies the Cisco ITP range of SCTP related parameters to comply with these specifications. It also supports a new configuration option for the SACK Frequency of SCTP associations and a new configuration option for the valid cookie life of an SCTP association.

SCTP RFC 4960 Compliance Phase Two

Release 12.4(15)SW5 completes additional SCTP RFC 4960 criteria.

New Hardware Features in Release 12.4(15)SW4

No new hardware features are supported.

New Software Features in Release 12.4(15)SW4

The following new software features are supported:

- Inter-Carrier Accounting and Accounting Reliability Enhancement (ICARE), page 7
- GTT Overflow Load Sharing, page 8
- GTT Weighted Load Balancing, page 8
- ASP Binding Enhancement, page 8
- SCTP RFC 4960 Compliance, page 8

Inter-Carrier Accounting and Accounting Reliability Enhancement (ICARE)

Inter-Carrier Accounting enables Cisco ITP to accumulate ingress and egress traffic statistics into accounts, where each account can stand for an operator or carrier. This allows the use of ITP accounting records as Signaling Data Records (SDR) for inter-carrier billing.

GTT Overflow Load Sharing

GTT Overflow Load Sharing allows Cisco ITP to send only a certain amount of GTT traffic up to a defined limit to a primary destination. Traffic that exceeds the threshold is routed to a secondary destination.

GTT Weighted Load Balancing

GTT Weighted Load Balancing adds a Weighted Round Robin (WRR) multiplicity mode for GTT application groups. In WRR mode both class 0 and class 1 traffic use weighted loadsharing for distribution to different available destinations in the GTT application group. For class 1 traffic, the messages with same signaling link selector (SLS) are sent to same destination. An SLS, CGPA-SLS or OPC-SLS can be the seed for the WRR algorithm.

ASP Binding Enhancement

The ASP Binding Enhancement eliminates the dynamic creation and maintenance of a unique data structure for an ASP binding. The elimination of these operations greatly reduces the ITP CPU load, SGMP management traffic, and SUP/LC updates for a Cisco ITP. This feature applies to Cisco ITPs that forward M3UA/SUA traffic with large CIC or SLS ranges and use the loadshare binding traffic mode. ASP bindings use a deterministic ranking of ASPs in the AS. The rankings combined with the local and remote ASP state determine the loadsharing.

SCTP RFC 4960 Compliance

Prior to this release, Cisco ITP was compliant with SCTP RFC 2960 but not compliant with SCTP RFC 4960. Releases 12.2(33)IRD, 12.4(15)SW4 and later are compliant with SCTP RFC 4960.

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, page 9
- ASP Binding Enhancement, page 9
- Enhanced SCTP Monitoring, page 9
- Support of 32 ASPs per AS, page 9
- CgPA Checking of the MO-SMS Messages, page 9
- GCP (H.248) Support, page 9
- Large MSU Support on M2PA and M3UA Associations, page 9
- Increased Local Port Numbers, page 9

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

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-fm**t 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, page 11
- Support for 16 Application Server Processes (ASPs) per Application Server (AS), page 12
- Support for GTT Inter-Instance, page 12
- Support for the cs7 mtp3 rct-opc-from-tfc Command, page 12
- Support for TTC Variant Conversion, page 12

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 Routeset 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
- MLR Routing to M3UA AS without Modifying the DPC
- 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 rulesets, 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, page 14
- Integrated GWS and MLR Triggers, page 15

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, page 15
- GWS SCCP Error Return, page 16
- MLR SCCP Error Return, page 16
- Multiple HSL PVCs per Physical ATM interface, page 16
- SCCP/MAP Address Modification for SRI-SM Messages, page 16

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 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 on Cisco.com, you can use the Bug Toolkit to find caveats of any severity. To reach the Bug Toolkit, log into 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)SW9

There are no open caveats in this release.

Resolved Caveats—Cisco IOS Release 12.4(15)SW9

All the caveats listed in this section are resolved in Cisco IOS Release 12.4(15)SW9 and are organized by the level of severity.

Severe

- CSCty22362

Symptom Unnecessary UPU and DUPU has been seen in the network, which causes destination inaccessible.

Conditions This symptom occurs when we update route in the route table of ITP for non-adjacent XUA-point code.

Workaround None.

Moderate

- CSCtw49365

Symptom M2PA link down by invalid BSN. The M2PA links flapped:

```
YGIN_SG8 | NOTI  | Sep 28 21:14:54.356: %CS7MTP3-5-LINKUPDOWN: Link 4 in linkset
KTC_YGIN_SG03 is unavailable
YGIN_SG8 | ERROR | Sep 28 21:14:54.528: %CS7MTP3-3-LINKNOTUP: Link 4 in linkset
KTC_YGIN_SG03 failed. Reason=protocol error (invalid BSN)
YGIN_SG8 | ERROR | SLOT 5/0: Sep 28 21:14:54.359: %CS7MTP3-3-LINKNOTUP: Link 4 in linkset
KTC_YGIN_SG03 failed. Reason=protocol error (invalid BSN)
YGIN_SG8 | NOTI  | Sep 28 21:15:04.600: %CS7MTP3-5-LINKUPDOWN: Link 4 in linkset
KTC_YGIN_SG03 is available
```

Conditions Links flapped while the border case of bsnr=16777215 and fsnt = 0 occurred during pumping traffic.

Workaround None.

Minor

- CSCtx17174

Symptom ITP incomplete **cs7 instance 0 pam** command in SW8 but not in SW5

Conditions SSN number becomes mandatory in SW8.

```
SW-5:
ITP_LAB(config)#cs7 instance 0 pam NIB_Test
ITP_LAB(config-cs7-pam)#cgpa gt prefix 12 34609090676f ?
  pc   Modifies the SCCP calling party address point code
  ssn  Modifies the SCCP calling party address subsystem number
  tt   Configure calling party address translation type modification
  <cr>

SW-8:
ITP_LAB(config)#cs7 instance 0 pam NIB_Test
ITP_LAB(config-cs7-pam)#cgpa gt prefix 12 34609090676f ?
  pc   Modifies the SCCP calling party address point code
  ssn  Modifies the SCCP calling party address subsystem number
  tt   Configure calling party address translation type modification
```

Workaround None.

Enhancement

- CSCty41676

Symptom After loading the gtt file, the associations failed to come up.

Conditions After reload, a shutdown and no shutdown was performed on the association.

Workaround None.

- CSCty61266

Symptom No warning or error message is generated when trying to configure a Network Appearance (NA) value 1-7 already being used by another instance.

Conditions If we try to configure 1-7 NA value that is already being used by another instance, then IOS doesn't not populate a warning or error message.

Workaround None.

Open Caveats—Cisco IOS Release 12.4(15)SW8a

There are no open caveats in this release.

Resolved Caveats—Cisco IOS Release 12.4(15)SW8a

All the caveats listed in this section are resolved in Cisco IOS Release 12.4(15)SW8 and are organized by the level of severity.

Catastrophic

- CSCtr28857

  A vulnerability in the Multicast Source Discovery Protocol (MSDP) implementation of Cisco IOS Software and Cisco IOS XE Software could allow a remote, unauthenticated attacker to cause a reload of an affected device. Repeated attempts to exploit this vulnerability could result in a sustained denial of service (DoS) condition.

  Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are available. This advisory is available at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-msdp

Severe

- CSCtr91106

  A vulnerability exists in the Cisco IOS Software that may allow a remote application or device to exceed its authorization level when authentication, authorization, and accounting (AAA) authorization is used. This vulnerability requires that the HTTP or HTTPS server is enabled on the Cisco IOS device.

  Products that are not running Cisco IOS Software are not vulnerable.

  Cisco has released free software updates that address these vulnerabilities.

  The HTTP server may be disabled as a workaround for the vulnerability described in this advisory.

  This advisory is available at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-pai

Moderate

- CSCtw49365

Symptom M2PA link down by invalid BSN

Conditions As shown below, the M2PA links flapped while the border case of bsnr=16777215 and fsnt=0 occurred while pumping traffic:

```
YGIN_SG8 | NOTI | Sep 28 21:14:54.356: %CS7MTP3-5-LINKUPDOWN: Link 4 in linkset
KTC_YGIN_SG03 is unavailable
YGIN_SG8 | ERROR | Sep 28 21:14:54.528: %CS7MTP3-3-LINKNOTUP: Link 4 in linkset
KTC_YGIN_SG03 failed. Reason=protocol error (invalid BSN)
YGIN_SG8 | ERROR | SLOT 5/0: Sep 28 21:14:54.359: %CS7MTP3-3-LINKNOTUP: Link 4 in
linkset KTC_YGIN_SG03 failed. Reason=protocol error (invalid BSN)
YGIN_SG8 | NOTI | Sep 28 21:15:04.600: %CS7MTP3-5-LINKUPDOWN: Link 4 in linkset
KTC_YGIN_SG03 is available
```

Workaround None.

Minor

- CSCtx17174

Symptom ITP incomplete command error in SW8 but not in SW5 release

Conditions When running SW8 release, a SW5 release configuration generates incomplete command errors. SSN number becomes mandatory in SW8 release.

Workaround None.

Open Caveats—Cisco IOS Release 12.4(15)SW8

There are no open caveats in this release.

Resolved Caveats—Cisco IOS Release 12.4(15)SW8

All the caveats listed in this section are resolved in Cisco IOS Release 12.4(15)SW8 and are organized by the level of severity.

Moderate

- CSCto41321

Symptom A Cisco 7600 Router with ITP image may not retain all CS7-related MIB configuration on a reload.

Conditions The following commands are known to be affected:

- – cs7 snmp dest-max-r1-window
- – cs7 snmp mgmt-max-r1-window

Workaround Reapply the configuration once the router has come back up.

- CSCtq77292

Symptom Newly added cs7 update route configuration can't be synchronized to the alternate ITP (ITP2). Load_share parameter is lost from both ITP configurations.

Conditions This symptom may occur when the active ITP is reloaded with the cs7 group feature configured.

Workaround None.

- CSCtt29023

Symptom A Cisco 7200 Router running code version 12.4(15)SW5 reloads after saving GTT table.

Conditions This symptom may occur when this configuration:

```
cs7 instance 1 gtt address-conversion E212TOE214
update in-address 73001 out-address 56982 np 7 nai 4  es 1 remove 5
update in-address 73002 out-address 56916 np 7 nai 4  es 1 remove 5
update in-address 73003 out-address 56920 np 7 nai 4  es 1 remove 5
```

Is followed by the save command:

```
cs7 1 save gtt-table disk2:gtttable_ins1.
```

Workaround None.

Open Caveats—Cisco IOS Release 12.4(15)SW7

This section documents possible unexpected behavior by Cisco IOS Release 12.4(15)SW7 and organizes caveats by the level of severity.

Moderate

- CSCto36193

Symptom The default option in MLR table is not working for USSD Transaction.

Conditions When MLR ruleset with opcode mobileUSSD is triggered via default option of MLR table, the USSD Transaction does not succeed.

Workaround Use the recommended method of GWS for triggering MLR rulesets.

- CSCto24908

Symptom Tracebacks are observed when traffic is routed through a GTT application group.

Conditions This symptom occurs when traffic is being routed via a GTT application group and the receive-side congestion onsets for the first time. There is no impact on traffic being routed.

Workaround Keep the threshold of receive-side congestion high.

- CSCtl73824

Symptom Linkset is not available even when all links bound with linkset are available.

Conditions This symptom occurs when the linkset on the peer is shutdown, removed, and then added during a time frame in which MTP3 restart is ongoing in phase 2, i.e. after T18 expiry.

Workaround If problem occurs, issue the **shutdown** and **no shutdown** commands on the linkset.

Resolved Caveats—Cisco IOS Release 12.4(15)SW7

All the caveats listed in this section are resolved in Cisco IOS Release 12.4(15)SW7 and are organized by the level of severity.

Catastrophic

- CSCtl74562

Symptom On an ITP/CS7 gateway, a 'small' buffers leak eventually leads to memory depletion.

Conditions The symptom occurs when ITP/CS7 is enabled and running on a gateway device and the cs7 group feature is configured. Also, the ITP is acting as an alternate in standby mode.

Workaround None.

Severe

- CSCtl79854

Symptom System messages concerning SCCP similar to the following may appear:

```
%CS7SCCP-5-SCCPGNRL:
Translated DPC xxxx:y congested.
```

Conditions The symptom occurs when a point code goes into the SCCP congested state and does not abate.

Workaround There are two workaround options:

- Issue the **cs7 instance <instance-number> gtt map sp available <point-code>** command in privileged EXEC mode to reset the SCCP congestion state for the specified point code.
- Remove the routes to the corresponding DPC, and add it again using the **no update route** and **update route** commands.

Moderate

- CSCtl58694

Symptom Virtual linkset with no route allows default route to be treated as available.

Conditions During normal operating conditions, route may not be marked as UNAVAIL during DPC isolation.

Workaround Configuring the **cs7 instance <instance-num> summary-routing-exception** command is a viable workaround if it is done before the problem has occurred. Removing default route (pc-conversion default) will also work, but in this case you'll need to reload the setup or apply **shutdown** and **no shutdown** commands to the linkset to clear the problem.

- CSCtn31541

Symptom ITP is returning NULL value on MWTM corresponding to the given OID.

Conditions Query from SNMP tool is returning NULL values on the following MIB elements: cimrMsuProcAcceptableThreshold, cimrMsuProcWarningThreshold, cimrMsuProcOverloadThreshold

Workaround Obtain these values using the **show cs7 msu-rates configuration** command.

Minor

- CSCtl77055

Symptom "No sms operation code matched" message appears on console and in logs.

Conditions The symptom occurs when logging to the console is enabled. The messages appear on the console of the linecard used for offload and may lead to high CPU utilization.

Workaround Disable logging to the console. Use the **logging buffer** command to log system messages.

Open Caveats—Cisco IOS Release 12.4(15)SW6

This section documents possible unexpected behavior by Cisco IOS Release 12.4(15)SW6 and organizes caveats by the level of severity.

Moderate

- CSCtj23210

Symptom When a Cisco 7600 Series router running Cisco ITP with only one linkset is reloaded, it takes more than 15 minutes for the links to come up from the time the message *linkset <name> activation is in progress* appears.

Conditions The Cisco ITP is reloaded with a SAMI card powered down.

Workaround Remove the powered down SAMI card from the setup and then reload.

- CSCth94205

Symptom The BFD BGP adjacency does not comes up after the removal of an IP address from the interface. The BFD BGP adjacency is not formed and does not comes up even after the configuration is present. System messages similar to the following may appear:

```
6: %BGP-3-NOTIFICATION: sent to neighbor 10.78.170.130 active 2/3 (BGP identifier wrong) 4
bytes AC122CD7 14:55:36: %BGP-4-MSGDUMP: unsupported or mal-formatted message received
from 10.78.170.130: FFFF FFFF FFFF FFFF FFFF FFFF FFFF FFFF 0032 0104 0082 00B4 AC12 2CD7
1502 0601 0400 0100 0102 0280 0002 0202 0002 0383 0100
```

Conditions The symptom occurs when:

- An IP address is removed from one end of the BFD adjacency formation.
- The neighboring device's address is configured on its interface.
- It is deregistered and the original IP address is configured back again.

Workaround None

- CSCti88349

Symptom While running traffic from M2PA SAMI Sup L2 ----> HSL FW on 10000 MSU there is a drop of packets ranging from 5000-15000 MSU depending on the total traffic run.

Conditions While performing a switchover, a packet drop is observed. This issue occurs when a SUP interface with a L2 config is used to make linksets.

Use other interfaces for configuring linksets.

Resolved Caveats—Cisco IOS Release 12.4(15)SW6

All the caveats listed in this section are resolved in Cisco IOS Release 12.4(15)SW6 and are organized by the level of severity.

Severe

- CSCti33126

Symptom The NTP configuration is accepted, but is not shown in the running configuration. The NTP process does not start.

Conditions This occurs only on the Cisco ITP 12.2(33)IRE1 release.

Workaround None

Moderate

- CSCtf77789

Symptom The CS7XUA syslog messages are not in the Cisco ITP documentation.

Conditions This information was added to the Cisco ITP user documentation's "ITP System Messages" chapters.

Workaround None. Information added to the user documentation.

- CSCth07837

Symptom The Cisco ITP incorrectly acknowledges User Data before the link is proved.

Conditions The problem is with the M2PA User Data carrying acknowledgment of the test packet. The acknowledgment is confirmed by the incremented BSN sent by the Cisco ITP.

Workaround None.

- CSCth20626

Symptom The Cisco ITP Release 12.2(33)IRD on the Cisco 7609-S router does not react or respond to simultaneous MSUs with incorrect BSN.

Workaround None.

- CSCtj23257

Symptom Undocumented or debug output appears on the console:

```
The billing is not configured
load route table from disk0:route_20100923_0 successfully.
load route table from disk0:route_20100923_1 successfully.
```

Conditions This symptom occurs during an ITP reload.

Workaround None.

Minor

- CSCtg90759

Symptom The **cs7 instance x ignore-sccp-pcconv y** command is not covered in the documentation.

Conditions User Documentation

Workaround None. Information added to user documentation.

- CSCtg35799

Symptom When the user tries to **write mem** or **reload** the Cisco router an invalid system message appears. The message incorrectly indicates that the MTP3 routing table contains unsaved data.

Conditions The cs7 routing configuration is stored in the running configuration rather than as a file in the flash memory. A change is made to the mtp3 routing table for the Cisco ITP. It is configured to store routing information in the running configuration file.

Workaround This is an invalid notice and can be ignored. The **write mem** is sucessful and the routing change is saved to the startup configuration file.

- CSCth24165

Symptom The Cisco ITP incorrectly acknowledges the short MSU.

Conditions A short MSU is received by Cisco ITP on an M2PA link.

Workaround None.

- CSCth50519

Symptom The behavior of the command **cs7 all save gtt-tables** was changed in the Cisco ITP 12.2(33)IRE release. Now the command asks for the confirmation for saving each gtt-table.

For example:

```
ITP-2#cs7 all save gtt-tables
GTT files for all instances must be saved in case of inter-instance
next-table configuration [confirm]y
GTT table save to 'disk0:instance_0_gtt.conf' successfully
GTT files for all instances must be saved in case of inter-instance
next-table configuration [confirm]y
GTT table save to 'disk0:instance_1_gtt.conf' successfully
GTT files for all instances must be saved in case of inter-instance
next-table configuration [confirm]y
GTT table save to 'disk0:instance_2_gtt.conf' successfully
GTT files for all instances must be saved in case of inter-instance
next-table configuration [confirm]
GTT table save to 'disk0:instance_3_gtt.conf' successfully
```

Conditions Constant

Workaround Use the EEM script in order to ask for confirmation automatically.

- CSCti33103

Symptom The counters displayed in the **show cs7 offload instance** output are not covered in the user documentation.

Workaround None. Information added to the user documentation.

- CSCth63331

Symptom ITP was incorrectly incrementing the FSN of a FISU falsely acknowledging a too long MSU during Q.781 5.2 testing.

Workaround None.

Open Caveats—Cisco IOS Release 12.4(15)SW5

There are no open caveats in this release.

Resolved Caveats—Cisco IOS Release 12.4(15)SW5

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

Severe

- CSCtf45209

Symptom

Route state of alias point code are access state even though its real point code is INACC state.

For example, the pc-conversion config is set below:

cs7 instance 0 pc-conversion x.x.x alias-pc 1 y.y.y

The **show cs7 route** command shows that route state of alias and the real pc is inconsistent.

Destination C Q P Linkset Name   Linkset Non-adj Route

---------------------- - - - ------------------- -------

x.x.x   INACC   3 [real linkset]   UNAVAIL allowed UNAVAIL

y.y.y   acces   1 VirtualLS1-0   avail   allowed avail

By this issue, customer experienced that traffic to this alias-PC could not be received from adjacent node.

Conditions The Cisco IOS boots up with the down state of linkset.

Workaround Use the **shutdown** and then **no shutdown** commands on the linkset of destination instance (Instance 0 in the example).

- CSCtb08449

Symptom The Cisco ITP reloads when the **show cs7 gtt configuration** command is configured.

Conditions The system operator is showing the gtt configuration.

- The console goes into a '-More-' state.
- The configured gtt application group is removed.
- As a result, when the system operator hits enter, then the viewing gtt application might be removed. The pointer is referring to a invalid memory location which causes the system reload.

Workaround None.

- CSCso84249

Symptom ITP may reload all offloaded SS7 linecards upon experiencing the following error message:

```
%DCS7-3-INTERRM: dcs7_route_update_xdr(): Malloc failed. Slot all
```

Conditions An extended data record (XDR) pool must become exhausted while the MTP3 controlled rerouting procedure executes on the Supervisor processor. The pool may become exhausted due to a large network event or due to any spike in communication between Supervisor and FlexWAN linecards.

Workaround None.

Moderate

- CSCtd94010

Symptom Route state to AS keep Active/Access via **show cs7 route** CLI after AS is shutdown.

Under this state, if ITP send SRT to this AS's PC via C-link , opposite ITP never returned TFP. As a result, AS and c-link route keep avail state.

Conditions C-link route exist to AS's PC. Route between ITP and AS are shutdown.

Workaround Shutdown the c-link before starting maintenance work, because when linkset of C-link is shutdown, route state to AS change to unavail/INACC expectedly.

- CSCta44455

Symptom ITP routes are not shown in the ss7 routing table.

When input **show cs7 route x.x.x**, the output route table is correct.

However, when input **show run | section x.x.x**, not all the route table is displayed.

Conditions The route table is updated in unknown condition.

Workaround If the route table is updated, the route table should be saved to disk/flash. save route-table in disk0 using **cs7 save route-table ...**

- CSCtf77789

Symptom CS7XUA syslog messages need explanation in ITP documentation.

Conditions This information was added to the ITP user documentation's *ITP System Messages* chapter.

Workaround None.

- CSCsz94790

Symptom ITP forwards MSU to peer with error OPC, the OPC A-B-C will change to A-B-A.

Conditions In ANSI network, when MSU route on C-LINK or route to AS, the OPC will be changed.There is no such issue in ITU network.

Workaround There is no known workaround.

Further Problem Description When using GWS to trigger an mlr result group to make MSU reroute to AS, the OPC of this MSU will change.When trigger MSU traffic route on C-link, the OPC in MSU will change.

- CSCta44187

Symptom The ITP doesn't send out SHUTDOWN-ACK when it receives SHUTDOWN in SHUTDOWN_RCVD state.

Conditions This problem happens in SHUTDOWN_RCVD state only. When the ITP receives a shutdown chunk with cumulative tsn ack less than the tsn number ITP sends out, the ITP doesn't respond with shutdown ack. The remote side then sends out a shutdown chunk with cumulative tsn ack equal to the tsn number ITP send out. The ITP still doesn't respond with the shutdown ack.

Workaround None.

- CSCta78201

Symptom SCCP_UNQUAL definition missing from documentation. Should be in Table 24 for **show cs7 gtt measurements**

Conditions User Documentation

Workaround The following definition was added to the user documentation: Definition: *The total number of times SCCP failed due to an error that is unqualified by any of the other errors listed.*

- CSCtb51424

Symptom Only one of the matched GTT application groups measurement is updated.

Conditions This issue only happen, on one linecard, if more than 1 GTT application group are matched during GTT, only the first GTT application group measurements are sent to SUP.

Workaround None.

- CSCtb69898

Symptom If the ASP association is restarted from a remote node when the ASP is in active state, the TOS value for ASP/SCTP is reset to default.

Conditions The issue only occurs when the destination AS has the same DPC as the affected PC.

Workaround None.

- CSCtb78835

Symptom On reloading the ITP or GTT, the reload fails due to the missing MAP entries. As the GTT load halts on reaching the error, this can result in the majority of the GTT configuration missing which leads to a major network outage. ITP software needs to be updated to prevent the removal of MAP entries which are still required by application groups and/or gta entries.

Conditions When loading an application group 'PC' or GTA with a routing indicator of 'pcssn', it is necessary to have pre-loaded at least one MAP entry for that point code. The ITP software enforces this requirement. It is subsequently possible to delete these MAP entries, even though the gta and/or application groups are defined.

Workaround Manually ensure the MAP entries are not removed if they are still required by application groups and/or GTA entries.

- CSCtc60936

Symptom Second ASP is INACTIVE in load share mode. ITP did not send out NOTIFY message to second ASP, so no ASP Active message can be received from remote side.

Conditions

a. The problem was observed with Cisco ITP (7600) running 12.2(18)IXF1 interacting with a service provider

b. After applying correct configuration, customer was not able to get both ASPs in Active state.

c. In addition, we also confirmed that SCTP connection is ESTABLISHED for ASP2, but still it was showing as "Inactive".

d. Collected further traces and observed that for failed ASP2 we do not receive ASPAC; so therefore the reason why of the ASP2 being "Inactive". After customer worked with their provider on this problem, they have disabled the NOTIFY reception restriction on their side, and we then obtained ASP2 in Active.

e. Their provider has mentioned that for ASP2, they do not originally received NOTIFY (AS-Inactive) (as they did for ASP1) and that is the reason why they do not sent us ASPAC. They mentioned that they are following RFC 4666 and that the call flow should as the one on point 5.1.3 as per same RFC.

Workaround Lifting the restriction of receiving NOTIFY message in order to send out ASP Active message on second ASP, and the ASP is becoming ACTIVE. According to RFC 4666, the condition of bypassing the Notify message seems to be a valid optional scenario.

Further Problem Description There is a large amount of additional information on this caveat in the CDETs database.

- CSCtc76255

Symptom When specifying a point code at the end of the **show cs7 pc-conversion** command, it may display incorrect information.

Workaround Use the **show cs7 pc-conversion** without specifying a point code at the end.

- CSCtd07178

Symptom Normally, you should configure point code conversion for not only MTP3 layer but also SCCP layer. If the user does not configure point code conversion for point code in SCCP layer, the conversion will fail. However, customer want a knob to turn off the SCCP layer point code conversion check because they do not know which pc will be contained in the CxPA.

Conditions The three conditions are:

a. Instance conversion required for the SCCP packet routing.

b. In packet, CxPA, route on PCSSN

c. The CxPA pc has no point code conversion item configured for it.

Workaround You have three options:

  - Configure the PC for the point code in the SCCP layer.

  - Change the traffic to route on gt.

  - Configure the default pc conversion without the default route.

Minor

- CSCtb80915

Symptom ITP cli parses out *instance* when access-lists are defined

Conditions When adding an access-list to the ITP, the "instance" is required:

```
mssol-itp-f(config)#access-list 2714 ?
  instance  Specify a specific CS7 instance
```

but then the configuration is accepted, it is parsed on in the running-config:

```
mssol-itp-f(config)#access-list 2714 instance 0 remark BE1-XXXX-YYYY-incoming
mssol-itp-f(config)#do sh ru | inc remark
access-list 2714 remark BE1-XXXX-YYYY-incoming
mssol-itp-f(config)#
```

Workaround None.

- CSCtc43304

Symptom Only one of the matched GTT application groups measurement is updated.

Conditions This issue only happen, on one linecard, if more than one GTT application group are matched during GTT, only the first GTT application group measurements are sent to the SUP.

Workaround There is no known workaround.

Enhancement

- CSCtd87928

The **distribute-sccp-sequenced-negate** command was added. This command used in the application group submode can override the instance level setting of in-sequence or out-of-sequence delivery for that specific application group.

Open Caveats—Cisco IOS Release 12.4(15)SW4

There are no open caveats in this release.

Resolved Caveats—Cisco IOS Release 12.4(15)SW4

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

Severe

- CSCtb08449

Symptom The Cisco ITP reloads when the **show cs7 gtt configuration** command is configured.

Conditions The system operator is showing the gtt configuration.

- The console goes into a '-More-' state.
- The configured gtt application group is removed.
- As a result, when the system operator hits enter, then the viewing gtt application might be removed. The pointer is referring to a invalid memory location which causes the system reload.

Workaround There is no known workaround.

Moderate

- CSCsz94754

Symptom The MLR reroutes to a backup PC failure.

Conditions You have configured an MLR result group to wrr mode and the congestion-mode is set to defer-to-backup. If the DPC whose weight is larger than 0 comes into congestion, the traffic is rerouted to an available DPC whose weight equals 0. But if this DPC is XUA DPC, the rerouting fails.

Workaround The customer can use the AS name to trigger MLR result.

- CSCsz94790

Symptom The ITP forwards the MSU to peer with error OPC, the OPC A-B-C will change to A-B-A.

Conditions In an ANSI network, when the MSU routes on C-LINK or routes to an AS, the OPC change. There is no such issue in ITU network.

Workaround There is no known workaround.

- CSCsy73811

Symptom The following two issues occur on ITP when it 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 cannot be updated.

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

Workaround There is no known workaround.

- CSCta44187

Symptom The ITP doesn't send out SHUTDOWN-ACK when it receives SHUTDOWN in SHUTDOWN_RCVD state.

Conditions This problem happens in SHUTDOWN_RCVD state only. When the ITP receives a shutdown chunk with cumulative tsn ack less than the tsn number ITP sends out, the ITP doesn't respond with shutdown ack. The remote side then sends out a shutdown chunk with cumulative tsn ack equal to the tsn number ITP send out. The ITP still doesn't respond with the shutdown ack.

Workaround There is no known workaround.

- CSCta44455

Symptom ITP routes are not shown in the ss7 routing table.

Conditions When the **show cs7 route** command is entered, the output route table displayed is correct. When the **show run | section** command is entered, not all the route table is displayed. The route table is updated with an unknown condition.

Workaround Save the route-table to disk0 using the **cs7 save route-table** command.

- CSCta59767

Symptom The outbound network indicator value may change from the inbound network indicator value, if the received m3ua packet contains a message priority out of range (i.e. not 0 to -3).

Conditions An incoming message priority greater than or equal to 4 is received from m3ua.

Workaround Sending AS should send the correct Message Priority value.

- CSCtb29561

Symptom DUPU is sent to an AS that has the same DPC as the affected PC. To filter this kind of DUPU, you should configure the cs7 xua-ssnm-filtering.

Conditions The issue only occurs when the destination AS has the same DPC as the affected PC.

Workaround There is no known workaround.

- CSCtb69898

Symptom If the ASP association is restarted from a remote node when the ASP is in active state, the TOS value for ASP/SCTP is reset to default.

Conditions The issue only occurs when the destination AS has the same DPC as the affected PC.

Workaround There is no known workaround.

- CSCtb78835

Symptom On reloading the ITP or GTT, the reload fails due to the missing MAP entries. As the GTT load halts on reaching the error, this can result in the majority of the GTT configuration missing which leads to a major network outage. ITP software needs to be updated to prevent the removal of MAP entries which are still required by application groups and/or gta entries.

Conditions When loading an application group 'PC' or GTA with a routing indicator of 'pcssn', it is necessary to have pre-loaded at least one MAP entry for that point code. The ITP software enforces this requirement. It is subsequently possible to delete these MAP entries, even though the gta and/or application groups are defined.

Workaround Manually ensure the MAP entries are not removed if they are still required by application groups and/or GTA entries.

- CSCsy65977

Symptom A route is configured to transport messages through C-LINK. If the indirect route is AS and it doesn't come up, the C-LINK route displays 'unavailable' even when the AS became active later.

Conditions When configuring an indirect route, but the indirect route is AS and unavailable, the C-Link route always displays unavailable.

Workaround Make the AS active and then shut and no shut C-link.

- CSCsy89971

Symptom ITP selects the second IP address for the primary path of the M3UA/SUA.

Conditions The issue occurs when an INIT packet from the remote side has a different order of IP addresses from the ITP M3UA/SUA configuration. ITP selects the primary IP address in the INIT packet.

Workaround Ask the remote side to send INIT packet with the same IP address order as the ITP M3UA/SUA configuration.

- CSCsz30865

Symptom You cannot query the cmlrInstTable with SNMP, when you use GWS to trigger MLR.

Conditions The issue occurs when you use GWS to trigger MLR.

Workaround There is no known workaround.

- CSCsz50535

Symptom When there is a query from MWTM, the CISCO-ITP-MSU-RATES-MIB can't be visited.

Conditions When you configure the cs7 msu-rate threshold-proc xxx on ITP, then reload the ITP router, the avl tree of the CISCO-ITP-MSU-RATES-MIB has a problem. It will return an error when it gets an SNMP query.

Workaround There is no known workaround.

- CSCta00588

Symptom ITP fails to match the IMSI of an sms rule with the HLR returned IMSI.

Conditions The issue occurs when ITP uses the obtain-orig-imsi next-rule as the result of the sms rule, and the ITP uses the imsi to match the following rules.

Workaround There is no known workaround.

- CSCtc05721

Symptom The SS7 link flaps due to t7 timeout at the far end and the far end sends SIOS. ITP stops sending FISUs with new FSN/BSN online when receiving MSUs. ITP sends FISUs with new FSN/BSN online when sending MSUs

Conditions The issue occurs when the ITP is receiving MSUs and no MSUs are sent from the ITP. The ITP runs only ingress MSUs.

Workaround Configure no encapsulation on the interface, then reconfigure the encapsulation on the interface and the link in the linkset.

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 and 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

• 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 circualr 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 **cs7 instance X national-options TFR** command**.**

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 formated 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 comes 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, severity 2, 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.

- CSCsl08358

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.

- CSCsl59128

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.

- CSCsl93462

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

  Roouter(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, severity 2, 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 instanc**e 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** *t1* or *e1* 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, severity 2, 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, severity 2, 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

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