



Release Notes for IP Transfer Point (ITP) 7600 for Cisco IOS Release 12.2(18)IXG

Software Release Date September 2008
Cisco IOS Release 12.2(18)IXG

These release notes for the ITP 7600 platform describe the enhancements provided in Cisco IOS Release 12.2(18)IXG and earlier. These release notes are updated as needed.

For a list of the software caveats that apply to Cisco IOS Release 12.2(18)IX, see the [“Caveats for Cisco IOS Release 12.2\(18\)IX”](#) section on page 15.

Contents

These release notes include the following topics:

- [System Requirements, page 1](#)
- [New and Changed Information, page 4](#)
- [Caveats for Cisco IOS Release 12.2\(18\)IX, page 15](#)

System Requirements

This section describes the system requirements for Cisco IOS Release 12.2(18)IX and includes the following sections:

[Memory Requirements, page 2](#)



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

© 2006 Cisco Systems, Inc. All rights reserved.

[Hardware Supported, page 3](#)

[Determining the Software Version, page 3](#)

Memory Requirements

Table 1 *Images and Memory Recommendations for the ITP 7600 Cisco IOS Release 12.2(18)IXG*

Platform	Feature Sets	Image Name	Software Image	Flash Memory Recommended	DRAM Memory Recommended	Runs From
Cisco 7600	IP Transfer Point	IP Transfer Point	s72033-itpk9v-mz	512	512	Flash

Table 2 *Images and Memory Recommendations for the ITP 7600 Cisco IOS Release 12.2(18)IXF*

Platform	Feature Sets	Image Name	Software Image	Flash Memory Recommended	DRAM Memory Recommended	Runs From
Cisco 7600	IP Transfer Point	IP Transfer Point	s72033-itpk9v-mz	512	512	Flash

Table 3 *Images and Memory Recommendations for the ITP 7600 Cisco IOS Release 12.2(18)IXE*

Platform	Feature Sets	Image Name	Software Image	Flash Memory Recommended	DRAM Memory Recommended	Runs From
Cisco 7600	IP Transfer Point	IP Transfer Point	s72033-itpk9v-mz	512	512	Flash

Table 4 *Images and Memory Recommendations for the ITP 7600 Cisco IOS Release 12.2(18)IXD*

Platform	Feature Sets	Image Name	Software Image	Flash Memory Recommended	DRAM Memory Recommended	Runs From
Cisco 7600	IP Transfer Point	IP Transfer Point	s72033-itpk9v-mz	512	512	Flash

Table 5 *Images and Memory Recommendations for the ITP 7600 Cisco IOS Release 12.2(18)IXC*

Platform	Feature Sets	Image Name	Software Image	Flash Memory Recommended	DRAM Memory Recommended	Runs From
Cisco 7600	IP Transfer Point	IP Transfer Point	s72033-itpk9v-mz	512	512	Flash

Table 6 *Images and Memory Recommendations for the ITP 7600 Cisco IOS Release 12.2(18)IXB1*

Platform	Feature Sets	Image Name	Software Image	Flash Memory Recommended	DRAM Memory Recommended	Runs From
Cisco 7600	IP Transfer Point	IP Transfer Point	s72033-itpk9v-mz	512	512	Flash

Table 7 *Images and Memory Recommendations for the ITP 7600 Cisco IOS Release 12.2(18)IXA*

Platform	Feature Sets	Image Name	Software Image	Flash Memory Recommended	DRAM Memory Recommended	Runs From
Cisco 7600	IP Transfer Point	IP Transfer Point	s72033-itpk9v-mz	512	512	Flash

Hardware Supported

Table 8 shows the supported interfaces for the ITP 7600 platform.

Table 8 *Supported Interfaces for the Cisco ITP 7600*

Interface or Linecard	Introduced In ¹
Cisco 7600 Supervisor Engine 720-3B	12.2(18)IXB1
ATM Port Adapter (PA-A6-0C3)	12.2(18)IXB1
ITP SS7 Q.703 High-speed Port Adapter (PA-MCX-4TE1-Q)	12.2(18)IXB1
Cisco 7600 Supervisor Engine 720-3BXL	12.2(18)IXA
Enhanced FlexWAN module for the Cisco 7600 Series Router (WS-X6582-2PA)	12.2(18)IXA
2 Port FE (PA-2FE-TX)	12.2(18)IXA
ITP SS7 Port Adapter for SS7 low-speed links (PA-MCX-8TE1-M)	12.2(18)IXA
ATM Port Adapter for SS7 high speed links (PA-A3-8E1IMA)	12.2(18)IXA
ATM Port Adapter for SS7 high speed links (PA-A3-8T1IMA)	12.2(18)IXA

1. The number in the "Introduced In" column indicates the Cisco IOS Release in which the interface was introduced on the ITP 7600.

Determining the Software Version

To determine the version of Cisco IOS software running on your Cisco ITP 7600, use the **show version EXEC** command.

New and Changed Information

New Hardware Features in Release 12.2(18)IXG

No new hardware features are supported.

New Software Features in Release 12.2(18)IXG

The following new software features are supported:

- [MLR Concatenated SMS Option](#)
- [MLR MAP Error Return](#)
- [GSM MAP Version Check In](#)
- [MLR Update Location for IMSI Blacklist](#)
- [MLR Instance Conversion](#)
- [Circular Route Detection](#)
- [SMS MO Proxy Offload](#)
- [Support for the cs7 xua-err-diag-fmt Command](#)

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.

SMS MO Proxy Offload

SMS MO Proxy offload allows you to configure ITP to distribute the SMS MO Proxy and SMS Not Proxy applications to the FlexWAN CPUs. When this feature is not enabled, these applications are sent to the Supervisor Engine (SUP).

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

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

New Hardware Features in Release 12.2(18)IXF1

No new hardware features are supported by the ITP 7600 for Cisco IOS Release 12.2(18)IXF1.

New Software Features in Release 12.2(18)IXF1

The following new software features are supported by the ITP 7600 in Cisco IOS Release 12.2(18)IXF1:

- [Support for the `cs7 snmp link-congestion-delay` Command](#)

Support for the `cs7 snmp link-congestion-delay` Command

When a link rapidly switches in and out of congestion, it generates many notifications that provide little management value. The new `cs7 snmp link-congestion-delay` global configuration command reduces the number of notification generated due to link congestion.

New Hardware Features in Release 12.2(18)IXF

No new hardware features are supported by the ITP 7600 for Cisco IOS Release 12.2(18)IXE.

New Software Features in Release 12.2(18)IXF

The following new software features are supported by the ITP 7600 in Cisco IOS Release 12.2(18)IXF:

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

- [Support for 7600 Table Size Management](#)

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

In Cisco IOS 12.2(18)IXF 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.

The **cs7 mtp3 rct-opc-from-tfc** command is documented in the *ITP Command Set: A - D* chapter of the *IP Transfer Point (ITP) on the Cisco 7600 Platform*.

Support for TTC Variant Conversion

In Cisco IOS 12.2(18)IXF 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.

TTC Variant Conversion is documented in the *IP Transfer Point (ITP) on the Cisco 7600 Platform*.

Accounting Support for xUA and Virtual Linkset

In Cisco IOS 12.2(18)IXF 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.

Accounting Support for xUA and Virtual Linkset is documented in *IP Transfer Point (ITP) on the Cisco 7600 Platform*.

Support for GTT Inter-Instance

In Cisco IOS 12.2(18)IXF 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.

GTT Inter-Instance is documented in *IP Transfer Point (ITP) on the Cisco 7600 Platform*.

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

In Cisco IOS 12.2(18)IXF and later releases, Cisco ITP supports 16 ASPs per AS.

Support for 7600 Table Size Management

This feature validates the concurrent support of the following database sizes under operating conditions.

Table Type	Concurrent Capacity
Routesets	10,000 - (5 routes per)
GWS Rules	35,000
GTT Entries	200,000
MAP Entries	3,000
Application Groups	3,000
Application Group Members	25,000
M3UA/SUA Routing Keys	5,000
MLR Entries	25,000
MLR Address Table Entries	25,000
MLR Rules	1000
MLR Result Group Members	5000
MLR Modify Profiles	100

New Hardware Features in Release 12.2(18)IXE

No new hardware features are supported by the ITP 7600 for Cisco IOS Release 12.2(18)IXE.

New Software Features in Release 12.2(18)IXE

The following new software features are supported by ITP 7600 on Cisco IOS Release 12.2(18)IXE:

- [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](#)
- [Extending the Application Group to 64 Entries per Group](#)
- [Enhancing GTT Address Conversion Flexibility](#)
- [MLR Routing to M3UA AS without modifying the DPC](#)
- [Enhanced MLR Modification CdPA \(and CgPA\)](#)

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

In Cisco IOS 12.2(18)IXE and later releases, you can save a 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.

This feature is documented in the *IP Transfer Point (ITP) on the Cisco 7600 Platform*.

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

In Cisco IOS 12.2(18)IXE and later releases, you can save the general MLR configuration to a local or remote file system, load the general configuration from a local or remote file system, and non-disruptively replace the running MLR configuration on an operational system.

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

This feature is documented in the *IP Transfer Point (ITP) on the Cisco 7600 Platform*.

Translation Type (TT) Modification within an Application Group

GTT currently allows post-translation modification of the TT on a per-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.

This feature is documented in *IP Transfer Point (ITP) on the Cisco 7600 Platform*.

TTMAP support for xUA AS

Mapping the CdPA TT to a configured value is supported for all 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 M3UA or SUA AS.

This feature is documented in the *IP Transfer Point (ITP) on the Cisco 7600 Platform*.

Extending the Application Group to 64 Entries per Group

This feature extends the limit of eight 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.

This feature is documented in the *IP Transfer Point (ITP) on the Cisco 7600 Platform*.

Enhancing GTT Address Conversion Flexibility

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.

This feature is documented in the *IP Transfer Point (ITP) on the Cisco 7600 Platform*.

MLR Routing to M3UA AS without modifying the DPC

This feature gives the MLR ability to route a received packet to an M3UA AS without modifying the DPC. This is not an MSU copy feature, but a modification to the routing of the received MSU.

This feature is documented in the *IP Transfer Point (ITP) on the Cisco 7600 Platform*.

Enhanced MLR Modification CdPA (and CgPA)

This feature allows MLR to modify the SCCP CdPA GT selector and digits prior to routing to the specified result. MLR modifies the SCCP CdPA PC and SSN using a modification profile. MLR modifies the SCCP CdPA via modify-profile for all MAP-based operations. MLR expands its SCCP CgPA modification to be applied to all MAP-based operations

This feature is documented in the *IP Transfer Point (ITP) on the Cisco 7600 Platform*.

New Hardware Features in Release 12.2(18)IXD

No new hardware features are supported by the ITP 7600 for Cisco IOS Release 12.2(18)IXD.

New Software Features in Release 12.2(18)IXD

The following new software features are supported by ITP 7600 on Cisco IOS Release 12.2(18)IXD:

- Integrated GWS and MLR Triggers
- SS7 Port Adapter for SS7 Low-Speed Links Supports 126 Links
- SMS MO Proxy
- Enhanced Loadsharing

Integrated GWS and MLR Triggers

In Cisco IOS 12.2(18)IXD and later releases, MLR triggers and 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.

Integrated GWS and MLR Triggers are documented in *IP Transfer Point (ITP) on the Cisco 7600 Platform*.

SS7 Port Adapter for SS7 Low-Speed Links Supports 126 Links

In Cisco IOS 12.2(18)IXD and later releases, the SS7 Port Adapter for SS7 Low-Speed Links (PA-MCX-8TE1-M) supports 126 links. This specific port adapter is supported in earlier releases, but Cisco IOS 12.2(18)IXD and later release offer full support of an increased the number of links.

The SS7 Port Adapter for SS7 Low-Speed Links is documented in the SS7 guide, *SS7 Port Adapter Installation and Configuration* on Cisco.com:

<http://www.cisco.com/univercd/cc/td/doc/product/core/cis7507/portadp/multicha/mcx8te1/index.htm>

It is also documented in the *IP Transfer Point (ITP) on the Cisco 7600 Platform*.

SMS MO Proxy

The ITP SMS MO proxy capability is extended to the Cisco 7600 Platform in this release. This feature allows MO-proxy, a stateful application, to work with the Cisco 7600 supervisor module (SUP). Previously, this feature was not supported on the 7600 platform.

SMS MO proxy is documented in the *IP Transfer Point (ITP) on the Cisco 7600 Platform*.

Enhanced Loadsharing

The Enhanced Loadsharing feature creates a 3-bit hash from a subset of bits (6 each) taken from the OPC and 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.

Enhanced Loadsharing is documented in the *IP Transfer Point (ITP) on the Cisco 7600 Platform*.

New Hardware Features in Release 12.2(18)IXC

No new hardware features are supported by the ITP 7600 for Cisco IOS Release 12.2(18)IXC.

New Software Features in Release 12.2(18)IXC

The following new software features are supported by ITP 7600 on Cisco IOS Release 12.2(18)IXC:

- GWS SCCP Error Return
- MLR SCCP Error Return
- Multiple HSL PVCs per Physical ATM interface

- SCCP/MAP Address Modification for SRI-SM Messages.
- C-Link Backup Routing of M3UA/SUA Traffic

MLR SCCP Error Return

Cisco IOS Release 12.2(18)IXC allows you to configure MLR to return a UDTS to the source of the 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.

GWS SCCP error return is documented in *IP Transfer Point (ITP) on the Cisco 7600 Platform*.

GWS SCCP Error Return

Cisco IOS Release 12.2(18)IXC allows you to configure GWS to return a UDTS to the source of the SCCP packet when the SCCP packet is dropped. You configure a return UDTS when you define the gateway screening action set in enhanced GWS.

GWS SCCP error return is documented in *IP Transfer Point (ITP) on the Cisco 7600 Platform*.

Multiple HSL PVCs per Physical ATM interface

Cisco IOS Release 12.2(18)IXC allows multiple HSL PVCs per physical ATM interface. This is done through the support of subinterface configuration on the ATM link. Prior to Cisco IOS Release 12.2(18)IXC, 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.

The multiple HSL PVCs feature is documented in *IP Transfer Point (ITP) on the Cisco 7600 Platform*.

SCCP/MAP Address Modification for SRI-SM Messages

Cisco IOS Release 12.2(18)IXC permits SCCP and MAP address modification using a MLR **modify-profile**. MLR currently supports modifying only the service center address (`orig-smsc`) and the calling party address (`CgPA`) for SRI-SM messages.

With Cisco IOS Release 12.2(18)IXC, 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 UDTS to the source of the SCCP packet when the SCCP packet is blocked by specifying an optional **sccp-error** parameter on block results.

SCCP and MAP address modification is documented in *IP Transfer Point (ITP) on the Cisco 7600 Platform*.

C-Link Backup Routing of M3UA/SUA Traffic

Cisco IOS Release 12.2(18)IXC supports a C-link Backup Routing feature that provides backup routing to M3UA and SUA ASs. It uses an MTP3/M2PA linkset to a remote SG serving the same ASs over SCTP/IP. This configurable software feature is available to any 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.

C-link Backup Routing is documented in *IP Transfer Point (ITP) on the Cisco 7600 Platform*.

New Hardware Features in Release 12.2(18)IXB1

The following new hardware features are supported by ITP 7600 on Cisco IOS Release 12.2(18)IXB1:

Support for the ATM Port Adapter (PA-A6-OC3)

The ATM Port Adapter (PA-A6-OC3) provides 8K VCs per port adapter and represents a performance improvement over the PA-A3-OC3 Port Adapter. The feature and function of the PA-A6-OC3 is unchanged.

The PA-A6-OC3 Port Adapter is supported in three variants:

- Multimode (PA-A6-OC3MM)
- Single-mode intermediate reach (PA-A6-OC3SMI)
- Single-mode long reach (PA-A6-OC3SML)

Each variant of the PA-A3-OC3 Port Adapter supports 2 physical optical connections for ATM signaling, one transmit and one receive for OC3 or STM-1 direct connectivity.

Support for the Cisco 7600 Supervisor Engine720 with Policy Feature Card 3B (SUP720-3B)

The Cisco 7600 Supervisor Engine 720-3B (SUP720-3B) is a member of the SUP720 family with a modular PFC3B forwarding engine daughter card.

Support for Q.703 Annex A High-speed Links (PA-MCX-4TE1-Q)

Cisco IOS Release 12.2(18)IXB1 provides support for Q.703 Annex A high-speed links on the ITP. The SS7 Q.703 High-speed Port Adapter (PA-MCX-4TE1-Q) supports enhanced Message Transfer Part Level 2 (MTP2) functions and procedures that are suitable for the operation and control of signalling links at data rates of 1.5 and 2.0 Mb. The ITP software for Cisco IOS Release 12.2(18)IXB1 enables configuration of the card type and controller and enables configuration of the interface for SS7 high speed MTP2 encapsulation.

Support for Q.703 Annex A high speed links is documented in *SS7 Q.70 High Speed Port Adapter Installation and Configuration Guide* and in *IP Transfer Point (ITP) on the Cisco 7600 Platform*.

New Software Features in Release 12.2(18)IXB1

The following new software features are supported by ITP 7600 on Cisco IOS Release 12.2(18)IXB1:

Preventive Cyclic Redundancy (PCR) Error Correction

Cisco IOS Release 12.2(18)IXB1 supports Preventive Cyclic Redundancy (PCR) Error Correction as described in Q.703 and GR-246. PCR is an alternative form of error correction for MTP2 links and is typically used on links that have a long delay (such as satellite links).

The PCR error correction feature is documented in *IP Transfer Point (ITP) on the Cisco 7600 Platform*.

Multi-Layer Routing (MLR) Generic Opcode Support

Cisco IOS Release 12.2(18)IXB1 extends Mobile Access Part (MAP) operation support to include all GSM-MAP (3GPP TS 29.002 version 5.9.0 Release 5) operations in MLR rules.

MLR Generic Opcode support is documented in *IP Transfer Point (ITP) on the Cisco 7600 Platform*.

Insert Destination Point Code (DPC) in Called Party (CDPA) PC

Cisco IOS Release 12.2(18)IXB1 provides a global option to insert DPC into the CDPA PC for packets that are MLR-routed.

The Insert DPC in CDPA feature is documented in *IP Transfer Point (ITP) on the Cisco 7600 Platform*.

New Hardware Features in Release 12.2(18)IXA

The initial release of ITP 7600 in Release 12.2(18) IXA includes the following hardware feature set:

- Cisco 7600 Supervisor Engine 720-3BXL
- Enhanced FlexWAN module for the Cisco 7600 Series Router (WS-X6582-2PA)
- 2 Port FE (PA-2FE-TX)
- ITP SS7 Port Adapter for SS7 low-speed links (PA-MCX-8TE1-M)
- ATM Port Adapter for SS7 high speed links (PA-A3-8E1IMA)
- ATM Port Adapter for SS7 high speed links (PA-A3-8T1IMA)

New Software Features in Release 12.2(18)IXA

The ITP 7600 platform provides the following key features:

- Non-Disruptive Upgrade
- Standard STP routing (MTP, GTT) and variant support
- Standard M3UA/SUA Signaling Gateway (Offloaded)

- QoS
- Gateway Screening
- Multiple Instances and Instance Translation
- Multiple Point Codes (primary, secondary, capability) per instance.
- Offloaded Multi-Layer Routing
- Offloaded Enhanced Gateway Screening

Caveats for Cisco IOS Release 12.2(18)IX

Caveats describe unexpected behavior in Cisco IOS software releases.



Note

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

Open Caveats—Cisco IOS Release 12.2(18)IXG

This section documents possible unexpected behavior by Cisco IOS Release 12.2(18)IXG. It organizes caveats by severity levels.

Moderate

- CSCsu45269

Symptom The statistics for an SMS ruleset or address-table are always displayed as zero on the supervisor module (SUP).

Conditions ITP is in sms offload mode.

Workaround Add the **execute-on** command to the beginning of the show command to execute the show commands on the line card.

For example, if sms is offloaded to module 1 bay 0, then you can see the corrects statistics by using the show command in this form.

execute-on 1 0 show cs7 sms ruleset name <ruleset>

- CSCsu02291

Symptom After system boot, a subset of key Cisco IOS CLI commands may be missing from the exec command list, and the commands are rejected if entered.

Conditions This occurs when the console is detached from the ITP, a telnet session is used to reload, and then the console is attached to the ITP when the system comes up.

Workaround There are three workarounds:

- Log out and then log back in using the console.
- Telnet instead of using the console.
- Initiate a reload using the console connection not the telnet session.

Resolved Caveats—Cisco IOS Release 12.2(18)IXG

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(18)IXG. Caveats are organized by the level of severity

Severe

- CSCsm76956

Symptom Some packets become hung on internal work queues within the ITP and are never delivered.

Conditions Some packets may become queued and never processed during periods of heavy system stress and/or congestion.

Workaround If this condition is detected by the user, issuing a **shut** then **no shut** command on each affected link clears the condition.

- 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.

- CSCsq36322

Symptom On a 7600 ITP, a FlexWAN2 line card may become disabled if a NSO switchover occurs while the linecard is reloading.

Conditions This issue has been observed only when a linecard such as FlexWAN2 or SAMI processor, is reloading and an NSO switchover occurs. After switchover completes, output of the 'show cs7 mtp3 offload' command shows the linecard processors in a 'DisabledSys' state, and is not reinitialized by the active SUP.

Workaround The linecard may be manually reset using the hw-module module reset command.

- CSCsq97726

Symptom M2PA links fail to activate after a **hw-module reset** of the enhanced FlexWan.

Conditions Running the ITP 76xx with M2PA links defined such that the first local-ip address resides on different processor from location of local-peer.

Workaround Remove the links and associated local-peer statement and ensure that the first local-ip address statement resides on the same processor as the location that is indicated by local peer statement.

- 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.

- CSCso43444

Symptom On the 7600 platform, MSU routing may fail to an M3UA or SUA Application Server (AS) that is locally *down*, but *active* on the SGMP mate. The AS state displayed on the linecard is *down* instead of *dwn-re*.

Conditions This occurs under the following conditions:

- ITP is configured with a mated SG.
- The AS is inactive but is active on the SGMP mate.

- ITP is configured with M3UA and SUA local instances.
- If rerouting AS is M3UA, FlexWANs that show incorrect AS state must have one or more SUA instances offloaded to them, and SUA instances only (no M3UA). Conversely, if rerouting AS is SUA, FlexWANs that show incorrect AS state must have one or more M3UA instances offloaded to them, and M3UA instances only (no SUA).

Workaround There are two possible workarounds. You can unconfigure all M3UA and SUA offload instances from linecards that are ingress interfaces for outbound M3UA and SUA traffic, or ensure that all such ingress linecards have at least one M3UA and one sua instance offloaded to them.

- CSCso78286

Symptom During the configuration of ITP on the Cisco 7600 platform, the system allows the user to exceed the maximum number of supported serial interfaces and MTP2 serial links for a PA-MCX-8TE1-M.

Conditions ITP on the 7600 platform only supports a maximum of 126 MTP2 links on a single PA-MCX-8TE1-M. However, configuration allows 127.

Workaround The user should limit the configuration of serial interfaces and MTP2 links to a maximum of 126 for each PA-MCX-8TE1-M.

- CSCso79569

Symptom All linksets become unavailable after an NSO switchover, but the linksets recover shortly afterwards.

Conditions The problem only occurs if a linecard reload is in progress when the switchover is initiated.

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.

- CSCsm66950

Symptom ITP HSL links may fail and recover during an NSO switchover.

Conditions HSL link failures may occur during NSO Switchover when the amount of traffic exceeds 6000 MSU/sec in each direction (60% of the maximum throughput).

Workaround Traffic over HSL links should be engineered below 60% of the maximum stated throughput for the target platform and release.

- CSCsq61641

Symptom There are two possible symptoms. The first symptom is that the linecard I/O Memory becomes depleted after an NSO switchover or linecard OIR. In this case, the **show cs7 asp bindings** command output on a linecard shows multiple ASP bindings stuck in pending state.

The second symptom is that the linecard I/O Memory becomes depleted during normal M3UA operations. In this case, the **show cs7 offload queues** output on a linecard shows a high cs7_info_count.

Conditions The first symptom only occurs when using SGMP. The amount of I/O memory depleted is dependent on the number of M3UA/SUA associations on the LC, the number of bindings, and the traffic rate when the switchover occurs. In the worst case where high traffic is occurring and 100+ ASPs are offloaded to a single processor, and 1000s of bindings exist, the I/O memory leak can consume all of the memory on the card.

The second symptom is restricted to M3UA traffic where the ISUP/TUP/BICC payload size leaves insufficient space to add M3UA headers to the internal packet buffer.

Workaround There are two workarounds for the first symptom. The first is to not use SGMP, but instead use a C-link alternate route for xua destinations. The second is to modify the AS traffic mode to use loadshare roundrobin. To clear the ASP bindings stuck in a pending state, **shut** then **no shut** the affected ASPs.

There is no known workaround for the second symptom.

- CSCsq77114

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

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

- CSCsq84291

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

```
SCCP encoding error, badly formatted or unsupported part
```

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

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

- CSCsr01623

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

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

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

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

- CSCsr09619

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

Conditions This occurs with the following conditions:

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

Workaround There is no known workaround.

- CSCsr58145

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

Conditions The problem occurs under the following conditions:

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

Workaround There are two possible workarounds:

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

Minor

- CSCsr25825

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

Conditions The problem occurs under the following conditions:

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

Workaround You can workaround 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 12.2(18)IXF1

This section documents possible unexpected behavior by Cisco IOS Release 12.2(18)IXF1 and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCsd73254

On the ITP 7600 platform, if a specific software error on the active 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 has only been observed in specific lab tests that force a specific software failure on the active RP.

There is no known workaround.

- CSCsq17850

The SSCOP max-pd parameter fails to be updated when a CS7 profile that modifies the parameter is applied to an HSL linkset.

The problem occurs on ITP 7600 platforms running Cisco IOS release 12.2(18)IXF or earlier.

There is no known workaround.

- CSCso00287

The SUP processor on a distributed Cisco ITP platform or the 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.

The workaround is to turn off GWS console logging. File logging may be used as an alternative.

Resolved Caveats—Cisco IOS Release 12.2(18)IXF1

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(18)IXF1. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCso84249

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

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

This happens when 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.

There is no known workaround.

- CSCsg 35077

A device that is running Cisco IOS software may crash during processing of an Internet Key Exchange (IKE) message. This bug is triggered deep into the IKE negotiation, and an exchange of message between IKE peers is necessary. If IPsec is not configured, it is not possible to reach the point in the IKE negotiation where the bug exists.

For this to occur the device must have a valid and complete configuration for IPsec. IPsec VPN features in Cisco IOS software that use IKE include Site-to-Site VPN tunnels, EzVPN (server and remote), DMVPN, IPsec over GRE, and GET VPN.

The workaround is that customers that do not require IPsec functionality on their devices can use the **no crypto isakmp enable** command in global configuration mode to disable the processing of IKE messages and eliminate device exposure. If IPsec is configured, this bug may be mitigated by applying access control lists that limit the hosts or IP networks that are allowed to establish IPsec sessions with affected devices. This assumes that IPsec peers are known. This workaround may not be feasible for remote access VPN gateways where the source IP addresses of VPN clients are not known in advance. ISAKMP uses port UDP/500 and can also use UDP/848 (the GDOI port) when GDOI is in use.

- CSCsh61946

After an SSO switchover has occurred, the second of two 6000 W DC power supplies in the chassis is shut down.

This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 router when both power supplies are powered on before the SSO switchover occurs.

There is no workaround.

- CSCsd42603

The FRU type of PWR-6000-DC is not displayed properly with the CLI **show idprom power 1:**

```
(FRU is '(power supply type 0.0.0.168)').
```

The expected display is shown below:

```
(FRU is 'DC power supply, 6000 watt')
```

There is no workaround.

- CSCso70775

SCCP XUDT message with optional parameter may be corrupted during inter-instance conversion.

This happens when SCCP XUDT traffic with any optional parameter that undergoes multi-instance conversion.

The workaround is to eliminate SCCP XUDT traffic using optional parameters.

- CSCsq03358

After an MTP2 Link recovers from remote processor outage, the link fails with reason "unknown" then recovers.

This occurs when MTP2 Links that receive an Processor Outage (SIPO) from the adjacent node. This problem only occurs in very rare cases - usually when a large number of links are failing for valid reasons, then receive processor outage from the remote node after the links recover

There is no known workaround. The link recovers on its own.

- CSCso64820

Issuing a **no shutdown** on an ATM (IMA) interface that is already up will reset the interface.

The problem only occurs on ITP 7600 platforms running Cisco IOS release 12.2(18)IXF or earlier.

There is no known workaround.

- CSCso74241

On the 7600 ITP platform, Message Signal Units (MSU) being sent out over an ATM HSL link may be continuously discarded without any notification to the system console after issuing **no shut** on an already active ATM interface. A system console message is required when this condition is detected.

This occurred when a customer issues **no shut** command on an already active ATM interface. See CSCso64820.

The workaround is to not issue **no shut** command on an already active ATM interface.

- CSCso74297

After a Non-Stop Operation switchover on a 7600 ITP, the %DCS7-6-CONFIG_RELOAD_AFTER_SWO message may appear for several enhanced FlexWan slots. These messages will then also appear after every subsequent NSO switchover.

The Switchover initiated from Active to Standby before Distributed CS7 (DCS7) download was complete to all slots.

The workaound is to not issue a manual switchover using the 'redundancy force switchover' prior to seeing the %'DCS7-5-INFO: Start all Links and ASPs for slot <slot>/<bay>' issued for each configured slot/bay.

- CSCso94423

Memory leak on active Supervisor

Occurs on any condition using MTP3 Offload with active line cards.

A workaround is to have the switchover to standby processor re-claim the leaked memory. This should be done prior to processor free memory getting critically low. A good margin would be to have free at least 20% of total processor memory.

- CSCso45349

The 7600 ITP may send a TFC to an adjacent node with a DPC set to the Cisco ITP's local point code.

On the Cisco 7600 router, when traffic is sent to the ITP for GTT, and the result is route-on-global title to a destination that uses a congested link, the ITP sends a TFC with DPC set to the ITP's point code.

There is no known workaround.

- CSCso33607

A flexwan may drop one or more low priority messages intended for the active SUP or RP processor. Under such conditions, an SBETH-3-TOOBIG: EOBC0/0 message will be generated on the SUP or RP processor console to inform the user this event has occurred. No other impact to the system occurs, however

This failure occurs when the max MTU size for communication between Flexwan and SUP or RP processor has been exceeded. The only conditions under which this failure has been observed are periods of heavy stress on the SUP and/or Flexwan. For example, a Flexwan with a large number of links and heavy traffic may incur this error if an supporting interface on board the Flexwan begins to flap.

There is no known workaround.

- CSCso42614

Loadshare distribution of traffic over a combined linkset may not work properly after deleting a route using the same combined linkset on a distributed ITP platform.

This problem occurs on a distributed Cisco ITP platform, when two or more routes exist that use the same combined linkset. The individual linksets are specified in the reverse order, and the last route using a particular individual linkset order is deleted.

Delete one of the individual linkset definitions in ALL routes using the combined linkset, then add the individual linkset back.

- CSCso85809

Link becomes stuck in unavailable state but shows as available in "show cs7 linkset" command on RP.

This problem can occur when the ITP receives a Changeover Order (COO) for the link, then the link quickly goes into and out of processor outage (remote node sends SIPO followed by FISU)

The workaround is to shut / no shut the affected link.

Open Caveats—Cisco IOS Release 12.2(18)IXF

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

- CSCs134355

Two crafted Protocol Independent Multicast (PIM) packet vulnerabilities exist in Cisco IOS software that may lead to a denial of service (DoS) condition. 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-multicast.shtml>.

- CSCsd73254

On the ITP 7600 platform, if a specific software error on the active 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 has only been observed in specific lab tests that force a specific software failure on the active RP.

There is no known workaround.

- CSCso00287

The SUP processor on a distributed Cisco ITP platform or the 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.

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

- CSCso45349

The 7600 ITP may send a TFC to an adjacent node with a DPC set to the Cisco ITP's local point code.

On the Cisco 7600 router, when traffic is sent to the ITP for GTT, and the result is route-on-global title to a destination that uses a congested link, the ITP sends a TFC with DPC set to the ITP's point code.

There is no known workaround.

- CSCso42614

Loadshare distribution of traffic over a combined linkset may not work properly after deleting a route using the same combined linkset on a distributed ITP platform.

This problem occurs on a distributed Cisco ITP platform, when two or more routes exist that use the same combined linkset. The individual linksets are specified in the reverse order, and the last route using a particular individual linkset order is deleted.

Delete one of the individual linkset definitions in ALL routes using the combined linkset, then add the individual linkset back.

Resolved Caveats—Cisco IOS Release 12.2(18)IXF

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

- CSCsd95616

Two crafted Protocol Independent Multicast (PIM) packet vulnerabilities exist in Cisco IOS software that may lead to a denial of service (DoS) condition. 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-multicast.shtml>.

- CSCsg58153

The PA has crashed and is unresponsive

Bad circuits on uplink links cause all the SS7 links to go down and flap continuously.

The workaround is to bring the PA up once it has crashed.

- CSCsk79377

The **remove** option specified in a GTT address conversion table is not applied when performing GTT address conversion.

This only occurs when the GTT address conversion table is used for SCCP conversion across instances when cs7 multi-instance is configured.

There is no known workaround.

- CSCsl08358

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

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 XUUDT 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 is no known workaround.

- CSCsl17157

When using the multi-pvc feature on either ATM-OC3 or ATM-IMA PA, the IP PVC are not carrying the IP traffic properly. IP traffic, either locally terminated or through switched may fail.

On a Cisco 7600 router, multi-pvc is configured, that is "atm nni" on the main interface and sub-interface with IP enabled and configured.

When dealing with IP traffic:

- There is no workaround for the locally terminated IP traffic
- For the traffic going through the box, as long as the network is using static routing, traffic will forward without problems.

When dealing with SS7 traffic:

- SS7 through-traffic to the remote nodes (either LSL or M3UA) works.
- Local **cs7 ping** does not work, the path FW->SUP seems broken.

- CSCsl70663

The same ASP binding may exist for two different ASPs on SGMP mated ITPs.

SGMP enabled and traffic mode = loadshare bindings.

There is no known workaround.

- CSCs170708

The Application Server (AS) state on a linecard shows "dwn-re" when the state on a Supervisor processor shows "down".

SGMP is enabled on the 7600 ITP platform.

There is no known workaround.

- CSCs193462

No linkUp and linkDown SNMP traps are generated when the remote end is down for the controller. No linkUp trap generated when controller is brought up by **no shutdown** CLI

Problem is specific to PA-MCX-8TE1-M and PA-MCX-4TE1-Q port adaptors.

There is no known workaround.

- CSCs188843

Crash when updating time zone with extra long string.

Issuing a lengthy configuration command similar to the following. clock timezone 123456789012345678901234567890 -23 59

Input the correct length for the timezone parameter.

- CSCsm47893

A User Part Unavailable (UPU) message destined for an M3UA AS in a different MTP3 instance is not converted to a DUPU message.

This problem occurs on the Cisco 7600 router when inter-instance conversion is being used. Traffic initiated by an M3UA AS in one instance is sent to an unavailable user part in a different instance, triggering a response mode UPU.

There is no known workaround.

- CSCsm62597

The ITP may choose the wrong clock source when more than one PA with "clock source line secondary" is configured.

If you have more than clock source line secondary defined on the same PA, the first port with this definition will be the primary clock source. In other words, the priority field after the key word secondary is ignored. If you have clock source line primary and 1 or more clock source line secondary defined on the same PA, the first port with one of these definitions will be primary clock source.

There is no known workaround.

- CSCsm76092

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

For example:

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

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

This occurs when ITP has multiple instances configured and default instance conversion configured. You can workaround the problem by entering the default conversion with the **no-route** option:

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

- CSCsm85233

All through-switched ISUP traffic is punted to the SUP. This results in higher CPU utilization on the SUP when running ISUP traffic. This occurs for all incoming link types (MTP2, M2PA, HSL).

If the ISUP traffic is less than 44 bytes and came in over an ATM HSL link, the bytes are added to the end of the packet to make it 44 bytes. So for example, if the ISUP packet is 30 bytes coming in, the outgoing packet is 44 bytes, with the original 30 bytes followed by 14 bytes set to 0.

The problems only occurs if no M3UA is configured on the ITP.

To work around the problem, configure a local M3UA instance.

- CSCso01412

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

```
RMTC-ITP#sh 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 occurs when an ATM link does not activate after reload.

The link comes up after executing a **shut** than **no shut** commands or unplugging and plugging the cable.

- 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
```

To workaround this problem, do not remove links using a cut and paste of a script. Wait 4 to 5 seconds after shutting a link and before issuing the **no link** command.

- CSCsl59128

Cisco ITP does not reject M3UA/sua messages without a Routing Context parameter when the ASP is active in multiple AS's.

Sending ASP is active in multiple AS's.

There is no known workaround.

- CSCs120383

When using ATM configuration and the ATM, IMA E1 or T1 port adapters, the user may need to re-enter ATM related commands after the Cisco 7600 router reloads.

This resolution of CSCs120383 also resolves CSCse13374.

The workaround is to re-enter the commands after the Cisco 7600 router reloads.

Open Caveats—Cisco IOS Release 12.2(18)IXE

This section documents possible unexpected behavior by Cisco IOS Release 12.(18)IXE and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCsh35975

Bad VCD msg observed traffic on the other links and subinterfaces does not seem to be affected.

The below steps cause the condition

- a. shut the main interface and its sub-interfaces that are used in links
- b. no shut the main interface but keep the sub-interfaces shut

There are no known workarounds

- CSCsd34549

An unexpected config_state value is seen during reload or switchover.

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

There are no known workarounds

- CSCsd73254

On the ITP 7600 platform, if a specific software error on the active 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 has only been observed in specific lab tests that force a specific software failure on the active RP.

There are no known workarounds

Resolved Caveats—Cisco IOS Release 12.2(18)IXE

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

- CSCek63758

MSU Rates spike after clearing counters

This problem occurs on all ITP platforms

There are no known workarounds

- CSCsg27676

The SGMP link between ITP mates may flap when an ASP becomes active

This problem occurs on all ITP platforms

There are no known workarounds

- CSCsg58153
 - The PA has crashed and is unresponsive
 - Bad circuits on uplink links cause all the SS7 links to go down and flap continuously
 - The fix is to bring the PA up once it has crashed
- CSCsh69956
 - Syslog messages and 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.
- CSCsi40918
 - The RSP crashed causing a switchover to standby RSP.
 - This crash occurred during normal router operations.
 - There are no known workarounds.
- CSCsi60319
 - The MMSC gateway feature of the ITP is not returning the responding HLR E.164 address to the 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 VIP crashes while processing GTT traffic.
 - This problem occurs with MTP3 offload enabled with a VIP performing GTT on both UDT and XUDT SCCP messages.
 - There are no known workarounds.
- CSCsi68966
 - 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: GTAs entered in config should point to AS name directly instead of PC.
- CSCsi79035
 - The M3UA 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 have shown two.
 - When M3UA ASPs have local-ip addresses from different FlexWANs, then sometimes only one IP address is used by the Sctp instance.
 - Workaround: Doing **shutdown** and **no shutdown** of the affected M3UA instance clears the problem. The output of the command **show ip sctp instance** will now show two local-ip addresses.
- CSCsi98081
 - A buffer leak caused by a large quantity of SNMP traps.
 - This problem occurs on all ITP platforms
 - There are no known workarounds.

- CSCsj36934
7507MX crashes due to a bus error: System returned to ROM by bus error at PC 0x4107D360 TLB (load or instruction fetch) exception, CPU signal 10, PC = 0x4107D360
This occurs during normal operations.
There are no known workarounds.
- CSCsj60899
Flexwan crash while processing outbound M3UA sccp msu 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
New ASP binding during NSO bulk sync causes SYNCERR.
This occurs on an NSO switchover on ITP running M3UA/sua traffic.
There are no known workarounds.
- CSCsk15118
ITP may crash while performing SCCP instance address conversion
This occurs when the following three conditions are met:
 - sccp instance conversion where address conversion is used between instances
 - MSU with more than 16 digits 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 will 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 M2PA link will stop processing received messages and will eventually fail after receiving an SCTP DATA chunk that is 300 bytes or more. The DATA chunk is an invalid message because it is larger than the maximum MSU size allowed on the link, and is discarded before the Forward Sequence Number (FSN) in the M2PA header is updated for the link. This causes all subsequent messages received over the link to be dropped due to an invalid FSN. The link will eventually fail if an SLTM/SLTA is dropped, or when the remote peer can no longer buffer forwarded messages.

The output of 'show cs7 m2pa statistics' and 'show cs7 m2pa' may be used to identify that this problem is occurring. 'show cs7 m2pa statistics' will show an elevated number of UnexpectedFSN_rcvd errors. 'show cs7 m2pa state' will show that the 'bsnr' field is not incrementing despite data chunks being received over the association.

This occurs when ITP receives an SCTP DATA chunk that is 300 bytes or more over an active M2PA link.

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, however, will not prevent the problem from re-occurring.

- CSCsk50308

When configuring an mtp3 route to an M3UA/sua point code, the initial route status is "available" even though the M3UA/sua point code is locally inactive.

This occurs only upon initial route configuration.

Workaround: Do one of the following:

- Bring the M3UA/sua point code active to match the route availability.
- Execute an mtp3 restart.

- CSCsf15218

An SCTP Association is missing from SCTP tables

This occurs when all SS7 sctp based links are not offload to line cards. When VIP in slot 0 is OIR associations are deleted from MIB tables.

There are no known workarounds.

- CSCsj60907

SCCP management messages like SST, SSA, SSC, and SSP do not get processed properly particularly when XUA SGMP association for the SG Mate show some congestion and some of the ASs require re-routing.

This condition happens on 7600 routers when SGMP association for the SG Mate shows congestion and some of the ASs are in re-routing state.

Workaround: Disable SGMP and perform a graceful switchover to the standby SUP.

- CSCsk18339

The Standby Supervisor Module on a 7600 running with an ITP image is constantly reloading due to a Redundancy Facility notification timeout. The following messages are displayed on the Active Supervisor console log about five and a half minutes after the Standby Supervisor is brought online:

```
%OIR-SP-3-PWRCYCLE: Card in module <slot>, is being power-cycled (RF request)
  %OIR-SP-3-PWRCYCLE: Card in module <slot>, is being power-cycled (OIR slot disable)
  %PFREDUN-SP-6-ACTIVE: Standby processor removed or reloaded, changing to Simplex
mode
```

The **show redundancy history** command output shows that the 'CS7 NSO' client failed to complete the RF_PROG_STANDBY_BULK stage of the Redundancy Facility client progression:

```
RF_PROG_STANDBY_BULK(104) CS7 NSO(5081) op=0 rc=0
  RF_EVENT_CLIENT_PROGRESSION(503) CS7 NSO(5081) op=7 rc=0
  *my state = ACTIVE(13) *peer state = UNKNOWN(0)
  Reloading peer (notification timeout)
```

There are three conditions that lead to the problem:

- The 7600 boots up with an ITP configuration (i.e. the **cs7 varian** command is included in the startup-config) and the startup-config does not contain the **cs7 gtt load** command.
- The **cs7 gtt load** command is issued after the 7600 is loaded.
- The Standby Supervisor is reloaded.

- CSCsk19670

SCTP packet retransmission can occur for SIGTRAN protocols. The ITP arp process that handles arp request for SIGTRAN links can inadvertently delete an arp entry and cause packets to not be sent for a period of time. The SCTP protocol detects that the packets have not been acknowledged and will retransmit the packets. There is no packet loss.

The ITP arp process populates arp entries in the IP arp table for destination IP addresses used by SIGTRAN protocols. If a routing protocol is used that generates multiple routes for a destination used by SIGTRAN protocols, the ITP arp process inadvertently deletes each one of the multiple routes and then triggers new arp requests for each route. When arp sends an arp request, the arp entry is marked as incomplete until an arp reply is received. The adjacency entry in the L3 forwarding table is marked as "punt" during the period the arp entry is incomplete and will drop any packets that are presented for forwarding during this window. The SCTP protocols detects that packets were dropped and will retransmit the packets. There is no packet loss.

This occurs when using IP routing protocols that generate multiple routes to a specific destination. The ITP arp process can inadvertently delete an arp entry for SIGTRAN IP destinations.

Workaround: Use static IP routes to the SIGTRAN destinations.

- CSCsk44543

An alignment traceback similar to the following may occur:

```
Sep 12 14:07:56.705: %ALIGN-3-CORRECT: Alignment correction made at 0x42442A70 reading 0x80495C3
Sep 12 14:07:56.705: %ALIGN-3-TRACE: -Traceback= 42442A70 4173CA38 41802774 41802A8C 4173D3EC 4177DBBC 41A4B648 41CD66FC
```

This occurs during normal operation.

There are no known workarounds.

- CSCsi34398

When unconfiguring and reconfiguring OC3 ATM interfaces and associated linksets, with multi-pvc feature, including sub-interface and IP protocol, system may reload unexpectedly.

The exact sequence of operation to recreate that problem has not been identified. Some conditions under an OC3 ATM interface, configuring and unconfiguring sub-interfaces, as well as ip protocol and atm nni.

Avoid configuring and unconfigure multiple times. Once the system is configured, it remains stable.

- CSCsh33248

A 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
```

In a multi-pvc configuration and after a switchover, configuration of a non-existent sub-interface may cause the trace back above.

Don't unconfigure non-existent sub-interfaces

- CSCse11887
IPCALLOCFAIL occurs during OIR of FlexWAN.
The problem occurs intermittently during FlexWAN OIR.
There are no known workarounds.
- CSCsf10777
An ATMPA-3-CMDFAIL may occur when you extract the Flexwan from the chassis.
Occurs only when the Flexwan contains an E1 IMA PA, and the Flexwan is extracted from the chassis. Once the Flexwan is reinserted no additional symptoms occur.
There are no known workarounds if the Flexwan is extracted.

Open Caveats - Release 12.2(18)IXD

CSCsg81906

Symptom An M3UA/SUA ASP may momentarily enter and exit congestion upon receiving a DAUD.

Conditions The problem only occurs when the ITP receives a DAUD with greater than 250 affected PCs.

Workaround The default ASP tx-queue-depth is 1000; adjust this to a higher value to avoid entering congestion.

- CSCsi34398

Symptom When unconfiguring and reconfiguring OC3 ATM interfaces and associated linksets, with multi-pvc feature, including sub-interface and IP protocol, system may reload unexpectedly.

Conditions The exact sequence of operation to recreate that problem has not been identified. Some conditions under an OC3 ATM interface, configuring and unconfiguring sub-interfaces, as well as ip protocol and atm nni.

Workaround Avoid configuring and unconfigure multiple times. Once the system is configured, it remains stable.

- CSCsh33248

Symptom A 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
```

Conditions In a multi-pvc config and after a switchover, configuration of a non-existent sub-interface may cause the trace back above.

Workaround Don't unconfigure non-existent sub-interfaces

- CSCsh35975

Symptom On 7600, bad VCD msg when no shut main int while keep sub-int shut

Conditions In IXC, following the below steps causes the condition

- shut the main interface and its sub-interfaces that are used in links
- no shut the main interface but keep the sub-interfaces shut
- Bad VCD msg observed Maybe a link test msg or alignment msg. Traffic on the other links and subinterfaces does not seem to be affected.

Workaround None

- CSCsd34549

Symptom Unexpected config_state value is seen during reload or switchover.

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

Workaround

- CSCsd73254

Symptom On the ITP 7600 platform, if a specific software error on the active 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.

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

Workaround None

- CSCse11887

Symptom IPCALLOCFAIL occurs during OIR of FlexWAN.

Conditions The problem occurs intermittently during FlexWAN OIR.

Workaround None

- CSCsf10777

Symptom An ATMPA-3-CMDFAIL may occur when you extract the Flexwan from the chassis.

Conditions Occurs only when the Flexwan contains an E1 IMA PA, and the Flexwan is extracted from the chassis. Once the Flexwan is reinserted no additional symptoms occur.

Workaround No workarounds are known if the Flexwan is extracted.

Resolved Caveats - Release 12.2(18)IXD

CSCsg11686

Symptom ITP running tests as defined in Q.781: linkset with 2 links, one of the links is brought out of service, linkset status remains available. When the failed link is re-activated, the ITP is using SIE instead of SIN.. When the second link is brought into service the ITP sends a SIE, the OMLSSU_XMIT_SIE count increases by 1 in the concerned link, and this msg can also be seen on the INET side.

Conditions NA

Workaround None

CSCsg34131

Symptom A 7500 ITP running SCTP offload will experience high CPU when another SCTP node attempts to establish an SCTP association to an offloaded port but on the wrong VIP card. That is:

- ITP with SCTP offload
- Port XXXX offloaded to VIP A
- Port YYYY offloaded to VIP B
- An attempt to establish an SCTP association to port YYYY on VIP A, or to port XXXX on VIP B, will cause high CPU utilization in the RSP.

Conditions When this situation occurs, the high CPU is due to the IP Input process.

Workaround None

CSCsh26503

Symptom ITP changes over with more than 16 combined linksets and corrupts SLT table.

Conditions None

Workaround None

CSCsh28961

Symptom ITP SUA signalling gateway reloads due to process watchdog timeout in the CS7 SCCP Input Process after the ITP memory has been exhausted. This DDTS addresses the watchdog timeout, not the memory depletion.

Conditions None

Workaround None

CSCsh37628

Symptom Running an snmp walk is causing a Bus Error and crash.

Conditions None

Workaround None

CSCsh49591

Symptom Bring an xua point code active on a pair of ITPs with C-link configured. Make sure the point code is configured in an ANSI instance (or ITU with "cs7 national-options TFR" not enabled). Bring the point code inactive on one ITP such that xua traffic is routed via the C-link. Preventive TFP is not sent to the C-link peer when the point code goes inactive.

Conditions None

Workaround None

CSCsh66422

Symptom Possible difficulties moving an instance from one instance to another.

Conditions A linkset is configured in an instance. An alternate route is created to that PC over a different linkset and the route table is saved to a file. Remove the automatically created route over the direct linkset and configure pc-conversion with an alias in instance X in instance Y, the router is reloaded. Remove the pc-conversion but with real alias instances in reverse order. At this point the route still exists in instance X but will not appear in show pc-conversion output.

Workaround The ITP can be reloaded.

CSCsh69956

Symptom Syslog messages & SNMP traps are not generated for clock transitions on the IMA PA.

Conditions None

Workaround None

CSCsh79649

Symptom SUA ASP may cause router crash after shut/no shut.

Conditions None

Workaround None

CSCsh85983

Conditions FW crash & traceback from R&D center. ASP was periodically flapping. See attachments for complete logs of current and prior crashes.

Conditions None

Workaround None

CSCsh91740

- CSCsg93892

Symptom An emergency changeover occurs, instead of the expected normal changeover, when the ATM interface is shutdown. This emergency changeover may cause packet loss.

Conditions The cs7 link associated with this ATM interface is available.

Workaround None

- CSCsf04659

Symptom MSU Rates are reported for non-existent interfaces.

Conditions If a FlexWAN is removed from the system, MSU rates continue to be reported for all interfaces on the affect FlexWAN.

Workaround None

- CSCsf01453

Symptom Disabling triggers during MLR configuration may drop MLR traffic.

Conditions The system sets a timer when you enter MLR configuration mode. When the timer expires all existing configuration is sent to the FlexWANs to update all MLR tables and configurations. This event occurs whether you complete configuration or not. When the configuration is sent to each FlexWAN, MLR is disabled for a short period of time for that FlexWAN. During this time period, MLR processing is not available for that FlexWAN. Also, statistics may incorrectly report for MLR.

Workaround Configure GTT for backup delivery when disabled MLR occurs. It is recommended to configure MLR during maintenance periods of little or no existing traffic.

- CSCsg01213

Symptom Egress FE interface incorrectly reports total output_drops

Conditions This bug is present in 76xx platforms running 12.2(18)IXA and 12.2(18)IXB and 12.2(18)IXB1.

Workaround None

- CSCsg09620

Symptom The beat message is processed by SG between ASPUP and ASPAC.

Conditions This occurs in a timing window where the beat messages are sent by the ASP, immediately after receiving ASP Up Ack from the ITP.

Workaround None

- CSCsg27544

Symptom While processing retrieved paks for M3UA, the SUP encounters a CPUHOG and reloads.

Conditions The CPUHOG and reload happen when the SUP is trying to process a retrieved pak.

Workaround None

- CSCsg40048

Symptom While processing an unexpected message, the SUP reloads in XUA Offload Inbound

Conditions All 7600-based ITPs running M3UA and/or sua.

Workaround None

- CSCsg42706

Symptom SUP shows CS7 XUA ERROR: binding already exists

Conditions None

Workaround None

- CSCsg72008

Symptom A reload occurs after deleting ASP from the AS submode when bindings are available.

Conditions This occurs when routing M3UA/sua traffic for a loadshare bindings AS.

Workaround None. The problem is only cosmetic.

- CSCsg87626

Symptom Updating the AS from dwn-re --> down state on FlexWAN fails.

Conditions This occurs when you are routing M3UA/sua traffic with SGMP enabled, the SGMP association goes down, or the ASP goes inactive on mate.

Workaround None

Open Caveats - Release 12.2(18)IXC

- CSCsg93892

Symptom An emergency changeover occurs, instead of the expected normal changeover, when the ATM interface is shutdown. This emergency changeover may cause packet loss.

Conditions The cs7 link associated with this ATM interface is available.

Workaround None

- CSCsd34549

Symptom Unexpected config_state value is seen during reload or switchover.

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

Workaround There is no known workaround. However, there are no known harmful effects.

- CSCsd73254

Symptom On the ITP 7600 platform, if a specific software error on the active 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.

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

Workaround None

- CSCse11887

Symptom IPCALLOCFAIL occurs during OIR of FlexWAN.

Conditions The problem occurs intermittently during FlexWAN OIR.

Workaround None

- CSCsf04659

Symptom MSU Rates are reported for non-existent interfaces.

Conditions If a FlexWAN is removed from the system, MSU rates continue to be reported for all interfaces on the affect FlexWAN.

Workaround None

- CSCsf10777

Symptom An ATMPA-3-CMDFAIL may occur when you extract the Flexwan from the chassis.

Conditions Occurs only when the Flexwan contains an E1 IMA PA, and the Flexwan is extracted from the chassis. Once the Flexwan is reinserted no additional symptoms occur.

Workaround No workarounds are known if the Flexwan is extracted.

Resolved Caveats - Release 12.2(18)IXC

- CSCsd96345

Symptom An ITP with HSL links running at high utilization (near 100% capacity) of the physical underlying T1/E1, after entering congestion, may begin to flap and continue to flap until traffic is suppressed through TFC messages by the originator.

Conditions HSL link is driven into congestion when priority 0 traffic nears a 100% of the physical T1/E1 capacity.

Workaround None

- CSCsf22759

Symptom XUA packets drop under high traffic with several ASPs.

Conditions Multiple ASPs are sending & receiving M3UA/SUA traffic.

Workaround None

- CSCsf22768

Symptom Active ASPs with zero weight do not use the round robin, as is expected.

Conditions M3UA/SUA traffic routed to a loadshare round robin AS.

Workaround None

- CSCsf29679

Symptom The Instance SLS Shift does not download to FlexWan

Conditions ITU variant, M3UA, or SUA configuration, and cs7 sls-shift, configured to 1, 2, or 3.

Workaround None

- CSCsg01213

Symptom Egress FE interface incorrectly reports total output_drops

Conditions This bug is present in 76xx platforms running 12.2(18)IXA and 12.2(18)IXB and 12.2(18)IXB1.

Workaround None

- CSCsg09620

Symptom The beat message is processed by SG between ASPUP and ASPAC.

Conditions This occurs in a timing window where the beat messages are sent by the ASP, immediately after receiving ASP Up Ack from the ITP.

Workaround None

- CSCsg27544

Symptom While processing retrieved paks for M3UA, the SUP encounters a CPUHOG and reloads.

Conditions The CPUHOG and reload happen when the SUP is trying to process a retrieved pak.

Workaround None

- CSCsg40048

Symptom While processing an unexpected message, the SUP reloads in XUA Offload Inbound

Conditions All 7600-based ITPs running M3UA and/or sua.

Workaround None

- CSCsg42706

Symptom SUP shows CS7 XUA ERROR: binding already exists

Conditions None

Workaround None

- CSCsg72008

Symptom A reload occurs after deleting ASP from the AS submode when bindings are available.

Conditions This occurs when routing M3UA/sua traffic for a loadshare bindings AS.

Workaround None. The problem is only cosmetic.

- CSCsg87626

Symptom Updating the AS from dwn-re --> down state on FlexWAN fails.

Conditions This occurs when you are routing M3UA/sua traffic with SGMP enabled, the SGMP association goes down, or the ASP goes inactive on mate.

Workaround None

Open Caveats - Release 12.2(18)IXB1

- CSCsd34549

Symptom Unexpected config_state value is seen during reload or switchover.

Conditions Error seen with IMA card after a reload or switchover.

Workaround There is no known workaround. However, there are no known harmful effects.

- CSCsd73254

Symptom On the ITP 7600 platform, if a specific software error on the active RP causes the active RP to fail, the standby SUP may not detect the failure, but instead the active SUP may reload the ITP to restore ITP manageability.

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

Workaround None

- CSCsd96345

Symptom An ITP with HSL links running at high utilization near 100% capacity of the physical underlying T1/E1, after entering congestion may begin to flap and continue to flap until traffic is suppressed via TFC messages by the originator.

Conditions HSL link is driven into congestion with priority 0 traffic at near 100% of the physical T1/E1.

Workaround None

- CSCse11887

Symptom IPCALLOCFAIL occurs during OIR of FlexWAN.

Conditions Problem intermittently occurs during FlexWAN OIR.

Workaround None

- CSCsf01453

Symptom MLR traffic may be dropped when triggers are disabled during MLR configuration.

Conditions The system sets a timer when you enter MLR configuration mode. When the timer expires all existing configuration is sent to the FlexWANs to update all MLR tables and configurations. This event occurs whether you complete configuration or not. When the configuration is sent to each FlexWAN, MLR is disabled for a short period of time for that FlexWAN. During this time period, MLR processing is not available for that FlexWAN. Also, statistics may incorrectly report for MLR.

Workaround Configure GTT for backup delivery during occurrences where MLR is disabled. Configure MLR during maintenance periods where traffic may be low or non-existent.

- CSCsf03311

Symptom SUP and FlexWAN ASP configuration becomes mismatched.

Conditions If user modifies the configuration of an existing ASP, the configuration is saved on SUP but never relayed to the FlexWAN. Thus, the FlexWAN continues to use the original configuration parameters, use (for example, src and destination ports).

Workaround ASPs must be deleted completely then reconfigured with new parameter data.

- CSCsf04659

Symptom MSU Rates are reported for non-existent interfaces.

Conditions If a FlexWAN is removed from the system, MSU rates continue to be reported for all interfaces on the affect FlexWAN.

Workaround None

Resolved Caveats - Release 12.2(18)IXB

- CSCek38607

Symptom ITP running on the Cisco 7600 platform may experience error messages and global title translation table errors if a switchover from the active RP to the standby RP happens after the system reaches ITP NSO mode, but before GTT table download to the line cards is complete.

Conditions The switchover must happen between the system reaching NSO state (indicated by console message) and GTT table download complete (also indicated via console log message).

Workaround Avoid issuing a redundancy force-switchover until after the system has reached NSO mode and the GTT download complete message has been displayed on the console or in system logs.

- CSCek38702

Symptom An ITP running on Cisco 7600 platform when switching from active RP to standby RP due to a failure on the active RP due to certain software errors may encounter a switchover delay. Normally this delay is expected to be 2 to 4 seconds, but in this failure mode, the delay may be longer. Depending on

the traffic load and the length of switchovers, some links may be taken out of service temporarily due to local or remote protocol errors. If the duration of the switchover is long enough, some FlexWANs may be reloaded by the new active to clear the condition.

Conditions This has only been observed in specific lab tests using internal debug commands that force software failures on the active RP. This issue only happens a small percentage of the times this specific test is executed.

Workaround None

- CSCsd83706

Symptom Unexpected FlexWAN reload upon update and save of MLR configuration.

Conditions This is a timing related bug and it does not happen every time. When an update of MLR trigger or route table configuration is done, followed by a save configuration, some FlexWANs might unexpectedly reload.

Workaround None

- CSCsd91506

Symptom Under rare circumstances, packets may be lost during rerouting of packets destined for a failed ASP to an active ASP in an AS.

Conditions The problem may occur when there are two or more active ASPs in an AS, and one of the active ASP's SCTP association fails.

Workaround None

- CSCsd92741

Symptom Under rare circumstances, a spurious memory access may occur at bootup on a FlexWAN with M2PA links.

Workaround None

- CSCsd94495

Symptom All FlexWANs reload.

Conditions Occurs when user deletes an MLR secondary trigger directly.

Workaround If it is necessary to remove a secondary trigger, delete the primary trigger and then add the primary back. The secondary trigger will be deleted and no reload on FlexWANs will occur.

- CSCsd94659

Symptom MLR continues to route data based on an address which was deleted from an existing MLR address-table. The deleted address does not appear in the MLR address-table configuration, and it is not displayed via the **show cs7 mlr address-table** on the RP.

Conditions This problem only occurs when the user configures multiple address-table names that are unique only in the use of upper/lower case (for example, TABLENAME and TableName).

Workaround Define unique MLR address-table names, regardless of the use of upper/lower case. Do not configure an address-table name which consists of the same characters in a different case.

Open Caveats - Release 12.2(18)IXA

- CSCek38607

Symptom ITP running on the Cisco 7600 platform may experience error messages and global title translation table errors if a switchover from the active RP to the standby RP happens after the system reaches ITP NSO mode, but before GTT table download to the line cards is complete.

Conditions The switchover must happen between the system reaching NSO state (indicated by console message) and GTT table download complete (also indicated via console log message).

Workaround Avoid issuing a redundancy force-switchover until after the system has reached NSO mode and the GTT download complete message has been displayed on the console or in system logs.

- CSCek38702

Symptom An ITP running on Cisco 7600 platform when switching from active RP to standby RP due to a failure on the active RP due to certain software errors may encounter a switchover delay. Normally this delay is expected to be 2 to 4 seconds, but in this failure mode, the delay may be longer. Depending on

the traffic load and the length of switchovers, some links may be taken out of service temporarily due to local or remote protocol errors. If the duration of the switchover is long enough, some FlexWANs may be reloaded by the new active to clear the condition.

Conditions This has only been observed in specific lab tests using internal debug commands that force software failures on the active RP. This issue only happens a small percentage of the times this specific test is executed.

Workaround None

- CSCsd34549

Symptom Unexpected config_state value is seen during reload or switchover.

Conditions Error seen with IMA card after a reload or switchover.

Workaround There is no known workaround. However, there are no known harmful effects.

- CSCsd73254

Symptom On the ITP 7600 platform, if a specific software error on the active RP causes the active RP to fail, the standby SUP may not detect the failure, but instead the active SUP may reload the ITP to restore ITP manageability.

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

Workaround None

- CSCsd83706

Symptom Unexpected FlexWAN reload upon update and save of MLR configuration.

Conditions This is a timing related bug and it does not happen every time. When an update of MLR trigger or route table configuration is done, followed by a save configuration, some FlexWANs might unexpectedly reload.

Workaround None

- CSCsd91506

Symptom Under rare circumstances, packets may be lost during rerouting of packets destined for a failed ASP to an active ASP in an AS.

Conditions The problem may occur when there are two or more active ASPs in an AS, and one of the active ASP's SCTP association fails.

Workaround None

- CSCsd92741

Symptom Under rare circumstances, a spurious memory access may occur at bootup on a FlexWAN with M2PA links.

Workaround None

- CSCsd94495

Symptom All FlexWANs reload.

Conditions Occurs when user deletes an MLR secondary trigger directly.

Workaround If it is necessary to remove a secondary trigger, delete the primary trigger and then add the primary back. The secondary trigger will be deleted and no reload on FlexWANs will occur.

- CSCsd94659

Symptom MLR continues to route data based on an address which was deleted from an existing MLR address-table. The deleted address does not appear in the MLR address-table configuration, and it is not displayed via the **show cs7 mlr address-table** on the RP.

Conditions This problem only occurs when the user configures multiple address-table names that are unique only in the use of upper/lower case (for example, TABLENAME and TableName).

Workaround Define unique MLR address-table names, regardless of the use of upper/lower case. Do not configure an address-table name which consists of the same characters in a different case.

- CSCsd96345

Symptom An ITP with HSL links running at high utilization near 100% capacity of the physical underlying T1/E1, after entering congestion may begin to flap and continue to flap until traffic is suppressed via TFC messages by the originator.

Conditions HSL link is driven into congestion with priority 0 traffic at near 100% of the physical T1/E1.

Workaround None

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2006 Cisco Systems, Inc. All rights reserved.