



# Release Notes for IP Transfer Point (ITP) 7600 for Cisco IOS Release 12.2(18)IXD1

---

7/30/2007

Cisco IOS Release 12.2(18)IXD1

These release notes for the ITP 7600 platform describe the enhancements provided in Cisco IOS Release 12.2(18)IXD1 and later. 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 8](#).

## Contents

These release notes include the following topics:

- [System Requirements, page 1](#)
- [New and Changed Information, page 3](#)
- [Caveats for Cisco IOS Release 12.2\(18\)IX, page 8](#)

## 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](#)

[Hardware Supported, page 2](#)

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



---

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

© 2006 Cisco Systems, Inc. All rights reserved.

## Memory Requirements

**Table 1** *Images and Memory Recommendations for the ITP 7600 Cisco IOS Release 12.2(18)IXD1*

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)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 3** *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 4** *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 5 shows the supported interfaces for the ITP 7600 platform.

**Table 5** *Supported Interfaces for the Cisco ITP 7600*

Interface or Linecard	Introduced In <sup>1</sup>
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

**Table 5**      **Supported Interfaces for the Cisco ITP 7600**

Interface or Linecard	Introduced In <sup>1</sup>
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)IXD1

No new hardware features are supported by the ITP 7600 for Cisco IOS Release 12.2(18)IXD1.

### New Software Features in Release 12.2(18)IXD1

No new software features are supported by the ITP 7600 for Cisco IOS Release 12.2(18)IXD1.

### 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

Platforms: Cisco 7604, Cisco 7606, Cisco 7609, Cisco 7613

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

Platforms: Cisco 7604, Cisco 7606, Cisco 7609, Cisco 7613

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

Platforms: Cisco 7604, Cisco 7606, Cisco 7609, Cisco 7613

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

Platforms: Cisco 7604, Cisco 7606, Cisco 7609, Cisco 7613

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

Platforms: Cisco 7604, Cisco 7606, Cisco 7609, Cisco 7613

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

Platforms: Cisco 7604, Cisco 7606, Cisco 7609, Cisco 7613

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

Platforms: Cisco 7604, Cisco 7606, Cisco 7609, Cisco 7613

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

Platforms: Cisco 7604, Cisco 7606, Cisco 7609, Cisco 7613

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

Platforms: Cisco 7604, Cisco 7606, Cisco 7609, Cisco 7613

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)

Platforms: Cisco 7604, Cisco 7606, Cisco 7609, Cisco 7613

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)

Platforms: Cisco 7604, Cisco 7606, Cisco 7609, Cisco 7613

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)

Platforms: Cisco 7604, Cisco 7606, Cisco 7609, Cisco 7613

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

Platforms: Cisco 7604, Cisco 7606, Cisco 7609, Cisco 7613

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

Platforms: Cisco 7604, Cisco 7606, Cisco 7609, Cisco 7613

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

Platforms: Cisco 7604, Cisco 7606, Cisco 7609, Cisco 7613

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

### Hardware Caveats

None

### Open Caveats - Release 12.2(18)IXD1

This section documents possible unexpected behavior by Cisco IOS Release 12.2(18)IXD1 and describes only severity 1 and 2 caveats and select severity 3 caveats.

There are no known open caveats for Cisco IOS Release 12.2(18)IXD1.

### Resolved Caveats - Release 12.2(18)IXD1

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(18)IXD1. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCef77013

Cisco IOS and Cisco IOS XR contain a vulnerability when processing specially crafted with a Type 0 Routing Header present. Exploitation of this vulnerability can lead to leakage on affected Cisco IOS and Cisco IOS XR devices, and may also result in a affected Cisco IOS device. Successful exploitation on an affected device running Cisco not result in a crash of the device itself, but may result in a crash of the IPv6 subsystem. Cisco has made free software available to address this vulnerability for affected customers are workarounds available to mitigate the effects of the vulnerability.

This advisory is posted at

<http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-IPv6-leak.shtml>.

- CSCin95836

The Cisco Next Hop Resolution Protocol (NHRP) feature in Cisco IOS contains a vulnerability that can result in a restart of the device or possible remote code execution. NHRP is a primary component of the Dynamic Multipoint Virtual Private Network (DMVPN) feature. NHRP can operate in three ways: at the link layer (Layer 2), over Generic Routing Encapsulation (GRE) and multipoint GRE (mGRE) tunnels and directly on IP (IP protocol number 54). This vulnerability affects all three methods of operation.

NHRP is not enabled by default for Cisco IOS. This vulnerability is addressed by Cisco bug IDs CSCin95836 for non-12.2 mainline releases and CSCsi23231 for 12.2 mainline releases.

This advisory is posted at

<http://www.cisco.com/warp/public/707/cisco-sa-20070808-nhrp.shtml>.

- CSCsj44081

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

Workaround: None

- CSCsj53415

When traffic goes through GTT which results in going to an xUA AS, but is blocked by outbound GWS, the buffer is lost. Eventually all buffers are exhausted and the links fail and do not recover. Show buffers show a huge number of CS7 buffers and a huge number of misses in the global pool. The CS7 buffers keep increasing until the links fail.

Workaround: If the links fail, a reload of the individual line card that contains the inbound links or reload of the entire router is required. Removing the outbound GWS rule prevents the problem.

- CSCsi79035

M3UA ASP multi-homing test fails when one interface is disconnected even though there are multiple local-IP addresses are configured on multiple interfaces. The output of the **show ip sctp instance** shows only one local-ip address when it should have shown two.

Workaround: By doing shutdown and no shutdown of the affected M3UA instance clears the problem. The output of the command show ip sctp instance would show two local-ip addresses.

- 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 can happen 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.

- CSCsj60899

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.

Workaround: None

## 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 removing configurations or repeating the configuration of 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

- 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
- c. 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 KTF 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 the Cisco Square Bridge logo 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, BPX, 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, Networking Academy, Network Registrar, *Packet*, 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. (0705R)

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.

