



ITP Traps, Troubleshooting Tips, and Error Messages

This chapter includes the following sections:

- [ITP Traps, page 754](#)
- [Troubleshooting Tips, page 756](#)
- [GTT Error Messages, page 759](#)

ITP Traps



Note

The `snmp-server enable traps cs7` global configuration command activates all traps associated with the ITP. See the command reference entry for details about this command.

CISCO-ITP-RT-MIB

The current implementation of CISCO-ITP-RT-MIB supports the following traps:

Route state change trap(`cItpRouteStateChange`)

This trap is generated whenever the ability to route data to a particular destination changes states. This trap is disabled by default.

The route state change trap consists of the following fields:

- The route state change counter(`cItpRtStateChangeCount`).
- Flag to indicate whether notifications have been suppressed (`ItpRtNotifInfoSuppressedFlag`).
- List of destinations that have changed states(`ItpRtNotifInfoStateChanges`) formatted as an octet string.

CISCO-ITP-SP-MIB

The current implementation of CISCO-ITP-SP-MIB supports the following traps:

Linkset state change trap

This trap is generated when the state of a linkset changes. This trap is disabled by default.

The linkset state change trap consists of the following fields:

- The Common Language Location Codes.
- The linkset new state as follows:
 - available: Traffic may flow over this linkset.
 - shutdown: This linkset has been forced to an unavailable state by an administrative action.
 - unavailable: The linkset is currently unable to support traffic. Activation of this linkset will occur as required by protocol.
- The linkset display name.
- The source point-code formatted as an ASCII string.
- The adjacent point-code formatted as an ASCII string.

Link state change trap

This trap is generated when the state of a link changes. This trap is disabled by default.

The link state change trap consists of the following fields:

- The Common Language Location Codes.
- The link new state as follows:

- available: Traffic may flow over this linkset.
 - failed: Traffic management has detected a failure that prevents activating this linkset.
 - shutdown: This linkset has been forced to an unavailable state by an administrative action.
 - unavailable: The linkset is currently unable to support traffic. Activation of this linkset will occur as required by protocol.
- The link display name.
 - The source point-code formatted as an ASCII string.
 - The adjacent point-code formatted as an ASCII string.
 - The link reason code as defined in cItpSpLinkStateReason.

Link congestion change trap

The cItpSpLinkRcvdUtilChange and cItpSpLinkSentUtilChange traps provide information on the utilization of links. These traps are disabled by default.

The cItpSpLinkRcvdUtilChange trap comprises the following information:

- The Common Language Location Codes.
- The link receive utilization state.
- The link display name.
- The source point code formatted as an ASCII string.
- The adjacent point code formatted as an ASCII string
- The link receive utilization.

The cItpSpLinkSentUtilChange trap comprises the following information:

- The Common Language Location Codes.
- The link sent utilization state.
- The link display name.
- The source point code formatted as an ASCII string.
- The adjacent point code formatted as an ASCII string
- The link sent utilization.

CISCO-ITP-SCCP-MIB

The current implementation of CISCO-ITP-SCCP-MIB supports the following trap:

GTT Mated Application (MAP) State change trap

This trap is generated when the state of a Mated Application subsystem changes.

This trap is disabled by default.

The GTT MAP state change trap consists of the following fields:

- The Common Language Location Codes.
- Signalling Point Display Name formatted as an ASCII string.
- MAP point-code (PC) formatted as an ASCII string.
- MAP subsystem number (SSN) formatted as an ASCII string.

- MAP subsystem status which can be allowed or prohibited.

CISCO-ITP-XUA-MIB

The current implementation of CISCO-ITP-XUA-MIB (for managing ASPs, ASs, Mated Pair Signaling Gateways for M3UA and SUA) supports the following traps:

- The cItpXuaAspStateChange, cItpXuaAsStateChange, and cItpXuaSgmStateChange traps provide information on the state changes of the ASPs, ASes and SG Mate respectively. These traps are disabled by default.
- The cItpXuaAspStateChange trap consist of the following information:
 - The Common Language Location Codes.
 - The name of the ASP formatted as an ASCII string.
 - The name of the AS to which the ASP belongs formatted as an ASCII string.
 The state can be down, inactive or active.
- The cItpXuaSgmStateChange trap consist of the following information:
 - The Common Language Location Codes.
 - The name of the SG Mate formatted as an ASCII string.
 The state which can be inactive or active.
- The cItpXuaAsStateChange trap consist of the following information:
 - The Common Language Location Codes.
 - The name of the AS formatted as an ASCII string.
 The state which can be down, inactive, pending or active.

Troubleshooting Tips

Bouncing links:

1. Verify the origination point code (OPC), destination point code (DPC), and variant for the link.

The OPC and variant can be seen in the output of the **show cs7** command. Look for the lines with “Point Code” and “SS7 Variant.”

The DPC (which is the adjacent point code) for the link can be seen in the output of the **show cs7 linkset linkset-name brief** command. The adjacent point code follows the “apc” label.

2. Make sure that the Signal Link Code (SLC) matches on both ends of the link.

Issue the command **show cs7 linkset linkset-name** on the routers on each end of the linkset under investigation. The SLC value appears under the “SLC” heading. The SLC value is in the range 0-15.

Note the interface names for the SLCs. Then check that the cables connect the desired interfaces on the two routers. For a serial link, verifying that the cable directly connects the two interfaces is sufficient.

```
Router# show cs7 linkset polaris
lsn=polaris      apc=1.5.1      state=avail
  SLC  Interface      Service  PeerState      Inhib
  00   Serial0/0      avail   -----      ----
```

For channelized T1/E1, the cable must connect the correct interfaces. The same channel-group number must be used on both ends of any given link. The channel-group number is the number after the colon in the interface name. For example, in Serial4/0/0:1 the channel number is 1. The channel-groups must be identically configured to use the same time slots on the controllers on both ends.

The following is output of the **show run** command:

```
controller T1 4/0/0
  framing esf
  clock source line
  linecode b8zs
  channel-group 0 timeslots 1
  channel-group 1 timeslots 2

interface Serial4/0/0:1
  bandwidth 64
  no ip address
  ip mtu 1500
  encapsulation mtp2
  no ip route-cache distributed
  load-interval 30
```

The following is output of the **show cs7 linkset polaris** command:

```
lsn=polaris      apc=1.5.1      state=avail
  SLC  Interface          Service  PeerState      Inhib
   00  Serial4/0/0:0      avail    -----        -----
   01  Serial4/0/0:1      avail    -----        -----
```

For SCTP peer links, the remote and local peers and IP addresses must be configured on the two routers to point to each other. See the [“Verify M2PA Links” section on page 144](#).

3. Use the debugs to see if the router is sending the appropriate LSSUs and if any are being received.

To check whether Link Status Signal Units (LSSUs) are being exchanged with the adjacent point code on the linkset being investigated, enter the following debug command:

```
Router# debug cs7 mtp3 mgmt event SLTC linkset polaris
```

Periodic output such as the following appears:

```
4d23h:CS7 MTP3 Event:To:SLTC Fm:HMRT Ev:LTM_signal polaris 0
4d23h:CS7 MTP3 Event:To:SLTC Fm:LSAC Ev:start_link_test polaris 0
4d23h:CS7 MTP3 Event:To:SLTC Fm:HMRT Ev:LTA_signal polaris 0
4d23h:CS7 MTP3 Event:To:LSAC Fm:SLTC Ev:SLT_successful polaris 0
```

To stop the debug, enter the following command:

```
Router# undebug cs7 mtp3 mgmt event SLTC linkset polaris
```

4. Check the MTP2 statistics for excessive AERM & SUERM errors on the link. This would indicate a potential facility issue such as line encoding (B8ZS, ESF) or a hardware failure.

Enter the following command for the interface under investigation:

```
Router# show cs7 mtp2 statistics serial0/0
```

Look for the following lines:

```
OMAERMCOUNT          = 1
OMAERMFaILCOUNT    = 0
OMSUERMCOUNT         = 1
OMSUERMFaILCOUNT   = 0
```

Excessive values indicate hardware failures or configuration errors.

5. Finally, check to see if gateway screening or access lists are being used on the linkset.

Follow the instructions in the [“Gateway Screening: Defining an Access List and Applying It to a Linkset Definition” section on page 135](#) to ensure that messages are not being screened out inadvertently.

GTT Error Messages

Several scenarios exist when the ITP cannot successfully perform a GTT. These are mostly due to network conditions (such as a linkset outage) or database configuration issue (such as a non-provisioned GTA). The following table lists the GTT error messages currently supported by the ITP.


Note

For each message the arriving linkset shall be printed along with several fields from the SCCP portion of the message.

Table 38 GTT Error Messages

Error Text	Correction Procedures
SCCP did not find SSN in translation or MSU	This error occurs during final GTT when the operator did not provision an explicit SSN for a GTA and is relying on the SSN being previously set in the MSU. To correct this problem, either explicitly provision a SSN for the given GTA, or inform the originating node to include the needed CDPA SSN in the message.
SCCP received message for with no called party SSN present.	In the ANSI domain the ITP requires room in the message to replace the CDPA SSN when performing final GTT. To correct this problem, inform the originating node to include the SSN in the CDPA portion, even if it is zero.
SCCP received message with no translation for GTA.	A matching selector was found for the message, but no matching digits were located in the GTA table. To correct this problem, add the needed GTA to the appropriate selector.
SCCP received message for which no selector is defined.	No matching selector was found. To correct this problem, add the needed selector and GTA to the GTT database.
SCCP failed to translate: DPC=%s is not available.	GTT could not complete since the chosen destination is not available. To correct this problem, ensure at least one route to the destination is available.
SCCP failed to translate: DPC=%s is congested.	GTT could not complete since the chosen destination is congested. To correct this problem, reduce traffic to the destination to prevent congestion.
Subsystem is not available for the translated node CDPA DPC=%s SSN=%d.	GTT could not complete since the chosen destination is not available. To correct this problem, ensure the subsystem chosen is available.
Subsystem is congested for the translated node CDPA DPC=%s SSN=%d.	GTT could not complete since the chosen subsystem is congested. To correct this problem, ensure the subsystem chosen is available and not congested.
SCCP failed to translate, no MAP entry.	This error occurs during final GTT when the operator did not provision an explicit SSN for a GTA and is relying on the SSN being previously set in the MSU. In this case the SSN was set in the message, but a matching PC/SSN could not be found in the GTT MAP table. To correct this problem, ensure the subsystem chosen is provisioned in the GTT MAP table.
MTP3 was unable to route the message CDPA PC=%s SSN=%d.	GTT could not complete since the chosen point-code could not be reached by MTP3. To correct this problem, ensure the point-code is available via MTP3.
SCCP received message with hop counter expired.	This error results when a XUDT message arrives with a hop-counter that is not valid or has expired. To correct this problem, examine the network for circular SCCP routing or increase the originating hop-count to account for the needed hops to reach the final destination.

Table 38 *GTT Error Messages (continued)*

Error Text	Correction Procedures
SCCP MGMT received message with invalid routing indicator.	This error results when SCCP management receives a message with a routing indicator not equal to "route on PCSSN". To correct this problem, notify the originator of the message to correct the invalid format.
SCCP received message for GTT of an invalid type.	This error results when SCCP receives a message with an unsupported type or class. The ITP currently supports class 0 and 1 UDT and XUDT message types. To correct this problem, notify the originator of the message to correct the invalid/unsupported format.
SCCP translated message to application group with no available members.	This error results when GTT cannot complete because there are no available members in the chosen application group. To correct this problem, ensure that there is at least 1 member available in the chosen application group.

