C H A P T E R 4

SS7 SIGTRAN Troubleshooting

Revised: July 2010, OL-23039-01

This chapter describes tools and procedures for troubleshooting SIGTRAN problems on the Cisco BTS 10200 Softswitch and Cisco ITP, for clearing Cisco BTS 10200 Softswitch alarms, and for troubleshooting network problems. When an alarm is raised on the Cisco BTS 10200, a series of steps may be required to determine the source of the problem and may include viewing other alarms, invoking command line interface (CLI) status and control commands, viewing the Cisco BTS 10200 logs, and invoking ITP control and status requests.

This chapter contains the following sections:

- Cisco ITP Troubleshooting Procedures
- Cisco BTS 10200 Softswitch Troubleshooting Procedures
- Troubleshooting Cisco BTS 10200 Softswitch Alarms
- Debugging Network Problems for TCAP/SCCP Applications
- Troubleshooting With the Query Command

Cisco ITP Troubleshooting Procedures

The following procedures are useful for troubleshooting problems on the Cisco ITP.

ITP System Messages

The Cisco ITP displays system messages when you are logged in to the console port. Some of these messages are similar to alarms. Analyzing ITP system messages is outside the scope of this document. For details concerning ITP system messages, please see the *ITP Operations Manual*.

✎
Note   When debugging the ITP, note the version of the ITP so the associated *ITP Operations Manual* can be consulted.

Logging On to the ITP

Some of the troubleshooting sections in this chapter require the user to log on to the ITP. Access the ITP through the associated console server or through direct access with a console cable. You need the username and password to access the ITP.

Troubleshooting the ITP will require you to be in ITP enable mode. To get into enable mode, after logging in to the ITP, type **enable**. You will be prompted for the enable password.

Viewing the ITP Configuration

To view the ITP configuration, log in to the ITP and get into enable mode. Enter the command **show run**. The configuration will be displayed. Continue to hit the enter key until you have viewed the entire configuration, or type **q** to stop viewing the configuration.

ITP Status Commands

The following ITP commands are helpful for displaying the status of ITP resources:

- **show cs7** as—Retrieves the AS status.
- **show cs7 asp**—Retrieves the ASP status.
- **show cs7 linkset**—Retrieves the SS7 linkset status.
- **show cs7 route**—Retrieves the SS7 route status.
- **show cs7 group state**—Retrieves the SG-Group status.

Controlling ITP Resources

Change the administrative state of an ITP resource as follows:

Step 1 Log on to the ITP, and get into configure mode.

Step 2 Type the first configuration line of the resource that you want to control.

Step 3 Type **shut** to take the resource out of service, or type **no-shut** to place the resource back in service.

The following example takes a linkset out of service:

```
va-2651-33# conf t
```

Enter configuration commands, one per line

```
va-2651-33(config)# cs7 linkset lset1 1.1.20

va-2651-33(config-cs7-ls)# shut
*May 19 12:32:13.827: %CS7MTP3-5-ACTDEACTLINKSET: Linkset lset1 deactivation is in
progress
*May 19 12:32:13.827: %CS7MTP3-5-LINKUPDOWN: Link 0 in linkset lset1 is down
```

To put the linkset back in service, type the following command:

```
va-2651-33(config-cs7-ls)# no shut
*May 19 12:33:47.704: %CS7MTP3-5-ACTDEACTLINKSET: Linkset lset1 activation is in progress
*May 19 12:33:47.704: %CS7MTP3-5-ACTDEACTLINK: Link 0 linkset lset1 activation is in
progress
```

Cisco BTS 10200 Softswitch Troubleshooting Procedures

The following procedures are useful for troubleshooting problems on the Cisco BTS 10200 Softswitch:

- Using Cisco BTS 10200 Softswitch CLI Commands
- Viewing Cisco BTS 10200 Softswitch Logs

Using Cisco BTS 10200 Softswitch CLI Commands

In the following sections, examples of BTS CLI commands are used to aid in resolving BTS alarms. The following CLI commands are helpful to display and clear alarms.

To display all the currently active alarms, enter the following command at a CLI prompt:

show alarm

To display all alarms of a specific type, enter:

show alarm type=<alarm type>

To clear an alarm, enter the following command:

clear alarm id=<alarm id>

For a detailed description of the CLI commands that are used, see the *Cisco BTS 10200 Softswitch CLI Database.*

Viewing Cisco BTS 10200 Softswitch Logs

Viewing Cisco BTS 10200 logs is helpful when debugging M3UA related objects on the Cisco BTS 10200. Specific string patterns are printed out by the M3UA Interface Module and are useful to determine what is occurring in the log. These strings are formatted as follows:

```
MIM <functional area> <network object>
```

Functional areas include:

- CFG
- STATUS
- PDU
- STATISTICS
- CTRL
- PLATFORM

Network objects include:

- SCTP

- SGP

- SG

- DPC

- OPC

- ROUTING-KEY

- CALL-CONTROL-ROUTE

Search or grep the following example strings when searching the Cisco BTS 10200 logs:

- MIM CFG SCTP—Display how the Stream Control Transmission Protocol (SCTP) has been configured at startup.

- MIM PDU—Trace the incoming messages at the Multipurpose Internet Mail (MIM) layer.

- MIM STATUS DPC—Display how the Destination Point Code (DPC) status has changed in the system.

- MIM STATUS SCTP—Display how the SCTP status has changed in the system.

- MIM PLATFORM—Determine if a platform state change has been issued to the Signaling Gateway Adapter (SGA)/MIM module.

- MIM CTRL SCTP—Determine if an SCTP association has been administratively taken out of service or put back in service.

Troubleshooting Cisco BTS 10200 Softswitch Alarms

When an alarm is raised on the BTS, you must determine whether the issue is in the IP network, on the ITP, or in the public switched telephone network (PSTN). Subsequent sections provide troubleshooting steps for the following BTS Signaling System 7 (SS7) and SIGTRAN related alarms raised on the BTS. Click on the alarm name to display troubleshooting information for that alarm at both the MTP3-User Adaptation Layer (M3UA) and Single User Account (SUA) layers.

Table 4-1   Cisco BTS 10200 Softswitch SS7 and SIGTRAN Alarms

Alarm Type	Alarm Name	Alarm Severity
SIGNALING(23)	DPC Unavailable	MAJOR
SIGNALING(116)	DPC User Part Unavailable	MAJOR
SIGNALING(24)	DPC Congested	MINOR
SIGNALING(110)	Signaling Gateway Group Is Out of Service	CRITICAL
SIGNALING(113)	Signaling Gateway Failure	MAJOR
SIGNALING(114)	Signaling Gateway Process Is Out of Service	MAJOR
SIGNALING(109)	SCTP Association Failure	MAJOR
SIGNALING(111)	SCTP Association Degraded	MINOR
SIGNALING(112)	SCTP Association Configuration Error	MINOR
SIGNALING(122)	M3UA Cannot Go Active	MAJOR
SIGNALING(121)	M3UA Cannot Go Standby	MAJOR

Alarm Type	Alarm Name	Alarm Severity
SIGNALING(127)	TCAP Binding Failure	MAJOR
SIGNALING(124)	Remote Subsystem Is Out Of Service	MINOR

DPC Unavailable

This alarm indicates that the BTS is unable to communicate with the specified DPC in the SS7 network. Determine if the issue is a communication problem between the BTS and the ITP or if it is related to communication problems between the ITP and the DPC by following these steps:

Step 1   Use the BTS CLI **show alarm** command to determine if there is an active Signaling Gateway Group Out of Service alarm. This will occur if communication has been lost to both of the SGs in the SG-Group. If so, proceed to the "Signaling Gateway Group Is Out of Service" section on page 4-7. Otherwise, proceed to Step 2.

Step 2   Determine if there is an M3UA Cannot Go Active alarm. This occurs if, at the time of startup or failover, the BTS is not able to communicate with any of the SGs. If this is the case, proceed to the "M3UA Cannot Go Active" section on page 4-11. Otherwise, proceed to Step 3.

Step 3   If you arrive at this step, there is probably communication between the BTS and ITP at the M3UA and SUA layers, and a communication problem exists between the ITP and the unavailable DPC. To confirm this, log on to each ITP, get into enable mode, and enter **show cs7 route**. The output of this command tells you if the associated DPC is accessible or not from the ITP point of view and will look similar to the following:

```
va-2651-82# show cs7 route

Destination          Prio Linkset Name        Route
-------------------- ---- ------------------- -------
229.123.2/24    INACC   1  lset1chn              UNAVAIL
```

This output indicates that DPC 229.123.2 is unavailable from the ITP point of view.

Step 4   Determine if the problem is at the link level or at a higher level outage in the DPC by typing **show cs7 linkset**. If the ITP shows that the DPC is AVAIL, there is a configuration mismatch between the ITP and BTS.

Step 5   Check whether the DPC has been removed from the BTS database. At the BTS CLI prompt, enter **show call-ctrl-route** or **show sccp-route** and see if the DPC is in any of the routes. If not, the alarm was raised before the associated routes were deleted. If this is the case, manually clear the alarm.

Step 6   If you still cannot determine the cause of the problem, contact the Cisco Technical Assistance Centre(TAC).

DPC User Part Unavailable

This alarm indicates that a Layer 4 user part, such as ISDN user part (ISUP), is unavailable at the DPC in the SS7 network. Contact your SS7 service provider for help in resolving this problem.

DPC Congested

This alarm indicates that the DPC in the SS7 network is congested, that is, is in a state where it has received more traffic than it can handle. This should be a temporary state. If the type of network is National, which is generally the case in the United States, there will also be a level of congestion associated with the alarm.

The ITP should continually communicate with the DPC in the SS7 network to determine if congestion has abated. If this alarm does not clear or keeps reappearing after clearing, contact your SS7 service provider to determine why the DPC is congested.

Signaling Gateway Group Is Out of Service

This alarm indicates that after communication to the SG group was established, it was lost. This indicates that communication to the associated SGs is down, which also indicates that communication to all SGPs is down. See the "Signaling Gateway Failure" section on page 4-7 to determine why the associated SGs are down.

Signaling Gateway Failure

This alarm indicates that communication at the M3UA or SUA layer to an SG has failed. M3UA communications at all SGPs that make up the SG are unavailable. See the "Signaling Gateway Process Is Out of Service" section on page 4-7 to determine why the associated SGPs are down.

Signaling Gateway Process Is Out of Service

This alarm indicates that communication at the M3UA or SUA layer to an SGP has failed. In the majority of cases, there will also be a related SCTP Association Failure alarm. If this is the case, proceed to the "SCTP Association Failure" section on page 4-7. Otherwise, the problem is at the M3UA layer. Call the Cisco TAC for assistance.

SCTP Association Failure

This alarm indicates that the BTS is unable to communicate with an SGP at the SCTP level.

If the application for which SCTP is providing transport is ISUP, please refer to Debugging SCTP Problems for ISUP Applications, page 4-7.

If the application for which SCTP is providing transport is TCAP/SCCP, please refer to Debugging SCTP Problems for TCAP/SCCP Applications, page 4-11.

Debugging SCTP Problems for ISUP Applications

Use the following steps to determine the source of the problem at the M3UA layer:

Step 1 Determine if the administrative state of the SCTP is correct.

a. Type the following command at the BTS CLI prompt:

```
status sctp-assoc id=<sctp-assoc-name>
```

If the response displays ADMIN STATE ->ADMIN_OOS, the SCTP association has been taken administratively out of service and needs to be put back in service.

b. Enter the following command to put the SCTP association in service:

```
control sctp-assoc id=<sctp-assoc-name>; mode=forced; target-state=INS;
```

c. If the administrative state is ADMIN_INS, determine if the association has been taken out of service on the ITP. Log on to the ITP. If you are unable to log on to the ITP, proceed to Step 2.

d. If you are able to log on to the ITP, check the state of the associated ASP by entering the following command:

show cs7 asp

The following is an example of the output:

```
ASP Name      AS Name       State     Type  Rmt Port Remote IP Addr  SCTP
-----------   -----------   --------  ----  -------- --------------  ----------
hrn11asp      hrn11bts      shutdown  M3UA  11146    10.0.5.13
```

e. If the state of the ASP indicates shutdown, someone has administratively taken the association out of service. Refer to the *Cisco ITP User's Guide*, to put the ASP (SCTP association) back in service:

> **Note** When debugging the ITP, note the version of the ITP so the associated *ITP Operations Manual* can be consulted.

f. If the state is down proceed to Step 2.

g. If the state of the ASP is inactive, the ASP is probably on the standby BTS. If the ASP on the active BTS is inactive, proceed to Step 7.

Step 2 Determine if the problem is an IP address or port configuration mismatch between the ITP and the BTS.

a. Determine the BTS configured values for the BTS IP addresses and port. Look for the DNS name and port number that are configured for the SGA process in /opt/OptiCall/CA146/bin/platform.cfg. Go to the specified directory and enter:

cat platform.cgf | grep mdl

The output will look similar to the following:

```
Args=-t 1 -h mgcp-HRN11CA.hrndevtest.cisco.com -p 11146 -mdldir ../mdl -mdltracedir
../mdltrace -mdltestmode 0 -mdlloadmdo 0 -mdltriggertimer 200 -mdlgarbagetimer 5146
-resetcics 1 -fcmtimer 900 -fcmparalleljobs 4
```

- The local IP port number is shown directly after the -p option.

- The local IP addresses that are used by the BTS are derived from the DNS name, which is given directly after the -h option. At the BTS UNIX prompt, enter:

  NSlookup <DNS name>

  The output will look similar to the following:

  ```
  Server:  hrnbtsjs-1.cisco.com
  Address:  10.82.70.199
  Name:    mgcp-HRN11CA.hrndevtest.cisco.com
  Addresses:  10.0.5.136, 10.128.1.147
  ```

  The BTS configured local IP addresses are given in the Addresses line.

b. Determine the ITP configured values of the ITP BTS IP addresses and port.

- Log on to the ITP and get into enable mode.

- Enter the following command:

  show run

- Press **Enter** until the ASP configurations are displayed. A section similar to the following will appear, which shows you the ITP configured values for the BTS IP addresses of the SCTP association:

```
cs7 asp hrn11asp 11146 2905 m3ua
remote-ip 10.0.5.136
remote-ip 10.128.1.147
```

  The number after the ASP name "hrn11asp" is the port number that the ITP has configured for the BTS side of the SCTP association. The two remote-ip addresses are the addresses that the ITP has configured for the BTS side of the SCTP association. Make sure all of these values match the values found in Step 2a.

c. Determine the BTS configured values for the ITP IP addresses and port.

On the BTS EMS CLI console, type the following:

```
CLI> show sctp-assoc id=<SCTP assoc id>
```

An example of the output will show the IP addresses and port as follows:

```
REMOTE_PORT=2905
REMOTE_TSAP_ADDR1=10.0.1.54
REMOTE_TSAP_ADDR2=10.128.1.239
```

d. Determine the ITP configured values of the ITP BTS IP addresses and port.

- Log on to the ITP and get into enable mode.

- Enter **show run**.

- Press **Enter** until the M3UA (or SUA) configuration is displayed. In our example, we are considering the SCTP association connection between the Cisco BTS 10200 Softswitch and the ITP, so we will look at the ITP M3UA configuration. An example of this is as follows:

```
cs7 m3ua 2905
local-ip 10.0.1.54
local-ip 10.128.1.239
```

  – Make sure that the IP addresses and port number are the same values as found in step 2c.

Step 3 Determine if all Ethernet connections on the BTS have been disconnected or if communication has been lost to the IP router. In the platform log, look for the following ERROR message:

```
"All the IP interfaces are faulty!!"
```

If this message is found, the Ethernet connections of the BTS have been pulled or cut. If this message is not found, proceed to Step 4.

Note Platform log is the log file found under /opt/opticall/CA146/bin/logs. It is not a single log file.

Step 4   Determine if the problem is an IP routing issue.

    a. Determine what has been provisioned in the BTS for the destination IP interfaces of the SCTP association by typing the following command:

```
show sctp-association id=<sctp-association-id>
```

Information similar to the following will appear and display the destination IP addresses:

```
REMOTE_TSAP_ADDR1=10.0.1.54
REMOTE_TSAP_ADDR2=10.128.1.239
```

    b. Ping each of the destination IP addresses If one of the addresses does not respond to the ping, there is an IP routing problem that has disabled SCTP communication. Contact the Cisco TAC for assistance. If the ping commands are successful, proceed to Step 5.

Step 5   Determine if the BTS is reachable from the ITP.

    a. Log on to the ITP and get into enable mode.

    b. Find the BTS SCTP association endpoint IP addresses by typing the following command:

```
show run
```

    c. Pres **Enter** until the ASP configuration is displayed. A section similar to the following will appear the BTS IP addresses of the SCTP association:

```
cs7 asp hrn11asp 11146 2905 m3ua
remote-ip 10.0.5.136
remote-ip 10.128.1.147
```

    d. From the ITP prompt, ping each of the IP addresses. If you do not receive a response to the ping command for at least one of the BTS IP endpoint addresses, there is an IP routing problem that is causing the SCTP association to be down. Contact the Cisco TAC for assistance. Otherwise, proceed to Step 6.

Step 6   Bounce the SCTP association (take it administratively out of service and then put it in service).

    a. At the BTS CLI prompt, enter the following commands:

```
control sctp-assoc id=<sctp-assoc-name>; mode=forced; target-state=OOS;
control sctp-assoc id=<sctp-assoc-name>; mode=forced; target-state=INS;
```

    b. Check if the SCTP association has come back in service by entering the following:

```
status sctp-assoc id=<sctp-assoc-name>;
```

The output will either show OPER STATE -> SCTP-ASSOC out of service or OPER STATE -> SCTP-ASSOC in service.

If the OPER STATE still shows that the SCTP association is out-of-service, proceed to Step 7.

Step 7   Bounce the SCTP association from the ITP side by performing the following steps:

    a. Log on to the ITP and get into enable mode.

    b. Get into configure mode by typing configure terminal.

    c. Type the following commands to bounce the SCTP association back in service:

```
va-2651-82(config)# cs7 asp hrn11asp
va-2651-82(config-cs7-asp)# shut
va-2651-82(config-cs7-asp)# no shut
va-2651-82(config-cs7-asp)# end
```

d. Determine if the SCTP association has come back in service by typing the following BTS CLI command:

status sctp-assoc id=<sctp-assoc-name>**;**

The output will display either OPER STATE -> SCTP-ASSOC out of service or OPER STATE -> SCTP-ASSOC in service.

If the OPER STATE still shows that the SCTP association is out-of-service, there is probably an SCTP communication issue that must be debugged at the SCTP protocol level. Contact the Cisco TAC for assistance.

Debugging SCTP Problems for TCAP/SCCP Applications

Refer to Debugging Network Problems for TCAP/SCCP Applications, page 4-12 to determine the source of the problem at the SUA layer.

SCTP Association Degraded

This alarm indicates that one of the two sides of the multi-homed SCTP connection is down. Communication still exists if the other side of the multi-homed connection is up. Refer to the "SCTP Association Failure" section on page 4-7, or contact the Cisco TAC for assistance in resolving this issue.

SCTP Association Configuration Error

This alarm indicates that there is a provisioning error keeping the BTS from properly configuring the SCTP association. Perform the following steps to resolve the problem:

Step 1   If the associated application is ISUP, look at the platform.log for error messages containing the string "MIM CFG."

Step 2   Perform Step 2 of the "Debugging SCTP Problems for ISUP Applications" section on page 4-7 to verify that your IP addresses and ports are properly configured on the BTS.

Step 3   Contact the Cisco TAC for assistance in resolving this issue.

M3UA Cannot Go Active

This alarm is raised at initial startup or during failover by the BTS node that is trying to go into platform Active mode. It occurs when this BTS node is unable to communicate properly with any SGs to tell them that all active call traffic should be routing towards the BTS. See the "Signaling Gateway Process Is Out of Service" section on page 4-7 to determine why the BTS is unable to communicate with any of the ITPs at the M3UA layer. Refer to the "Verify the SCTP Association Status" section on page 4-12 to determine why the BTS is unable to communicate with any of the ITPs at the SUA layer.

M3UA Cannot Go Standby

This alarm is raised at initial startup or during failover by the BTS node that is trying to go into platform Standby mode. See the "Signaling Gateway Process Is Out of Service" section on page 4-7 to determine why the BTS is unable to communicate with any of the SGs at the M3UA layer. See the "Verify the SCTP Association Status" section on page 4-12 to determine why the BTS is unable to communicate with any of the ITPs at the SUA layer.

TCAP Binding Failure

This alarm is raised when the TCAP layer does not have enough service access point (SAP) to bind for the subsystem. Currently only 16 subsystems are allowed on the same platform. Check the Subsystem table to see if you have more than 16 subsystems on the same platform, FS for POTS/Tandem/Centrex (FSPTC) or AIN Feature Server (FSAIN).

Remote Subsystem Is Out Of Service

This alarm indicates the remote subsystem is out of service. Contact your service control point (SCP) service provider for assistance.

Debugging Network Problems for TCAP/SCCP Applications

Network failure issues can be caused by several problems. This section describes the procedures to locate the cause of the problem. These procedures describe an iterative process that must be performed in order. When a problem is found and resolved, perform the procedure again from the beginning.

This section describes how to perform the following procedures:

1. Verify the SCTP Association Status, page 4-12
2. Verify the Configuration, page 4-13
3. Verify the IP Routing, page 4-15
4. Verify if the ASP is Used by Any AS, page 4-15
5. Verify the ITP T1 Card Provisioning, page 4-16
6. Verify the ITP MTP2 Serial Interface, page 4-16
7. Verify the ITP-STP Linkset Status, page 4-17
8. Verify the Cisco ITP Route, page 4-17

Verify the SCTP Association Status

Step 1   Determine if the administrative state and the operational state of the SCTP association on the BTS Element Management System (EMS) are in service. If the SCTP association is not in service, bring it in service and repeat this step. The following is an example of a healthy SCTP association:

```
CLI> status sctp-assoc id=<id>

SCTP ASSOC ID -> sctp_assoc3
ADMIN STATE -> ADMIN_INS
```

```
OPER STATE -> SCTP-ASSOC in service
REASON -> ADM executed successfully
RESULT -> ADM configure result in success

Reply : Success:
```

Step 2   Determine if the ASP is in service on the Cisco ITP by entering **show cs7 asp name** <asp-name>. The ASP name corresponds to the SCTP association name provisioned on the BTS. Information similar to the following is displayed:

```
c2651-48# show cs7 asp name <asp name>
   Effect Primary
   ASP Name      AS Name       State         Type  Rmt Port Remote IP Addr  SCTP
   ------------  ------------  -------------  ----  -------- --------------  ----
   TB2-PRI-AIN   TB02-LNP-NC   active         SUA   12520    10.89.225.209   323
   TB2-PRI-AIN   TB02-SUALNP   shutdown       SUA   12520    10.89.225.209   323
   TB2-PRI-AIN   TB02-800A-NC  active         SUA   12520    10.89.225.209   323
   TB2-PRI-AIN   TB02-800T-NC  active         SUA   12520    10.89.225.209   323
   TB2-PRI-AIN   TB02-SUA800A  active         SUA   12520    10.89.225.209   323
   TB2-PRI-AIN   TB02-SUA800T  active         SUA   12520    10.89.225.209   323
```

a.   If the status is **shutdown**, enter the following commands on the ITP and check the status again:

```
config terminal
cs7 asp <asp name>
no shut
```

b.   If the status of the ASP is **inactive**, the ASP is probably on the standby BTS.

c.   If the ASP on the active BTS is inactive, enter the following commands on the ITP and check the status again:

```
config terminal
cs7 asp <asp-name>
no shut
```

d.   If the ASP is now active, proceed to the "Verify if the ASP is Used by Any AS" section on page 4-15. Otherwise, continue to the next section.

Verify the Configuration

Step 1   Determine if the problem is an IP address or port configuration mismatch between the ITP and the BTS. Enter the command **show sctp-assoc id=**<sctp-assoc-name> on the BTS EMS

Step 2   Enter the command **show cs7 sua** on the ITP.

Step 3   Verify that the remote TSAP address and the remote port of the SCTP association on the BTS is the same as the local IP address and the local port used by the ITP SUA. If the SCTP association is multi-homed, all of the IP addresses should be verified. The following example displays properly matched configurations:

```
CLI> show sctp-assoc id=sctp_assoc3

ID=sctp_assoc3
SGP_ID=itp_2651_1
SCTP_ASSOC_PROFILE_ID=sctp_prof
REMOTE_PORT=14001
REMOTE_TSAP_ADDR1=10.89.232.48
PLATFORM_ID=FSAIN520
IP_TOS_PRECEDENCE=FLASH
```

```
LOCAL_RCVWIN=64000
MAX_INIT_RETRANS=5
MAX_INIT_RTO=1000
STATUS=INS
ULP=XUA


Reply : Success: Entry 1 of 1 returned.


c2651-48# show cs7 sua
Sigtran SUA draft version: 14


SUA  Local port: 14001      State: active      SCTP instance handle: 2
Local ip address:                              10.89.232.48
Number of active SUA  peers:                   8
Max number of inbound streams allowed:         17
Local receive window:                          64000
Max init retransmissions:                      8
Max init timeout:                              1000 ms
Unordered priority:                            equal
SCTP defaults for new associations
 Transmit queue depth:   1000       Cumulative sack timeout:   200 ms
 Assoc retransmissions:  10         Path retransmissions:      4
 Minimum RTO:            1000  ms   Maximum RTO:               1000  ms
 Bundle status:          on         Bundle timeout:            400 ms
 Keep alive status:      true       Keep alive timeout:        10000 ms
```

Step 4   If there is no mismatch, proceed to Step 5. Otherwise, perform the following procedure:

   a. Correct the mismatch.

   b. Bounce the SCTP association on the BTS.

   c. Repeat the "Verify the SCTP Association Status" section on page 4-12.

Step 5   Verify that the SCTP port on the BTS and the remote port of the ASP on the ITP are the same.

   a. On the BTS, open the platform.cfg file and locate the section for TSA on FSAIN/FSPTC, as illustrated in the following example:

```
[ProcessParameters]
ProcName=TSA
#----------------- Process priority (valid values = -60 to 60)
--------------------------------#
Priority=24
#----------------- Max thread priority (valid values = -60 to 60)
---------------------------#
MaxDynamicThreadPriority=18
#------Resource limits = (max descriptors) / (max heap size bytes) / (max stack size
bytes)------#
ResourceLimits=0 / 524288000 / 0
ExecName=tsa.FSAIN520
ExecPath=./
Args=-numthread 1 -tsadns crit-aSYS02AIN.ipclab.cisco.com -sctpport 12520 -stackcfg
tri_stack.cfg -multithread 0 -sgw_option SUA
ProcessGroup=0
ReportsDisableLevel=0
DebugReportsDisableLevel=0
NewConsole=0
Enable=1
ThreadHealthMonitoring=yes
SwitchOverIfMaxRestartExceededInDuplex=yes
EndPlatformIfMaxRestartExceededWhenMateFaulty=yes
#----------- Restart rate = n /m (where n = Max restarts , m - interval in hours)
---------------#
RestartRate=0 /  1
```

b. On the ITP, enter the command **show run | begin** <asp-name>. Information similar to the following is displayed:

```
c2651-48# show run | begin TB2-PRI-AIN

cs7 asp TB2-PRI-AIN 12520 14001 sua
 remote-ip 10.89.225.209
 remote-ip 10.89.226.209
!
```

c. If the SCTP ort on the BTS and the remote port of the ASP on the ITP are the same, proceed to Step 6.

d. If the SCTP port on the BTS and the remote port of the ASP on the ITP are not the same, perform the following procedure:

- Correct the problem on the ITP.
- Bounce the SCTP association on the BTS.
- Repeat the "Verify the SCTP Association Status" section on page 4-12.

Step 6 Verify that the tsadns resolves to exactly the same remote-ip as the ASP on the ITP. If not, perform the following procedures as necessary:

a. Correct it in the /etc/hosts file and on the DNS server, if necessary.

b. Correct it on the ITP if the IP addresses on the ITP are incorrect.

c. Bounce the SCTP association on the BTS.

d. Repeat the "Verify the SCTP Association Status" section on page 4-12.

Verify the IP Routing

Step 1 Ping the ITP addresses discovered in the "Verify the Configuration" section on page 4-13 from the BTS in order to see if traffic is routed as planned.

Step 2 Ping the BTS addresses discovered in the "Verify the Configuration" section on page 4-13 from the ITP to see if traffic is routed as planned.

Step 3 If routing is not as expected, correct the routing setup.

Step 4 Repeat the "Verify the SCTP Association Status" section on page 4-12.

Verify if the ASP is Used by Any AS

If the ASP is not used by any AS in the ITP, the SCTP association will be taken down by the ITP. Make sure the AS using the ASP is provisioned before bringing up the SCTP association corresponding to the same ASP. If the ASP is used by any AS, continue to the next section. Otherwise, correct it and continue.

Verify the ITP T1 Card Provisioning

Enter the command **show controller t1** <slot/[bay/]port> on the ITP. Verify if T1 is up. If not, check if the framing, line code, and the clock source are provisioned as planned. The following example displays a healthy card status:

```
c2651-48# show controllers t1 0/0

T1 0/0 is up.
  Applique type is Channelized T1
  Cablelength is short 133
  No alarms detected.
  alarm-trigger is not set
  Version info Firmware: 20010805, FPGA: 15
  Framing is ESF, Line Code is B8ZS, Clock Source is Line.
  Data in current interval (477 seconds elapsed):
     0 Line Code Violations, 0 Path Code Violations
     0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
     0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
......
```

Verify the ITP MTP2 Serial Interface

To resolve problems with the ITP MTP2 serial interface, perform the following steps:

Step 1   To display the state of the ITP MTP2 serial interface, enter the command **show int serial** <number> on the ITP. Information similar to the following will be displayed:

```
c2651-48# show int serial 0/0:0

Serial0/0:0 is up, line protocol is up
  Hardware is PowerQUICC Serial
  Description: link_to_mgts_lic_10
  MTU 1500 bytes, BW 56 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation SS7 MTP2, loopback not set
  Keepalive not set
  Last input 33w5d, output 00:00:31, output hang never
  Last clearing of "show interface" counters 33w5d
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 23 drops
  30 second input rate 0 bits/sec, 0 packets/sec
  30 second output rate 0 bits/sec, 0 packets/sec
     1912000 packets input, 9866017 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 17 giants, 0 throttles
     3356 input errors, 128 CRC, 2641 frame, 0 overrun, 0 ignored, 587 abort
     1163961 packets output, 13234709 bytes, 0 underruns
     0 output errors, 0 collisions, 55 interface resets
     0 output buffer failures, 0 output buffers swapped out
     31 carrier transitions
  Timeslot(s) Used:1, SCC: 0, Transmitter delay is 0 flags
```

Step 2   If the interface is up and the line protocol is up, continue to the next section. If there is a problem, determine where the problem exists, as follows:

    a.   If the interface is down, shut down the interface manually.

    b.   If the line protocol is down, the problem exists in cabling or in the MTP2 layer.

    c.   If both the interface and the line protocol are down, there is a hardware failure or the interface is manually shutdown.

Step 3   After correcting the problem, continue to the next section.

Verify the ITP-STP Linkset Status

To resolve problems with the ITP-STP linkset status, perform the following steps:

Step 1   Verify whether the link-set is available on the ITP by entering the following command:

show cs7 linkset <ls-name>

Information similar to the following is displayed:

```
c2651-48# show cs7 linkset

lsn=ls_to_mgts_lic_10   apc=1.101.0        state=avail      avail/links=1/1
  SLC  Interface                      Service   PeerState        Inhib
  00   Serial0/0:0                    avail     ---------        -----
```

Step 2   If the status is not available and at least one of the serial interfaces is available, the problem could be the point code type or point code value mismatch with the remote peer.

Step 3   If the checking is successful, continue to the next section. Otherwise, correct the problem and continue.

Verify the Cisco ITP Route

To resolve problems with the Cisco ITP route, perform the following steps:

Step 1   Verify if there is a route to the destination point code provisioned in the BTS by entering the following command:

show cs7 route

Information similar to the following is displayed:

```
c2651-48# show cs7 route

Dynamic Routes 0 of 500

Routing table = system Destinations = 6 Routes = 6
Destination          Prio Linkset Name        Route
-------------------- ---- ------------------- -------
1.8.1/24      INACC   1  ls_to_mgts_lic_10   UNAVAIL
1.12.1/24     acces   5  ls_to_mgts_lic_10   avail
1.101.0/24    acces   1  ls_to_mgts_lic_10   avail
7.44.120/24   acces   1  ls_to_inet12_pod_1  avail
7.44.121/24   acces   1  ls_to_inet12_pod_1  avail
7.212.112/24  acces   1  ls_to_inet12_pod_1  avail


Routing table = XUA

Destination         Type
------------------- --------
7.2.1/24      acces  AS
7.2.3/24      acces  AS
7.44.1/24     acces  AS
7.44.3/24     acces  AS
```

Step 2   If the linkset is available and the route is UNAVAIL, the problem could be in the service provider's SS7 network. Contact the service provider to coordinate troubleshooting.

After successfully passing this step, the network failure should not happen. If it still happens, the supporting team or the developer should be contacted.

Troubleshooting With the Query Command

The Query Verification Tool (QVT) enables a user to generate TCAP queries to external databases through the CLI interface. For information about the QVT, see the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/voice/bts10200/bts4_4/featmods/qvttvt.htm#wp1168 709

Table Configuration Problems

The CLI query command with the table-info option displays the tables used for routing the external SS7 queries on the BTS. The query command can identify the following problems:

- Missing CA-CONFIG table
- Missing SLHR-PROFILE table
- Missing SLHR table
- Missing DPC table
- Missing OPC table
- Missing SUBSYSTEM-PROFILE table
- Missing SUBSYSTEM table
- Missing SCCP-NW table
- Missing SCCP-ROUTE table
- Missing ROUTING-KEY table
- Missing SG-GRP table
- Missing SG table
- Missing SGP table
- Missing SCTP-ASSOC table

To resolve a table error, add the appropriate entry to the table specified in the command response.

Network Related Problems

The CLI query command can provide information about network related problems. This section describes problems identified by the query command and the solutions to them.

No Translation for an Address of Such Nature

Layer: SCCP

Version: ITU88, ITU92, ITU96, ANSI88, ANSI92

Location: STP

Cause: The GTT entry is not provisioned correctly in the STP.

Solution: Correct the GTT entry in the STP.

No Translation for this Specific Address

Layer: SCCP

Version: ITU88, ITU92, ITU96, ANSI88, ANSI92

Location: STP

Cause: The GTT entry is not provisioned correctly in the STP.

Solution: Correct the GTT entry in the STP.

Subsystem Congestion

Layer: SCCP Subsystem (TCAP)

Version: ITU88, ITU92, ITU96, ANSI88, ANSI92

Location: SCP

Cause: The SCP subsystem is congested.

Solution: Ask the SCP service provider to solve the congestion problem.

Subsystem Failure

Layer: SCCP Subsystem (TCAP)

Version: ITU88, ITU92, ITU96, ANSI88, ANSI92

Location: SCP

Cause: The SCP is down or the subsystem of the SCP is down.

Solution: Verify that the SCP point code is correct.

Unequipped User

Layer: SCCP Subsystem (TCAP)

Version: ITU88, ITU92, ITU96, ANSI88, ANSI92

Location: SCP

Cause: The SCCP user is not equipped.

Solution: Verify that the SCP point code is correct.

Network Failure

Layer: MTP3/MTP2/MTP1 or SCTP

Version: ITU88, ITU92, ITU96, ANSI88, ANSI92 for NTP3/2/1, IETF RFC 2960 for SCTP

Location: Local, STP, or SCP

Cause: The BTS-ITP sctp-association is down or the SS7 link, linkset, or route is down.

Solution: See the "Debugging Network Problems for TCAP/SCCP Applications" section on page 4-12 section for assistance in solving this problem.

Network Congestion

Layer: SCCP

Version: ITU88, ITU92, ITU96, ANSI88, ANSI92

Location: Local, STP, or SCP

Cause: The SCTP layer or the SS7 network is congested.

Solution: The service provider of the SS7 network needs to either provide higher capacity or re-engineer the traffic. SCTP layer congestion normally indicates insufficient CPU power. Hardware needs to be upgraded or more BTSs need to be added to offload traffic.

Unqualified

Layer: SCCP

Version: ITU88, ITU92, ITU96, ANSI88, ANSI92

Location: STP or SCP

Cause: Unknown.

Solution: Contact the support team or developer for assistance.

Error In Message Transport

Layer: SCCP

Version: ITU92

Location: STP

Cause: There was a failure in message transportation.

Solution: Contact the support team or the developer.

Destination Cannot Perform Reassembly

Layer: SCCP

Version: ITU88, ITU92, ITU96, ANSI88, ANSI92

Location: SCP

Cause: The peer side is not capable of reassembling extended unit data service (XUDTS) packets.

Solution: The ITP does not support segmentation and reassembly. Contact the Cisco TAC for assistance.

SCCP Failure

Layer: SCCP

Version: ITU88, ITU92, ITU96, ANSI88, ANSI92

Location: Local, STP, or SCP

Cause: The Signal Connection Control Part (SCCP) layer failed or the local TCAP Signaling Adapter (TSA) could not find the appropriate entry in the Subsystem table or the SCCP-nw table.

Solution: Add or properly populate the Subsystem and SCCP-nw tables. If it still does not work, restart the platform providing the service (FSAIN or FSPTC).

Hop Counter Violation

Layer: SCCP

Version: ITU96, ANSI92

Location: STP

Cause: The maximum hop count is exceeded during the message routing.

Solution: Make sure the hop count value provisioned in the SCCP-NW table is not too small. Verify that the SS7 network provider does not have any route-loops.

Segmentation Not Supported

Layer: SCCP

Version: ITU96

Location: SCP

Cause: The peer side is not capable of reassembling XUDTS packets.

Solution: The ITP does not support segmentation and reassembly. Contact the Cisco TAC for assistance.

Segmentation Failure

Layer: SCCP

Version: ITU96

Location: STP

Cause: The segmentation failed.

Solution: The ITP does not support segmentation and reassembly. Contact the Cisco TAC for assistance.

QVT Timeout

Layer: Local

Cause: The SCP filed to respond or the TSA is out of service.

Solution: If the SCP failed, contact the service provider to solve the problem. If the TSA is out of service, perform a manual failover.

CLI Timeout

Layer: Local

Cause: The EMS and CA.FSAIN/FSPTC connections are down or the SCA on the CA/FSAIN/FSPTC is out of service.

Solution: If the SCA is down, restart the SCA or restart the platform where the SCA resides. If the EMS and CA/FSAIN/FSPTC connections are down, verify whether the IP routing is correct and the OptiCall Messaging System (OMS) hub is in service.