



# CHAPTER 13

## Network Troubleshooting

---

Revised: August 10, 2011, OL-25016-01

### Introduction

The chapter provides the information needed for conducting network troubleshooting on the Cisco BTS 10200 Softswitch. For Signaling System 7 (SS7) network troubleshooting information, refer to [Chapter 10, “Signaling Troubleshooting.”](#) For additional troubleshooting information for specific protocols refer to the following protocol guides.

- [Cisco BTS 10200 Softswitch H.323 Guide, Release 6.0.3](#)
- [Cisco BTS 10200 Softswitch ISDN Guide, Release 6.0.3](#)
- [Cisco BTS 10200 Softswitch PacketCable Guide, Release 6.0.3](#)
- [Cisco BTS 10200 Softswitch SIP Guide, Release 6.0.3](#)
- [Cisco BTS 10200 Softswitch SS7 SIGTRAN Guide, Release 6.0.3](#)



#### Caution

---

The use of the UNIX **ifconfig down** command on any signaling interface to test or troubleshoot network or interface failures of the Cisco BTS 10200 Signaling Interface might lead to undesirable consequences or conditions.

---

# Troubleshooting a Network Failure

Network failure issues can be caused by several problems. This section procedures you can use to isolate the cause of the problem. These procedures make up an iterative process, and they must be performed in the order indicated.

This section describes how to perform the following procedures:

- [Check the Stream Control Transmission Protocol Association Status, page 13-3](#)
- [Check the Configuration, page 13-4](#)
- [Check the Internet Protocol Routing, page 13-6](#)
- [Find Out If the Application Service Provider Is Used by Any Application Server, page 13-6](#)
- [Check the Internet Protocol Transfer Point T1 Card Provisioning, page 13-6](#)
- [Check the Internet Protocol Transfer Point Message Transfer Part 2 Serial Interface, page 13-7](#)
- [Check the Internet Protocol Transfer Point-Signal Transfer Point Linkset Status, page 13-8](#)
- [Check the Internet Protocol Transfer Point Route, page 13-9](#)
- [Oracle Database Tool Restart, page 13-10](#)

## Check the Stream Control Transmission Protocol Association Status

- Step 1** Determine if the administrative state and the operational state of the Stream Control Transmission Protocol (SCTP) association on the Cisco BTS 10200 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=sctp_assoc3

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 application service provider (ASP) is in service on the Cisco IP transfer point (ITP) by entering **show cs7 asp name <asp-name>**. The ASP name corresponds to the SCTP association name provisioned on the Cisco BTS 10200. Information similar to the following is displayed:

```
c2651-48#show cs7 asp name TB2-PRI-AIN
```

ASP Name	AS Name	State	Type	Rmt Port	Effect Remote IP	Primary Addr	SCTP
TB2-PRI-AIN	TB02-LNP-NC	active	SUA	12520	10.89.225.209	323	323
TB2-PRI-AIN	TB02-SUALNP	shutdown	SUA	12520	10.89.225.209	323	323
TB2-PRI-AIN	TB02-800A-NC	active	SUA	12520	10.89.225.209	323	323
TB2-PRI-AIN	TB02-800T-NC	active	SUA	12520	10.89.225.209	323	323
TB2-PRI-AIN	TB02-SUA800A	active	SUA	12520	10.89.225.209	323	323
TB2-PRI-AIN	TB02-SUA800T	active	SUA	12520	10.89.225.209	323	323

- 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
```
- If the status of the ASP is inactive, the ASP is probably on the standby Cisco BTS 10200.
- If the ASP on the active Cisco BTS 10200 is inactive, enter the following commands on the ITP and check the status again:
 

```
config terminal
cs7 asp <asp-name>
no shut
```
- If the ASP is now active, proceed to the [“Find Out If the Application Service Provider Is Used by Any Application Server”](#) section on page 13-6. Otherwise, continue to the next section.

## Check the Configuration

- Step 1** Determine if the problem is an Internet Protocol (IP) address or port configuration mismatch between the ITP and the Cisco BTS 10200. Enter **show sctp-assoc id-<sctp-assoc-name>** on the Cisco BTS 10200 EMS.
- Step 2** Enter **show cs7 sua** on the ITP.
- Step 3** Verify that the remote transport service access point (TSAP) address and the remote port of the SCTP association on the Cisco BTS 10200 are the same as the local IP address and the local port used by the ITP SCCP user adapter (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
DSCP=NONE
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:
- Correct the mismatch.
  - Bounce the SCTP association on the Cisco BTS 10200.
  - Repeat the [“Check the Stream Control Transmission Protocol Association Status”](#) section on page 13-3.

- Step 5** Verify that the SCTP port on the Cisco BTS 10200 and the remote port of the ASP on the ITP are the same.
- a. On the Cisco BTS 10200, open the platform.cfg file and locate the TCAP signaling adapter (TSA) section on the FSAIN/FSPTC (Feature Server for AIN services/Feature Server for POTS, Tandem, and Centrex) server, 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 `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 port on the Cisco BTS 10200 and the remote port of the ASP on the ITP are the same, proceed to Step 6.
  - d. If the SCTP port on the Cisco BTS 10200 and the remote port of the ASP on the ITP are not the same, perform the following procedure:
    - Correct the port setting on the ITP.
    - Bounce the SCTP association on the Cisco BTS 10200.
    - Repeat the [“Check the Stream Control Transmission Protocol Association Status”](#) section on page 13-3.
- Step 6** Verify that the tsadns resolves to exactly the same remote-IP as the ASP on the ITP. If it does not, perform the following procedures as necessary:
- a. Correct the tsadns in the /etc/hosts file and on the domain name system (DNS) server, if necessary.
  - b. Correct the tsadns on the ITP if the IP addresses on the ITP are incorrect.
  - c. Bounce the SCTP association on the Cisco BTS 10200.

- d. Repeat the “Check the Stream Control Transmission Protocol Association Status” section on page 13-3.

## Check the Internet Protocol Routing

- 
- Step 1** Ping the ITP addresses discovered in the “Check the Configuration” section on page 13-4 from the Cisco BTS 10200 in order to see if traffic is routed as planned.
  - Step 2** From the ITP, ping the Cisco BTS 10200 addresses discovered in the “Check the Configuration” section on page 13-4 to see if traffic is routed as planned.
  - Step 3** If routing is not as expected, correct the routing setup.
  - Step 4** Repeat the “Check the Stream Control Transmission Protocol Association Status” section on page 13-3.
- 

## Find Out If the Application Service Provider Is Used by Any Application Server

If the ASP is not used by any application server (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 the ASP and continue.

## Check the Internet Protocol Transfer Point T1 Card Provisioning

Enter `show controller t1 <slot/[bay/]port>` on the ITP. Verify that trunk level 1 (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
```

```
.....
```

## Check the Internet Protocol Transfer Point Message Transfer Part 2 Serial Interface

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

- Step 1** To display the state of the ITP MTP2 serial interface, enter **show int serial <number>** on the ITP. Information similar to the following is 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. Use this procedure:
- If the interface is down, shut down the interface manually.
  - If the line protocol is down, the problem exists in cabling or in the MTP2 layer.
  - If both the interface and the line protocol are down, there is a hardware failure or the interface is manually shut down.
- Step 3** After correcting the problem, continue to the next section.

## Check the Internet Protocol Transfer Point-Signal Transfer Point Linkset Status

To check for problems with the ITP-signal transfer point (STP) linkset status, perform the following steps:

---

**Step 1** Find out if 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.

---



## Check the Internet Protocol Transfer Point Route

To check for problems with the ITP route, perform the following steps:

- Step 1** Find out if there is a route to the destination point code provisioned in the Cisco BTS 10200 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 unavailable, the problem could be in the service provider's SS7 network. Contact the service provider to coordinate troubleshooting.

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

## Oracle Database Tool Restart

After a network failure, if dbadm tool indicates that database jobs 3, 4, 5, and 6 are broken, the database administrator needs to restart the jobs using the following procedure.

- 
- Step 1** Login to oracle.  
`su - oracle`
- Step 2** Restart database job 3.  
`$ java dba.rep.RepAdmin -enable job 3`
- Step 3** Restart database job 4.  
`$ java dba.rep.RepAdmin -enable job 4`
- Step 4** Restart database job 5.  
`$ java dba.rep.RepAdmin -enable job 5`
- Step 5** Restart database job 6.  
`$ java dba.rep.RepAdmin -enable job 6`
-