CHAPTER 14

# General Troubleshooting

**Revised: July 22, 2009, OL-8000-32**

## Introduction

The chapter provides the general troubleshooting information needed to conduct troubleshooting on the Cisco BTS 10200 Softswitch. This chapter is divided into the following sections:

- Troubleshooting CORBA Problems – Provides a reference to the Common Object Request Broker Architecture (CORBA) troubleshooting information in the *Cisco BTS 10200 Softswitch CORBA Adapter Interface Specification Programmer Guide*.
- Troubleshooting Local Number Portability Problems – Provides the information to solve local number portability (LNP) problems.
- Troubleshooting Alerting Notification Problems – Explains how to troubleshoot the system when the 3PTYFS does not appear to be receiving the alerting notification and call data.
- Command Responses – Describes success and failure responses to commands, as well as values for the term-reason and trunk-reason responses.
- Protocol Troubleshooting – Provides the troubleshooting information for resolving Cisco BTS 10200 Softswitch protocol problems.
- File Configuration – bts.properties - Provides instructions for editing and configuring the bts.properties file.
- Privacy Screening Troubleshooting - Provides instructions for troubleshooting privacy screening.

**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 Softswitch Signaling Interface may lead to undesirable consequences or conditions.

## Troubleshooting CORBA Problems

To troubleshoot CORBA interface problems, refer to the *Cisco BTS 10200 Softswitch CORBA Adapter Interface Specification Programmer Guide, Chapter 5*.

# Troubleshooting Local Number Portability Problems

Problems can arise when porting a subscriber's telephone number from one service provider to another. The Network Interconnection Interoperability Forum (NIIF), a part of the Alliance for Telecommunications Industry Solutions (ATIS) organization, has published a document (ATIS/NIIF-0017) that includes detailed steps that service providers should follow when LNP problems are encountered. The document is titled *Guidelines for Reporting Local Number Portability Troubles in a Multiple Service Provider Environment*, and it is available at http://www.atis.org/atis/clc/NIIF/niifdocs.htm.

The NIIF also maintains the National LNP Contact Directory, a protected document that provides telephone numbers of 24 by 7 LNP-qualified contacts for each service provider. The directory is located at the URL given above. You can download and submit an application for a password at the same URL.

## Resolving Local Number Portability Conflicts

Some conflicts can arise in the LNP processes. Figure 14-1 illustrates the causes of conflicts and the procedures that the Number Portability Administration Center (NPAC) service management system (SMS) uses to resolve them.

If either the old or new service provider did not send a notification to the NPAC SMS, the NPAC SMS notifies the service provider from which it did not receive a notification that it is expecting a notification. If the NPAC SMS receives the missing notification, and both notifications indicate agreement among the service providers, the process proceeds as normal.

The following list describes the actions that the NPAC SMS takes in different situations:

- If the NPAC SMS does *not* receive a concurring notification from the *old* service provider, the NPAC SMS logs the failure to respond and allows the new service provider to proceed with activation when the new service provider due date is reached.
- If the NPAC SMS does *not* receive a concurring notification from the *new* service provider, the NPAC SMS logs the failure to respond, cancels the request, and notifies both service providers of the cancellation.
- If the service providers disagree as to who will provide service for the telephone number, the NPAC SMS places the request in the "conflict" state and notifies both service providers of the conflict status and the Status Change Cause Code.
  - The service providers then determine between them who will serve the customer using their internal business processes.
  - When a resolution is reached, the NPAC SMS is notified by the new service provider and removes the request from the conflict state.

  Within the first 6 hours, only the old service provider can initiate "conflict off." After 6 hours, either service provider can remove the conflict status. The new service provider can alternatively request cancellation of the Subscription Version.

*Figure 14-1 Conflict Resolution Work Flow*

# Audit Requests

An audit function is necessary for troubleshooting customer problems and as a maintenance process to ensure Subscription Version data integrity across the entire LNP network. Audits are concerned with the process of comparing the NPAC SMS view of the LNP network's Subscription Version data with one or more of the service provider's views of its network.

The following methods help ensure data integrity across the LNP network:

- On-demand audits can be initiated by any service provider who believes a problem may exist in another service provider’s network. These audits are executed through queries to the appropriate service provider’s network, and corrected by means of downloads to those same networks.
- Local service providers are also responsible for comparing database extracts of Subscription data written to an File Transfer Protocol (FTP) site by the NPAC SMS with their own versions of the same Subscription data.
- The NPAC SMS selects a random sample of active Subscription Versions from its own database, then compares those samples to the representation of that same data in the various local SMS databases.

# Report Requests

The NPAC SMS supports report generation for predefined and ad hoc reports. The report generation function creates output report files according to specified format definitions, and distributes reports to output devices as requested. The report distribution service supports distribution to electronic files, to local or remote printers, to e-mail addresses, and to fax machines.

# Troubleshooting Alerting Notification Problems

This section explains how to troubleshoot the system when the 3PTYFS does not appear to be receiving the alerting notification and call data.

**Step 1** Verify that the ID, transport service access point (TSAP) ADDR, and TYPE are properly provisioned in the FEATURE-SERVER table.

**Step 2** Verify that the alerting notification feature (ALERT_NOTIFY) is provisioned properly.

**Step 3** Verify one of the following cases, as applicable:

- Verify that Alerting Notification is included in the SERVICE table applicable to the specific subscriber.
- Verify that Alerting Notification is included in the SERVICE table applicable to the specific POP (the service ID identified by the office-service-id token in the POP table).
- Verify that Alerting Notification is included in the default office service ID (if the feature is intended to be offered by default to all subscribers on the switch).

**Note** In the procedures included in this document, the alerting notification feature is provisioned using the feature identifier **FNAME=ALERT_NOTIFY**. The feature identifier can be any unique string of up to 16 ASCII characters chosen by the service provider. If you are not sure of the name used in your system for this feature, use the **SHOW FEATURE** command and view the system response to find the name.

**Example:**

```
SHOW FEATURE-SERVER;
SHOW FEATURE FNAME=ALERT_NOTIFY;
SHOW CA-CONFIG TYPE=DEFAULT-OFFICE-SERVICE-ID;
SHOW SERVICE ID=<the value of the default-office-service-id>
SHOW SERVICE ID=6543;
SHOW SUBSCRIBER-SERVICE-PROFILE SERVICE-ID=6543;
```

**Step 4** If a TSAP address is used for the 3PTYFS, verify that the domain name is correctly provisioned in the DNS and resolves to the intended 3PTYFS.

**Step 5** Enter the CLI command to check for Signaling alarm #12—Feature Server is not up or is not responding to Call Agent. If this alarm is raised, there is a communications problem between the Cisco BTS 10200 Softswitch and the 3PTYFS.

**Example:**

```
show alarm type=signaling;
show alarm type=signaling; number=12;
```

The following details apply to SIGNALING alarm #12:

- For a 3PTYFS that is more than one hop away from the Cisco BTS 10200 Softswitch, SIGNALING alarm #12 is raised when communications between the Cisco BTS 10200 Softswitch and the first-hop node go down. However, the alarm is *not* raised if communications on the second (or more distant) hop go down, or if the DNS value for the 3PTYFS does not resolve correctly.
- The system can take up to two minutes to detect a communications failure in the first hop toward the 3PTYFS.

**Step 6** Verify that you have connectivity from the Cisco BTS 10200 Softswitch to the 3PTYFS.

**Step 7** Verify that the 3PTYFS is provisioned to support this feature in accordance with the applicable product documentation. The Cisco BTS 10200 Softswitch does not send any provisioning or status/control commands to the 3PTYFS.

**Step 8** Verify that the 3PTYFS and peripheral devices are operating properly according to the applicable product documentation.

# Command Responses

This section describes success and failure responses to commands, as well as values for the term-reason and trunk-reason responses.

**Note** In this section, an asterisk preceding a token name means the token is mandatory. A token without an asterisk is optional.

# Success and Failure Responses

The following message is returned upon the success of a command:

```
Configuration Command Executed.
```

One of the following responses can be returned upon the failure of a command:

- Administrative (ADM) found no failure.
- ADM MGW(s) cannot be found.
- ADM subscriber(s) cannot be found.
- ADM trunk group(s) cannot be found.
- ADM trunk(s) cannot be found.
- ADM no termination(s) found in MGW.
- ADM no trunk group(s) found in trunking gateway.
- ADM no trunk(s) found in trunk group.
- ADM fail while in termination table.
- ADM fail while in trunk group table.
- ADM fail while in trunk table.
- ADM fail while looking to find trunk index.
- ADM fail while getting MGW administration state.
- ADM fail while getting trunk group administration state.
- ADM fail while looking for MGW index.
- ADM administration state invalid.
- ADM failed to allocate inter-process communication (IPC) message(s).
- ADM failed to dispatch IPC message(s).
- ADM operational state invalid.
- ADM MGW(s) state change and pending.
- ADM subscriber(s) state change and pending.
- ADM trunk group(s) state change and pending.
- ADM trunk(s) state change and pending.
- ADM found subscriber category invalid.
- ADM found trunk group type invalid.
- ADM found trunk group state invalid.
- ADM found MGW admin state not ready.
- ADM found trunk group admin state not ready.
- ADM entity in desired state.
- ADM not allow trunk to reset.
- ADM not allow subscriber to reset.
- ADM change to out-of-service state required.
- ADM change to request graceful mode error.

- ADM found entity unequipped in initial state.
- ADM operation not allowed because D Channel(s) is down.
- The H.323 Gateway was not found in database management (DBM).
- ADM found unknown failure reason(s).

# Termination Reason Responses

The following responses can be returned for the termination reason (term-reason) response for subscriber termination and trunk termination commands:

- All of wildcard too complicated
- Channel-associated signaling (CAS) signaling protocol error
- Codec negotiation failure
- Endpoint does not have a digit map
- Endpoint malfunctioning
- Endpoint redirected to another Call Agent
- Endpoint taken out of service
- Error in RemoteConnectionDescriptor
- Event/signal parameter error
- Facility failure
- Failure of a grouping of trunks
- Incompatible protocol version
- Insufficient bandwidth at this time
- Insufficient bandwidth
- Internal consistency in local connection options
- Internal hardware failure.
- Invalid call ID
- Invalid conn identifier
- Invalid or unsupported command parameter
- Invalid or unsupported LocalConnectionOptions
- Loss of lower connectivity
- Loss of lower layer connectivity
- Manual intervention
- Missing remote connection descriptor
- Missing remote connection descriptor
- No fault reason available
- No such event or signal
- Packetization period not supported
- Per endpoint connection limit exceeded

- Quality of service (QoS) resource reservation was lost
- Response too big
- The media gateway is down
- The media gateway is in a faulty state
- The media gateway is transitioning to another state
- The media gateway is unreachable
- The phone is already off hook
- The phone is already on hook
- The transaction could not be executed because a protocol error was detected
- The transaction could not be executed because of internal overload
- The transaction could not be executed because the command contained an unrecognized extension
- The transaction could not be executed because the endpoint is not ready
- The transaction could not be executed because the endpoint is restarting
- The transaction could not be executed because the endpoint is unknown
- The transaction could not be executed because the gateway cannot send the specified announcement.
- The transaction could not be executed because the gateway is not equipped to detect one of the requested events
- The transaction could not be executed because the gateway is not equipped to generate one of the requested signals
- The transaction could not be executed, because the endpoint does not have sufficient resources at this time
- The transaction could not be executed, because the endpoint does not have enough resources available [permanent condition]
- The transaction could not be executed, because the endpoint is [restarting]
- The transaction could not be executed, due to a transient error
- The transaction could not be executed, due to some unspecified transient error
- The transaction could not be executed, endpoint does not have enough resources available
- The transaction has been queued. An actual completion message will follow later
- The transaction is currently being executed. An actual completion message will follow later
- The transaction refers to an incorrect connection-id
- The transaction refers to an unknown call Id
- The transaction time out
- The transaction was aborted by some external action
- Unknown action or illegal combination of actions
- Unknown extensions in local connection options
- Unknown or unsupported command
- Unknown or unsupported digit map extension
- Unknown or unsupported quarantine handling
- Unknown or unsupported RestartMethod

- Unsupported or invalid mode
- Unsupported or unknown package
- Unsupported values on local connection options

# Trunk Reason Responses

The following responses can be returned for the trunk reason (trunk-reason) response. One or more values can be returned, depending upon the operating conditions of the Call Agent.

- ACL_CONGESTION_LEVEL_1—automatic congestion level (ACL) congestion is at level 1.
- ACL_CONGESTION_LEVEL_2—ACL congestion is at level 2.
- ACL_CONGESTION_LEVEL_3—ACL congestion is at level 3.
- DPC_INACCESSIBLE—the DPC is not accessible.
- HARDWARE-BLOCK—trunk-termination is manually controlled OOS (controlled mode=FORCED).
- MAINT-BLOCK—trunk-termination is manually controlled OOS (controlled mode=GRACE).
- MAINT-BUSY—trunk-termination is in maintenance state; controlled to MAINT.
- MAINT-OOS—trunk-termination is manually controlled OOS. (There is no difference between this and a BLOCK.)
- NON-FAULTY—Not blocked, available for service.
- OUTGOING_RESTRICTED—the outgoing call is not allowed.
- SIGNALLING-FAULT—Cannot exchange messages with public switched telephone network (PSTN) network:
  - dpc unavailable
  - user part unavailable
  - stcp association unavailable
  - Signaling link is faulty.
  - dpc congestion
- TERM-FAULT—Bearer termination is in faulty condition.
- TFC_CONGESTION_LEVEL_1—Transfer controlled (TFC) congestion is at level 1.
- TFC_CONGESTION_LEVEL_2—TFC congestion is at level 2.
- TFC_CONGESTION_LEVEL_3—TFC congestion is at level 3.
- TFC_INTL_CONGESTION
- UNKNOWN_REASON

# Trunk Termination Reason Responses, Signaling System 7 Only

The following responses can be returned for the trunk terminations on SS7 trunks. One or more values can be returned, depending upon the operating conditions of the Call Agent, in addition to the reason responses listed under Trunk Reason Responses.

- ACT_LOC_INIT_RESET—Reset circuit at startup as specified by command line argument for SGA process in the platform.cfg. Remains set until reset circuit (RSC)/group reset (GRS) and release complete (RLC)/group reset acknowledge (GRA) messages are exchanged with the remote switch.
- ACT_LOC_MML_RESET—This is set when the reset command is issued from the CLI and remains set until reset is performed. Remains set until RSC/GRS and RLC/GRA messages are exchanged with the remote switch.
- ACT_LOC_QUERY—This is set when the a diagnostic command is issued from the CLI to perform a circuit query and remains set until circuit query message (CQM) and circuit query response (CQR) messages are exchanged with a remote switch.
- ACT_LOC_UPU—This is set when ITP informs that the user part is unavailable and remains set until a circuit verification response (CVR) is received or the ITP informs that the user part is available. The first incoming message will also clear this response.
- ACT_LOC_VALIDATE—This is set when the a diagnostic command is issued from the CLI to perform a circuit validation and remains set until circuit validation test (CVT) and CVR messages are exchanged with the remote switch.
- ACT_LOC_COTTEST—This is set when the a diagnostic command is issued from the CLI to perform a customer-originated trace (COT) test and remains set until SRINI TO CHECK messages are exchanged with the remote switch.
- ACT_LOC_STOP—This is set to clear a call when a term-fault is received.
- BLK_LOC_UPU—This is set when a trunk is blocked because user part is unavailable.
- DES_LOC_GRACE—Local hardware restart in progress (RSIP) graceful.
- DES_LOC_SIG—SS7—This is set when cannot exchange messages with PSTN network (a signaling fault):
  - dpc unavailable
  - user part unavailable
  - stcp association unavailable
  - Signaling link is faulty.
  - dpc congestion
- SIGNALLING-FAULT-This is set to indicate that the Cisco BTS 10200 Softswitch processed a DES_LOC_SIG—SS7 signaling fault.
- DES_LOC_FORCE—Local hardware failure.
- DES_LOC_MML—MMLQ—This is set when a control command is issued with mode=graceful and target-state=OOS. Also set during CQR processing.
- DES_LOC_UPU—This is set when user part is unavailable.
- JOB_PENDING—Ongoing job in progress. There is an ongoing action of message exchange with the remote switch.
- JOB_REC—Job was received by the message definition language (MDL) component and is being processed.

- OPER_ACTIVE—Trunk is available for calls.
- REMOTE_GRACE—Trunk is blocked remotely because of a CLI command on the remote switch.
- REMOTE_FORCE—Trunk is blocked remotely because of a hardware failure on the remote switch.
- RESERVE_SPARE1—Reserved for future use.
- RESERVE_SPARE2—Reserved for future use.
- TERM_GRACE—Trunk is gracefully blocked because of an RSIP graceful from the MGW.

# Fault Reason Responses

The following responses can be returned for the fault reason (fault-reason) response for a subscriber termination command. One or more values can be returned, depending upon the operating conditions of the Call Agent.

- The media gateway is down.
- The media gateway is unreachable.
- The media gateway is in a faulty state.
- The media gateway is transitioning to another state.
- The transaction could not be executed, due to a transient error.
- The transaction could not be executed because the endpoint is unknown.
- The transaction could not be executed because the endpoint is not ready.
- The transaction could not be executed, endpoint does not have enough resources available.
- The transaction could not be executed because a protocol error was detected.
- The transaction could not be executed because the command contained an unrecognized extension.
- The transaction could not be executed because the gateway is not equipped to detect one of the requested events.
- The transaction could not be executed because the gateway is not equipped to generate one of the requested signals.
- The transaction could not be executed because the gateway cannot send the specified announcement.
- Invalid conn identifier.
- Invalid call ID.
- Unsupported mode or invalid mode.
- Unsupported or unknown package.
- Endpoint does not have a digit map.
- The transaction could not be executed because the endpoint is restarting.
- Endpoint redirected to another Call Agent.
- No such event or signal.
- Unknown action or illegal combination of actions.
- Internal consistency in local connection options.
- Unknown extensions in local connection options.
- Insufficient bandwidth.

- Missing remote connection descriptor.
- Incompatible protocol version.
- Internal hardware failure.
- CAS signaling protocol error.
- Failure of a group of trunks.
- Unsupported values on local connection options.
- Response too big.
- Endpoint malfunctioning.
- Loss of lower connectivity.
- Endpoint taken out of service.
- No fault reason available.

# Protocol Troubleshooting

This section provides the troubleshooting information for resolving Cisco BTS 10200 Softswitch protocol problems.

## Troubleshooting Signaling System 7 SIGTRAN Problems

This section describes tools and procedures for troubleshooting SIGTRAN problems on the Cisco BTS 10200 Softswitch and Cisco ITP. It also describes how to clear SIGTRAN related Cisco BTS 10200 Softswitch alarms. In the descriptions within, 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 Softswitch logs, and invoking ITP control and status requests.

For details on Cisco ITP operations, refer to the *Cisco IP Transfer Point Manual* at the following url:

http://www.cisco.com/univercd/cc/td/doc/product/wireless/moblwrls/itp/

This section contains the following sections:

- Cisco Internet Protocol Transfer Point Troubleshooting Procedures
- Viewing Cisco BTS 10200 Softswitch Logs
- 'Troubleshooting Transaction Capabilities Application Part with the Query Verification Tool

### Cisco Internet Protocol Transfer Point Troubleshooting Procedures

The following procedures are useful for troubleshooting problems on the Cisco ITP. This section contains the following procedures:

- Internet Protocol Transfer Point System Messages
- Logging On to the Internet Protocol Transfer Point
- Viewing the Internet Protocol Transfer Point Configuration
- Internet Protocol Transfer Point Status Commands
- Controlling Internet Protocol Transfer Point Resources

### Internet Protocol Transfer Point 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 at:

http://www.cisco.com/univercd/cc/td/doc/product/wireless/moblwrls/itp/23sw/index.htm

### Logging On to the Internet Protocol Transfer Point

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. The enable mode is password protected. To get into enable mode, after logging in to the ITP, type **enable**. You will be prompted for the enable password.

### Viewing the Internet Protocol Transfer Point 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.

### Internet Protocol Transfer Point Status Commands

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

- show cs7 as—Retrieves the application server (AS) status
- show cs7 asp—Retrieves the application service provider (ASP) status
- show cs7 linkset—Retrieves the Signaling System 7 (SS7) linkset status
- show cs7 route—Retrieves the SS7 route status
- show cs7 group state—Retrieves the signaling gateway (SG) group status

### Controlling Internet Protocol Transfer Point 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-ls)#

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
```

## Using Cisco BTS 10200 Softswitch Command Line Interface Commands

In the following sections, examples of Cisco BTS 10200 Softswitch CLI commands are used to aid in resolving Cisco BTS 10200 Softswitch 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, please see the *Cisco BTS 10200 Softswitch Command Line Interface Reference Guide, Release 4.5,* at the following universal resource locator (URL):

http://www.cisco.com/univercd/cc/td/doc/product/voice/bts10200/bts4_5/cli/index.htm

## Viewing Cisco BTS 10200 Softswitch Logs

Viewing Cisco BTS 10200 Softswitch logs is helpful when debugging MTP3 user adaptation (M3UA) related objects of the Cisco BTS 10200 Softswitch. 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:

- Configuration (CFG)
- STATUS
- Protocol decode unit (PDU)
- STATISTICS
- Control (CTRL)
- PLATFORM

Network objects include:

- Stream Control Transmission Protocol (SCTP)
- Signaling gateway process (SGP)
- SG
- Destination point code (DPC)

- Originating point code (OPC)
- Routing key (RKEY)
- CC_ROUTE

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

- M3UA Interface Module (MIM) CFG SCTP—Display how the SCTP has been configured at startup.
- MIM PDU—Trace incoming and outgoing ISUP messages at the MIM layer.
- MIM STATUS DPC—Display how the 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 SGA/MIM module.
- MIM CTRL SCTP—Determine if an SCTP association has been administratively taken out of service or put back in service.

## 'Troubleshooting Transaction Capabilities Application Part with the Query Verification Tool

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

http://www.cisco.com/univercd/cc/td/doc/product/voice/bts10200/bts4_4/featmods/qvttvt.htm#wp1168709

This section contains the following:

- Table Configuration Problems

### Table Configuration Problems

The CLI query command with the table-info option displays the tables used for routing the external SS7 queries on the Cisco BTS 10200 Softswitch. The query command can identify the following problems:

- Missing Call Agent (CA)-CONFIG table
- Missing SLHR-PROFILE table
- Missing Service Logic Host Route (SLHR) table
- Missing DPC table
- Missing OPC table
- Missing SUBSYSTEM-PROFILE table
- Missing SUBSYSTEM table
- Missing signaling connection control part (SCCP)-network (NW) table
- Missing SCCP-ROUTE table
- Missing ROUTING-KEY table
- Missing SG group (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.

# Debugging Network Related Transaction Capabilities Application Part/Signaling Connection Control Part 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.

This section contains the following:



## No Translation for an Address of Such Nature

| | |
|---|---|
| Layer | SCCP |
| Version | ITU88, ITU92, ITU96, ANSI88, ANSI92 |
| Location | Signal transfer point (STP) |
| Cause | The global text telephony (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 | Add the GTT entry in the STP. |

### Subsystem Congestion

| | |
|---|---|
| Layer | SCCP Subsystem (TCAP) |
| Version | ITU88, ITU92, ITU96, ANSI88, ANSI92 |
| Location | Service control point (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, Internet Engineering Task Force (IETF) RFC 2960 for SCTP |
| Location | Local, STP, or SCP |
| Cause | The Broadband Telephony Softswitch (BTS)-ITP sctp-association is down or the SS7 link, linkset, or route is down. |
| Solution | See Chapter 13, "Network Troubleshooting," section 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 central processing unit (CPU) power. Hardware needs to be upgraded or more Cisco BTS 10200 Softswitch 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 Technical Assistance Center (TAC) for assistance. |

### Signaling Connection Control Part Failure

| | |
|---|---|
| Layer | SCCP |
| Version | ITU88, ITU92, ITU96, ANSI88, ANSI92 |
| Location | Local, STP, or SCP |
| Cause | The 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 (Feature Server for AIN services (FSAIN) or Feature Server for POTS, Tandem, and Centrex services (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. |

### Query Verification Tool Timeout

| | |
|---|---|
| Location | 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. |

### Command Line Interface Timeout

| | |
|---|---|
| Location | Local |
| Cause | The Element Management System (EMS) and CA.FSAIN/FSPTC connection is down or the selective call acceptance (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 connection is down, verify whether the Internet Protocol (IP) routing is correct and the OptiCall Messaging System (OMS) hub is in service. |

# Troubleshooting H.323 Problems

This section provides examples of possible problems you may encounter while working with H.323, and recommended solutions:



## Outgoing Trunk Group is Out of Service

```
[I4 10:40:00.299 BCM  01-1 BCM_Main]  "bcm_sel_term_tg_id(): get_tg_from_route() fail"
[bcm_bcsm_util.c:2614]
[***ERROR*** 10:40:00.299 BCM  01-1 BCM_Main   ]  "Route Selection Failure"
[bcm_obcsm_sa_proc.c:3961]
```

This is an indication that the outgoing H.323 trunk group is out of service.

Verify the status of outgoing trunk group as follows:

```
CLI>status trunk_grp id=8991;
Reply : Success:

TGN ID -> 8991
ADMIN STATE -> ADMIN_OOS
OPER STATE -> Trunk group in-service
REASON -> ADM executed successful
RESULT -> ADM configure result in success
```

### Solution

Use CLI to place the trunk_grp in-service as follows:

```
CLI> control trunk_grp id=8991; target-state=ins; mode=forced;
```

## Outgoing H.323 Gateway is Out of Service

```
[***WARNING**** 10:47:44.793 H3A3 01-1 Main ] "Call failure H3A--->BCM sent for csaid=41
callid=0 reason=H323 gateway/gk seem to be OOS" [h3a_sig_sai.c:1525]
```

This is an indication that the outgoing H.323 gateway is "out of service".

Verify the status of outgoing H.323 gateway:

```
CLI> status h323_gw id=CHINA_3;
Reply : Success:

ADMIN STATE -> ADMIN_OOS
H3A PROCESS NUMBER -> 32
H3A PROCESS NAME -> H3A3
ENDPOINT ID ->
ACTIVE CALLS -> 0
RAS STATE -> CCH323_RAS_STATE_NONE
RAS PORT -> 0
IP ADDRESS ->
REGISTERED GATEKEEPER ID -> NOT REGISTERED
PRIMARY GATEKEEPER ID ->
PRIMARY GATEKEEPER PORT -> 0
PRIMARY GATEKEEPER IP ->
H323 VERSION -> 4
TIME TO LIVE -> 0
NUM ALT GATEKEEPERS -> 0
ALT GATEKEEPER PERMANENT -> FALSE
THRESHOLD ENABLED -> FALSE
OUT OF RESOURCES -> FALSE
ALT GATEKEEPER LIST ->
```

### Solution

Use CLI to place the h323_gw in-service as follows:

```
CLI> control h323_gw id=CHINA_3; target-state=ins;
Reply : Success: CLI change successful

H323GW ID -> CHINA_3
INITIAL STATE -> ADMIN_OOS
REQUEST STATE -> ADMIN_INS
RESULT STATE -> ADMIN_INS
FAIL REASON -> ADM found no failure
REASON -> ADM executed successful
RESULT -> ADM configure result in success
```

## H.323 Gateway Fails to Register With Gatekeeper (Invalid Alias)

When the H.323 gateway registers with a gatekeeper, sometimes an alias list is provided to the gatekeeper in the registration request (RRQ) message from gateway. Currently, this configuration is supported on Integrated Operating System (IOS) gateways (not in use on Cisco BTS 10200 Softswitch) when Foreign Exchange Station (FXS) ports are involved. If an request rejected (RRJ) message is received by gateway with reject reason of "invalidAlias", this is symptomatic of an alias list being provided to the gatekeeper but the gatekeeper not configured to be responsible for the prefix associated with each of the aliases.

```
[+ .            H3A3 .    .          ] "value RasMessage ::= gatekeeperReject : "
[+ .            H3A3 .    .          ] "    {"
[+ .            H3A3 .    .          ] "      requestSeqNum 11"
[+ .            H3A3 .    .          ] "      protocolIdentifier { 0 0 8 2250 0 3 }"
[+ .            H3A3 .    .          ] "      rejectReason invalidAlias : NULL"
[+ .            H3A3 .    .          ] "    }"
```

- Example:

  Local gatekeeper that gateway is trying to register with configured as follows:

  - zone prefix China-GK 30*
  - zone prefix China-GK 281*
  - zone prefix China-GK 29*

  Gateway has the following aliases that it wishes to register with:

  c2620.50#show gateway

  Gateway China-GW1 is not registered to any gatekeeper

  Alias list (CLI configured)

  - E164-ID 20751101
  - E164-ID 20751102
  - E164-ID 20751103
  - E164-ID 20751104

  In this case, China-GK does not have a prefix to match any of the E164 numbers.

### Solution

Add a zone prefix entry to China-GK that would cause a match on the alias numbers that are trying to be registered as follows:

- zone prefix China-GK 20*

## Outgoing H.323 Gateway Unregistered With Gatekeeper and Needs to Use Registration, Admissions, and Status

```
[I4 10:52:44.824 H3A3 01-1 Lib_DBM] "H3A: h3a_use_ras Checking for RAS" [h3a_dbm.c:543]
[I4 10:52:44.824 H3A3 01-1 Lib_DBM] "h3a_get_dest_ip_addr: Need to use RAS ......"
[h3a_dbm.c:484]
[4? 10:52:44.824 H3A3 01-1 H_EVT] ": for callID 5 <cch323_call_setup_normal in
gw/src/cch323_gw_api.c:4247>"
 [bts/os/src/bts_debug.c:200]
[4? 10:52:44.824 H3A3 01-1 H_225_EVT]  "H.225 SM: process event H225_EVENT_RAS_RESOLVE,
for callID 5 <cch323_send
_event_to_h225 in gw/src/cch323_h225.c:337>" [bts/os/src/bts_debug.c:200]
[4? 10:52:44.824 H3A3 01-1 H_225_EVT]  "cch323_run_h225_sm: received event
H225_EVENT_RAS_RESOLVE while at state
H225_IDLE <cch323_run_h225_sm in gw/src/cch323_h225.c:10085>" [bts/os/src/bts_debug.c:200]
[4? 10:52:44.824 H3A3 01-1 H_EVT]  ": state = 0 <cch323_traverse_enum_contact_list in
gw/src/cch323_gw_api.c:
4652>" [bts/os/src/bts_debug.c:200]
[I3 10:52:44.824 H3A3 01-1 Main]  "Rel message from STACK--->H3A for callid=5, cause
code=16" [h3a_sig_sai.c:1549]
```

This is an indication that the outgoing H.323 gateway needs to use Registration, Admissions, and Status (RAS) to complete the call, but because the gateway is not registered with a gatekeeper, the call is released.

Verify the status of the H.323 gateway with CLI command as follows:

```
CLI>status h323_gw id=CHINA_3;
Reply : Success:

ADMIN STATE -> ADMIN_INS
H3A PROCESS NUMBER -> 32
H3A PROCESS NAME -> H3A3
ENDPOINT ID ->
ACTIVE CALLS -> 0
RAS STATE -> CCH323_RAS_STATE_GRQ
RAS PORT -> 59723
IP ADDRESS -> 10.89.225.165
REGISTERED GATEKEEPER ID -> NOT REGISTERED
PRIMARY GATEKEEPER ID -> China-GK
PRIMARY GATEKEEPER PORT -> 1719
PRIMARY GATEKEEPER IP -> 10.89.227.198
H323 VERSION -> 4
TIME TO LIVE -> 0
NUM ALT GATEKEEPERS -> 0
ALT GATEKEEPER PERMANENT -> TRUE
THRESHOLD ENABLED -> FALSE
OUT OF RESOURCES -> FALSE
ALT GATEKEEPER LIST -> CLI>status h323_gw id=CHINA_3;
```

This shows that the H.323 gateway is in service, but it is not registered with a gatekeeper. The following are possible reasons for this: Incorrect provisioning for H323_GW2GK (incorrect gatekeeper (GK) name, incorrect GK IP address, security violation) ---- this can be verified by trace logs as a gatekeeper reject (GRJ) would be sent back by GK as follows:

```
[+  .           H3A3 .    .          ]  "value RasMessage ::= gatekeeperReject : "
[+  .           H3A3 .    .          ]  "    {"
[+  .           H3A3 .    .          ]  "      requestSeqNum 11"
[+  .           H3A3 .    .          ]  "      protocolIdentifier { 0 0 8 2250 0 3 }"
[+  .           H3A3 .    .          ]  "      rejectReason terminalExcluded : NULL"
[+  .           H3A3 .    .          ]  "    }"
```

Gatekeeper is down (no alternate GK or alternate is also down) --- this can be verified by trace logs as a timeout would occur (waiting for gatekeeper confirmation (GCF) or GRJ) after the H.323 gatekeeper request (GRQ) has been sent.

## Stable Calls Are Dropped When Call Agent Switches Over

If Annex E functionality is provisioned on the Cisco BTS 10200 Softswitch, but stable calls are being dropped when the H.323 process restarts or CA switches over, check to see whether configuration is correctly registered with the GK:

**Step 1** Log on to gatekeeper

**Step 2** # show gatekeeper endpoints

**Step 3** Examine the display of the GK, which should look similar to the example below:

| CallSignalAddr | Port | RASSignalAddr | Port | Zone Name | Type | Flags |
|---|---|---|---|---|---|---|
| aaa.bbb.ccc.ddd | 1234 | eee.fff.ggg.hhh | 12345 | City GK | VOIP-gateway (GW) | E |
| iii.jjj.kkk.lll | 5678 | ppp.qqq.rrr.sss | 56789 | City GK | VOIP-GW | E |

**Step 4** Verify that both the CA and H.323 Protocol (H323)-GW are registered with the GK with Flags=E as shown in the above example.

## No Matching Dial Plan Found on Incoming H.323 Trunk Group

```
[I2 14:45:24.288 BCM  01-1 Lib_RTM]  "dial_plan(pcld=45145211, dp_idx=0): no match"
[rtm_dial_plan.c:492]
[***ERROR*** 14:45:24.288 BCM  01-1 BCM_Main]  "No Dial Plan Entry for digits in dial plan
0" [bcm_obcsm_sa_proc.c:8916]
```

After the SETUP message has been received at incoming H.323 gateway, Basic Call module (BCM) uses the dial_plan_id in the incoming trunk group and the called number to find out how to route the call. If no match is found, then this error will be issued.

### Solution

Add an entry to dial_plan for called number and assign the identification (ID) to incoming trunk_grp.

```
CLI> add dial_plan id=cdp1; digit_string=451452; dest_id=ipdest; min_digits=7;
max_digits=10;
CLI> change trunk_grp id=8991; dial_plan_id=cdp1;
```

## Configuration at Softswitch or Gatekeeper Has Placed Routing Into a Loop

```
[I5 10:16:20.921 BCM  01-1 BCM_Main]  "BCM:TPM:Incr Counter( 3 ):4199302144"
[bcm_tpm_proc.c:106]
[***ERROR*** 10:16:20.921 H3A3 01-1 Main]  "alarm=99 reason=<Loop detected!!> call cleared
for callid=1
39 " [h3a_alarms.c:281]
```

### Solution

The routing problem could be in either the gatekeeper or the Cisco BTS 10200 Softswitch. Check the gatekeeper against the dialedDigits pattern in the admission request (ARQ), example:

```
destinationInfo "
[+  .           H3A3 .    .          ]  "      {"
[+  .           H3A3 .    .          ]  "        dialedDigits : "9991231234""
[+  .           H3A3 .    .          ]  "      }"
```

There are multiple ways that a gatekeeper could determine the destCallSignalAddress to send back in a admission confirmation (ACF):

- A registered E.164 address (in this case, highly unlikely)
- A static route configured (has been observed)
- Default routing (highest frequency of problem)

## Outgoing H.323 Calls Routed to Incorrect Endpoint When Using Registration, Admissions, and Status

```
[I3 14:25:17.215 H3A3 01-1 Main]  "Rel message from STACK--->H3A for callid=8, cause
code=3" [h3a_sig_sai.c:1549]
```

After the SETUP message has been sent out, a RELEASE COMPLETE is received from the remote endpoint. In this case, the remote endpoint does not service the destination address (cause code=3).

### Solution

Login to gatekeeper that outgoing H.323 gateway is registered with and determine the routing for called number. Gatekeeper could be configured to route based on several configurations:

- Called number is matched against static routing
- No routing defined for called number, uses default routing
- Routing is based on tech prefix (will be pre-pended to called number in ARQ)

## Outgoing H.323 Calls Routed to Incorrect Endpoint When Using Direct Signaling

```
[I3 14:25:17.215 H3A3 01-1 Main]  "Rel message from STACK--->H3A for callid=8, cause
code=3" [h3a_sig_sai.c:1549]
```

After the SETUP message has been sent out, a RELEASE COMPLETE is received from the remote endpoint. In this case, the remote endpoint does not service the destination address (cause code=3).

Verify the value assigned to the SOFTSW_TSAP_ADDR for the outgoing H.323 trunk group

```
CLI>show trunk_grp id=8991;
Reply : Success: Entry 1 of 1 returned.

ID=8991
CALL_AGENT_ID=CA146
TG_TYPE=H323
SOFTSW_TSAP_ADDR=10.89.227.119;
TG_PROFILE_ID=CHINA
STATUS=INS
DIRECTION=BOTH
SEL_POLICY=ASC
GLARE=SLAVE
ALT_ROUTE_ON_CONG=N
SIGNAL_PORTED_NUMBER=N
DIAL_PLAN_ID=cdp1
DEL_DIGITS=0
OPER_STATUS=NF
```

### Solution

If the value for the SOFTSW_TSAP_ADDR is incorrect, use CLI to make the change as follows:

```
CLI> change trunk_grp id=8991; softsw_tsap_addr=10.89.227.219;
```

## Registration, Admissions, and Status Still Used When Outgoing H.323 Call is Provisioned to Use Direct Signaling

```
[I4 14:29:21.163 H3A3 01-1 Lib_DBM    ]  "H3A: h3a_use_ras Checking for RAS"
[h3a_dbm.c:543]
[I4 14:29:21.163 H3A3 01-1 Lib_DBM    ]  "H3A: we need to use the destIP from trunk_grp
table " [h3a_dbm.c:489]
[***ERROR*** 14:29:21.163 H3A3 01-1 Lib_DBM    ]  "h3a_get_dest_ip_addr: softsw_tsap_addr
not set..." [h3a_dbm.c:494]
```

Although the configuration has specified to no use RAS, if no valid remote endpoint is provided, the fallback mechanism is to try RAS to determine the remote endpoint.

Verify the configuration for the outgoing trunk group with CLI:

```
CLI>show trunk_grp id=8991;
Reply : Success: Entry 1 of 1 returned.

ID=8991
CALL_AGENT_ID=CA146
TG_TYPE=H323
TG_PROFILE_ID=CHINA
STATUS=INS
DIRECTION=BOTH
SEL_POLICY=ASC
GLARE=SLAVE
ALT_ROUTE_ON_CONG=N
SIGNAL_PORTED_NUMBER=N
DIAL_PLAN_ID=cdp1
DEL_DIGITS=0
OPER_STATUS=NF
QOS_ID=china_qos1
TRAFFIC_TYPE=LOCAL
H323_GW_ID=CHINA_3
CAUSE_CODE_MAP_ID=H323_CHINA
ANI_BASED_ROUTING=N
NO_ANSWER_TMR=185
```

Since the SOFTSW_TSAP_ADDR column is not displayed, it contains a null value.

### Solution

Use CLI to change the outgoing trunk group as follows:

```
CLI> change trunk_grp id=8991; softsw_tsap_addr=10.89.227.219;
```

# Troubleshooting Integrated Services Digital Network Problems

This section describes ISDN troubleshooting and maintenance for the Cisco BTS 10200 Softswitch.

## How to Troubleshoot When the Integrated Services Digital Network Trunk Group Fails to Restore

This section shows how to troubleshoot if the ISDN trunk group fails to restore. Determine if the trunk group failed to restore by entering the following command:

```
status trunk-grp id=nnn;
```

- If the response shows Trunk group out-of-service (TG_OOS) for the administrative state, then enter the control command.

```
status trunk-grp id=100;

Reply : Success: Entry 1 of 1 returned.

TGN_ID -100
RESULT -ADM configure result in success
REASON -ADM executed successful
ADMIN_STATE -ADMIN_OOS          <================
OPER_STATE -Trunk group out-of-service
PRIMARY_OPER_STATE -NOT USED
BACKUP_OPER_STATE -NOT USED

control trunk-grp id=nnn;mode=forced; target-state=ins;
```

- If the response does not show an operational state of *Trunk group in-service* for the trunk group (non-facility associated signaling (NFAS) or D-channel backup should also show ISDN_DCHAN_STATE_INS for the D-channel operational status), then:
  - If the response is *Trunk group out-of-service*, go to Step 1.
  - If the response is *Trunk group restore session fail normal, switchover, or maint*, go to Step 2.
  - If the response is *Trunk group restore establish fail normal, switchover, or maint*, go to Step 3.
  - If the response is *ISDN_DCHAN_STATE_WAIT* or *ISDN_DCHAN_STATE_MB,* go to Step 4.
  - If the response is *Trunk group down session set fail hard normal, or maint*, go to Step 5.
  - If the response is *Trunk group down establish fail hard normal, or maint*, go to Step 6.
  - If the response is *Trunk group delete graceful*, go to Step 7.

---

**Step 1** Trunk group state for facility associated signaling (FAS): *Trunk group out-of-service,* or NFAS: *NFAS DCHAN_STATE_MOOS*.

This means the administrative state was set to in-service, but the command to go to operational state was ignored due to bad provisioning.

**Things to Check:**

Make sure that entries exist for this trunk group in the ISDN D Channel table.

**Step 2** Trunk group states for FAS: *Trunk group restore session fail normal, switchover, or maint;* or NFAS: *NFAS ISDN_DCHAN_STATE_SDN.*

This means the Call Agent and the media gateway are not communicating. The backhaul session is not coming up. The problem has to do with the User Datagram Protocol (UDP) port numbers, IP addresses or domain name system (DNS) names, or network connectivity. These values are all provisioned in the Reliable User Datagram Protocol (RUDP) Backhaul Session table in the Call Agent. For Cisco IOS gateways, these values are part of the *session group groupn.....*

**Things to Check:**

a. Do the four entries in the RUDP Backhaul Session table of the Call Agent match the values in the gateway (for Cisco IOS gateways, these values are part of session group groupn...)?

b. If the call-agent-tsap-addr, or the mgw-tsap-addr are DNS names, does **nslookup** on both Call Agents resolve the values to one unique IP address?

c. Can the call-agent-tsap-addr in the four entries be pinged from the media gateway? Do the Call Agents actually have the IP addresses, or DNS names, specified?

d. Can the mgw-tsap-addr be pinged from both Call Agents?

e. Does the trunk-grp isdn-profile exist (show isdn-tg-profile ID=%)? Keep in mind that the profile ID is case sensitive.

f. Snoop can be used to see if the gateway and Call Agent are talking in order to establish the session. Snoop can be used to eliminate whether the problem is on the Call Agent or the media gateway side.

g. The **show backhaul session all** command on the media gateway can be useful in debugging.

h. Look at the trace.log on the Call Agent. Search for BSM_create_ss or bsm_create_ss. This shows the exact values used by the Call Agent.

**Note** Backhaul deletion is triggered by all trunk groups of a backhaul-set being in the admin-oss state. Backhaul creation is triggered by controlling one of the trunk groups to in service (INS). The trunk group list can be determined by using the **show isdn-dchan set-id** command.

**Step 3** Trunk group states for FAS: *Trunk group restore establish fail normal, switchover, or maint* or NFAS: *ISDN_DCHAN_STATE_OOS.*

This means the specific ISDN channel could not be restored. This is likely related to ISDN layer1 or layer2 not being up, or related to DCHAN-SLOT and DCHAN-PORT in the ISDN D Channel table. The media gateway and Call Agent are communicating successfully (session came up).

**Things to Check:**

a. On the media gateway, enter a **show isdn status command**. Is Layer 1 shown as ACTIVE? If not, there may be a cable problem, or the private branch exchange (PBX) is down.

b. Does the **show isdn status** command return a *Network side configuration*? The PBX should be set up for the user side. The gateway should be setup for the network side.

c. Was the media gateway reloaded (rebooted) after setting up parameters? There can be problems when this has not been done. This is usually reflected by having two terminal endpoint identifier (TEI) values for the trunk level one (T1).

d. Are the DCHAN-SLOT and DCHAN-PORT provisioned correctly in the IDSN D Channel table for this trunk group?

e. Does the T1 on the media gateway show an alarm (red or yellow lights)? These are more clues that there is an ISDN layer1 or layer2 problem.

f. Is the controller T1, or interface Serialn:23, provisioned correctly on the gateway?

g. Look at the trace.log on the Call Agent. Search for BSM_dchan_tbl_insert or bsm_dchan_tbl_insert. The slot-port value is the actual value retrieved from the database. For the AS5300, this value should be 0, 1, 2, or 3. This is a decimal value. The top 16 bits are the slot and the bottom 16 bits are the port.

**Step 4** Trunk group states for NFAS: *ISDN_DCHAN_STATE_WAIT/ISDN_DCHAN_STATE_MB.*

This means the states at the far end are sending a SERVICE_ACK to the Cisco BTS 10200 Softswitch service message for primary rate interface (PRI).

**Things to Check:**

Make sure the far end is sending a SERVICE_ACK. There are some other trunk group states that happen after the ISDN backhaul is successfully established.

**Step 5** Trunk group states for FAS: *Trunk group down session set fail hard normal, or maint* or NFAS: *ISDN_DCHAN_STATE_SDN.*

This is the same as *Trunk group restore establish request fail*, or *ISDN DChannel State SDN.* However, in this case, the D channel was already successfully established, and then went out. This likely means that the Call Agent and media gateway have lost IP connectivity. Or, the media gateway has lost power. This can also happen if the provisioning was changed, particularly the session settings in the media gateway.

**Step 6** Trunk group states for FAS: *Trunk group down establish fail hard normal, or maint* or NFAS: *NFAS ISDN_DCHAN_STATE_OOS.*

This is the same as *Trunk group restore establish request fail*, or *ISDN DChannel State OOS*. However, in this case, the D channel was already successfully established, and then went out.

**Things to Check:**

a. Is, or was, the cable unplugged between the PBX and the gateway?

b. Was the provisioning changed on the gateway?

**Step 7** Trunk group state for FAS: *Trunk group delete graceful*.

The following command indicates you are waiting for calls to finish before going to out-of-service. If the wait time is too long, you can control the trunk group with *mode=forced.*

```
control trunk-grp id=xxxx mode=graceful target-state=oos
```

## Checking the Status of a Trunk Termination

Check the status of a trunk termination using the following command:

```
status trunk-termination tgn-id=<trunk group number;cic=<cic number;

Reply : Success:

RESULT -ADM configure result in success
REASON -ADM executed successful
TGN ID -2
CIC -8
TERM ADMIN STATE -ADMIN_INS
TERM OPER STATE -Termination is idle
TERM REASON -No fault reason available
TRUNK STATIC STATE -ACTV
TRUNK DYNAMIC STATE -TRNS
TRUNK REASON -NON_FAULTY
```

The above status shows that the trunk is active, in idle mode, and ready for call use.

If the trunk static state is set to locally blocked, go to the "Trunk Static State Is Set to Locally Blocked" section.

If the trunk static state is set to transient (TRNS), go to the "Trunk Static State Is Set to Transient" section.

If the trunk static state is set to remotely blocked, go to the "Trunk Static State Is Set to Remote Block" section.

If the trunk static state is set to TERM_STATUS_FAULTY, go to the "Termination Status Is Faulty" section.

If the trunk static state returns Cannot Make Call, go to the "Cannot Make a Call" section.

### Trunk Static State Is Set to Locally Blocked

Perform the following steps to check the *TRUNK REASON* field if the *TRUNK STATIC STATE* is set to locally blocked (LBLK) state.

**Step 1** If the TRUNK REASON is set to MAINT-OOS, then a user has manually taken the trunks out of service. The user must manually put the trunks into the in-service mode.

Use the **control** command on the specified trunk to put the trunk back into the in-service mode.

Clear the MAINT-OOS. Trunks should be in active or idle mode and ready for use.

**Step 2** If the TRUNK REASON is set to SIGNALLING-FAULT, then the D channels are not in-service. Check the trunk group ADMIN and OPER states.

- If the trunk group ADMIN state is ADMIN_OOS, use the **control** command to put the trunk group into in-service mode.
- If the trunk group ADMIN state is ADMIN _INS, verify that the trunk group OPER-STATE is IN-SERVICE (see the How to Troubleshoot When the Integrated Services Digital Network Trunk Group Fails to Restore section in case of any issues).
- Clear any SIGNALLING-FAULT states. Trunks must be in active or idle mode and ready for use.

**Step 3** If TRUNK REASON is set to TERM_FAULT, then the terminations are in FAULTY states. Verify the IP connectivity from the CA to the gateway.

**a.** Clear any termination faults at the gateway by turning off, then turning on, Media Gateway Control Protocol (MGCP) (use the mgcp, no mgcp procedure on the media gateway).

**b.** Clear any TERM_FAULT on the Cisco BTS 10200 Softswitch. Trunks must be in active or idle mode and ready for use.

### Trunk Static State Is Set to Transient

Perform the following steps when trunk static state is set to TRNS.

**Note** If trunk static state is set to TRNS, then the PBX has not responded with a SERVICE_ACK or RESTART_ACK for the service or restart message set by the Call Agent.

**Step 1** Verify that the initialization procedure, as depicted by the associated isdn-tg-profile, and as used by PBX, is synchronized.

**Step 2** Verify that the isdn-service-supp token is set to N if PBX does not support service messages.

### Trunk Static State Is Set to Remote Block

Perform the following steps if trunk static state is set to remote block (RBLK).

**Note** If the trunk static state is set to RBLK, and isdn-tg-profile has isdn-farend-init=Y then the PBX must start the initialization procedure, or the PBX specifically sends a service message with SERVICE-OOS mode to the Cisco BTS 10200 Softswitch to put the trunks into the remote out-of-state mode.

**Step 1** Verify that the initialization procedure (ISDN-FAREND-Initialize (INIT) token), as depicted by associated isdn-tg-profile in the Cisco BTS 10200 Softswitch, and as used by the PBX, is in sync.

**Step 2** Using the CLI command "control trunk-termination" to reset the RBLK state, perform a control trunk-termination to OOS, then control trunk-termination to INS—in case there is an error on the PBX side. Also, set the isdn-service-supp token in the ISDN trunk group profile per the procedures supported by the PBX.

### Termination Status Is Faulty

The *TERM_STATUS_FAULTY message* indicates an MGCP problem.

#### Things to Check:

- Is the media gateway (MGW) profile set up for the trunk?
- Is the MGW in the in-service operational state?

Perform the "no mgcp, mgcp" commands on the gateway if an MGCP problem is indicated.

### Cannot Make a Call

If you have a problem making a call, perform the following Things to Check, and then go to the "Checking Media Gateway Provisioning" section on page 14-34

#### Things to Check:

When terminations are added, they have strings like S0/DS1-2/1. The S# refers to the slot number. The DS1-# refers to the port number. The /# at the end refers to the specific B channel (1–23). The slot and port numbers must match the dchan values (dchan-slot, dchan-port) for the related trunk group ID (tgn-ID), assuming that the DS0 is on a T1 that contains a D channel.

## Checking Media Gateway Provisioning

The following example shows how a Cisco IOS gateway is provisioned.

**Note** The typical problem areas are in ***bold italic*** type. Look at the problem area after the Call Agent is provisioned.

```
Current configuration:
!
================
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime localtime
no service password-encryption
!
hostname c2421.200
!
enable password xxxxxxx
!
clock timezone CDT -6
network-clock base-rate 56k
network-clock-select 3 T1 0
network-clock-select 1 T1 1
network-clock-select 2 system (SCB)
IP subnet-zero
!
!
IP domain-name ipclab.cisco.com
IP name-server 10.89.224.1
!
IP audit notify log
IP audit po max-events 100
backhaul-session-manager
  set isdn1 client ft
  group group1 set isdn1
  group group2 set isdn1
  session group group1 10.89.225.223 9000 10.89.227.200 9000 1
  session group group1 10.89.226.223 9001 10.89.227.200 9001 2
  session group group2 10.89.225.224 9000 10.89.227.200 9000 1
  session group group2 10.89.226.224 9001 10.89.227.200 9001 2
isdn switch-type primary-ni
isdn voice-call-failure 0
!
!
!
!
!
!
!
no voice confirmation-tone
voice-card 0
!
controller T1 0
 framing esf
 linecode b8zs
 channel-group 0 timeslots 1-24 speed 64
!
controller T1 1
 framing esf
 linecode b8zs
 pri-group timeslots 1-24 service mgcp
!
!
!
```

```
!
interface Ethernet0
 IP address 10.89.227.200 255.255.255.0
 no cdp enable
!
interface Serial0
 no IP address
 shutdown
!
interface Serial0:0
 no IP address
 IP nat outside
 encapsulation ppp
 shutdown
 no cdp enable
!
interface Serial1:23
 bandwidth 64000
 no IP address
 no logging event link-status
 isdn switch-type primary-ni
 isdn protocol-emulate network
 isdn incoming-voice voice
 isdn bind-l3 backhaul grp1
 no cdp enable
!
IP classless
IP route 0.0.0.0 0.0.0.0 10.89.227.254
no IP http server
IP pim bidir-enable
!
!
access-list 1 permit 10.0.24.0 0.0.0.255
call rsvp-sync
!
voice-port 1:23
!
mgcp
mgcp call-agent mgcp-SYS01CA.ipclab.cisco.com service-type mgcp version 1.0
mgcp dtmf-relay voip codec all mode nte-gw
mgcp package-capability rtp-package
mgcp default-package dt-package
no mgcp timer receive-rtcp
!
mgcp profile default
 timeout tsmax 100
 max2 retries 3
!
dial-peer cor custom
!
!
!
dial-peer voice 1 pots
 application mgcpapp
 port 1:23
!
!
line con 0
line aux 0
line 2 3
line vty 0 4
 password xxxxxxxx
 login
!
```

```
ntp server 10.89.227.254
end
```

## Additional Command Line Interface Verification

Perform the following steps to provide additional CLI verification of a problem:

**Step 1** Use the control command to put the trunk group out of service (OOS) and back into INS:

Place OOS:

```
control tt tgn-id=17; cic=all; target-state=oos; mode=graceful;
```

Place INS:

```
control tgn-id=17; target-state=ins; mode=forced;
```

**Step 2** If the B channel is not IDLE, use the control command to put each circuit OOS and back INS:

Place OOS:

```
control trunk-termination tgn-id=17; cic=1; target-state=oos; mode=forced;
```

Place INS:

```
control trunk-termination tgn-id=17; cic=1; target-state=ins; mode=forced;
```

**Step 3** Check the status of the trunk group:

```
status trunk-grp id=<TG ID number; call-agent-id=<CA ID;
```

If the trunk group status has still not changed to ADMIN_INS—even though the commands in Steps 1 and 2 were successful—then it means that communication to the MGW has been lost. Notify your system administrator and have the problem corrected before continuing.

**Step 4** Check trunk termination and trunk status. The single command shown here queries both the trunk-termination status and trunk (channel) status:

```
status trunk-termination tgn-id=17; cic=all;

CONFIGURATION COMMAND EXECUTED TRUNK_GRP -17 -CIC -1
TERM ADMINstatus -ADMIN_INS
TERM OPERstatus -TERM_STATE_IDLE
CIC STATIC STATE -ACTV
CIC DYNAMIC STATE -IDLE

...
...

CONFIGURATION COMMAND EXECUTED TRUNK_GRP -17 -CIC -23
TERM ADMINstatus -ADMIN_INS
TERM OPERstatus -TERM_STATE_IDLE
CIC STATIC STATE -ACTV
CIC DYNAMIC STATE -IDLE

status trunk-termination tgn-id=17; cic=23

REPLY=CONFIGURATION COMMAND EXECUTED ISDN_TRUNK_GROUP -17 -CIC -23
TERM ADMINstatus -ADMIN_INS
TERM OPERstatus -TERM_STATE_IDLE
CIC STATIC STATE -ACTV
CIC DYNAMIC STATE -IDLE
```

## Maintenance of a Call Agent Connected to an Integrated Services Digital Network Trunk Group

During system operations, the operator can use the CLI *control* command to switch the Call Agent into one of two states:

- ACTIVE-STANDBY
- STANDBY-ACTIVE

When the control command is entered on a Call Agent connected to an ISDN trunk group (D channel), the Call Agent switchover time is approximately 20 seconds. During all but the first 6 seconds of this switchover time, the ISDN D channel is temporarily down. However, the D channel comes back up, and the ISDN trunk group automatically returns to INS, when the switchover completes.

**Note** This switchover process does not have any impact on stable calls.

# File Configuration – bts.properties

This section provides the instructions for extracting the bts.properties file from the util.jar file and for editing and changing configuration information in the extracted bts.properties file. The default content of the /opt/ems/etc/bts.properties file is in listed in Table 14-1.

***Table 14-1 Default Content of the bts.properties File.***

| Parameter | Variable |
|---|---|
| reportDir= | /opt/ems/report |
| reportDirSize= | 50000000 |
| reportSuffix= | .html |
| logDefLevel= | INFO |
| logMaxFileSize= | 50000000 |
| logMinFileSize= | 1000 |
| logDefFileSize= | 4000000 |
| logDir= | /opt/ems/log |
| logName= | BtsEms |
| logSuffix= | .log |
| logBakupSuffix= | .bak |
| usersDir= | /opt/ems/users |
| etcDir= | /opt/ems/etc |
| ftpErrorsAllowed= | 3000 |
| smgResources= | com.sswitch.oam.smg.smg |
| requestTimeout= | 60000 |
| nbsLib= | /opt/BTSlib/lib/libnbs.so |
| scTimeout= | 50000 |

*Table 14-1 Default Content of the bts.properties File.*

| Parameter | Variable |
|---|---|
| invalidChars= | "';<br>**Note** # spaces or other white space characters may be considered invalid. |
| LERGDuration= | 86400000 |
| throttleEnable= | N |

## File Extraction and Editing – bts.properties

Prior to extraction, the bts.properties file is part of the util.jar file. To change any of the bts.properties file parameters, it must be extracted from the util.jar file. Use the following instructions to extract the bts.properteries file from the util.jar file and to edit the extracted bts.properties file.

**Step 1** Locate the util.jar file and unjar it.

**Step 2** Locate to the bts.properties file in the directory that was unjared in Step 1.

**Step 3** Edit the bts.properties file to change the desired parameter(s).

**Step 4** Rejar the whole directory containing the bts.properties file.

**Step 5** Replace the old util.jar file with the new util.jar file created in Step 4.

**Step 6** Shutdown and restart the affected processes.

# Privacy Screening Troubleshooting

This section lists several privacy screening troubleshooting symptoms and solutions.

## Symptom One

With a Cisco 2421, calls are placed, but PRIVACY SCREENING is not displayed on the caller-id display for the subscriber.

## Solution One

Telnet to the Cisco 2421 and set dtmf-relay mode to nse. For example, execute the following command in config mode:

```
mgcp dtmf-relay voip codec all mode nse
```

## Symptom Two

The caller or the subscriber is on a Cisco ATA MGW and CRCX/MGCX is failing.

## Solution Two

Either the PS feature or the PS_MANAGE feature is working but not both.

For the trunk group against the DN that is mapped to the PS App, verify that the softsw-tsap-addr is set to an IP address and not a domain name. For the trunk group against the DN that is mapped to the PS_MANAGE App, verify that the softsw-tsap-addr is set to a domain name and not an IP address.

## Symptom Three

Privacy Screening is not able to collect digits or record with a Cisco 2421.

## Solution Three

In the Cisco 2421 media gateway, execute the following command:

```
mgcp rtp payload cisco-pcm-switch-over-ulaw 126
```

## Symptom Four

Only one Privacy Screening or Privacy Screening PIN Management application works for a subscriber.

## Solution Four

Verify the pilot number of the organization in the Privacy Screening application to which the subscriber belongs. This should match the ACCESS_DN in the app-server table to which the subscriber is associated.