CHAPTER 14

General Troubleshooting

Revised: July 2010, OL-23033-01

Introduction

The chapter provides the general troubleshooting information you need for conducting 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 CORBA Adapter Interface Specification Programmer's 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 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
- Call Agent Controlled Mode for RFC 2833 DTMF Relay Troubleshooting—Describes general troubleshooting procedures related to the call agent controlled mode for RFC 2833 DTMF relay
- NCS I10 and Audit Connection Troubleshooting—Describes the general troubleshooting procedures related to NCS I10 and the audit connection
- Multi-Lingual Support Troubleshooting—Describes the general troubleshooting procedures related to multi-lingual support
- Viewing Trace Logs for Throttled Flood of MGCP Messages From Specific Endpoint—Describes the general troubleshooting procedures related to viewing trace logs for a throttled flood of MGCP messages

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 CORBA Problems

To troubleshoot CORBA interface problems, refer to the *Cisco BTS 10200 CORBA Adapter Interface Specification Programmer's Guide*.

Troubleshooting Local Number Portability Problems

Problems can arise when a subscriber's telephone number is ported 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.

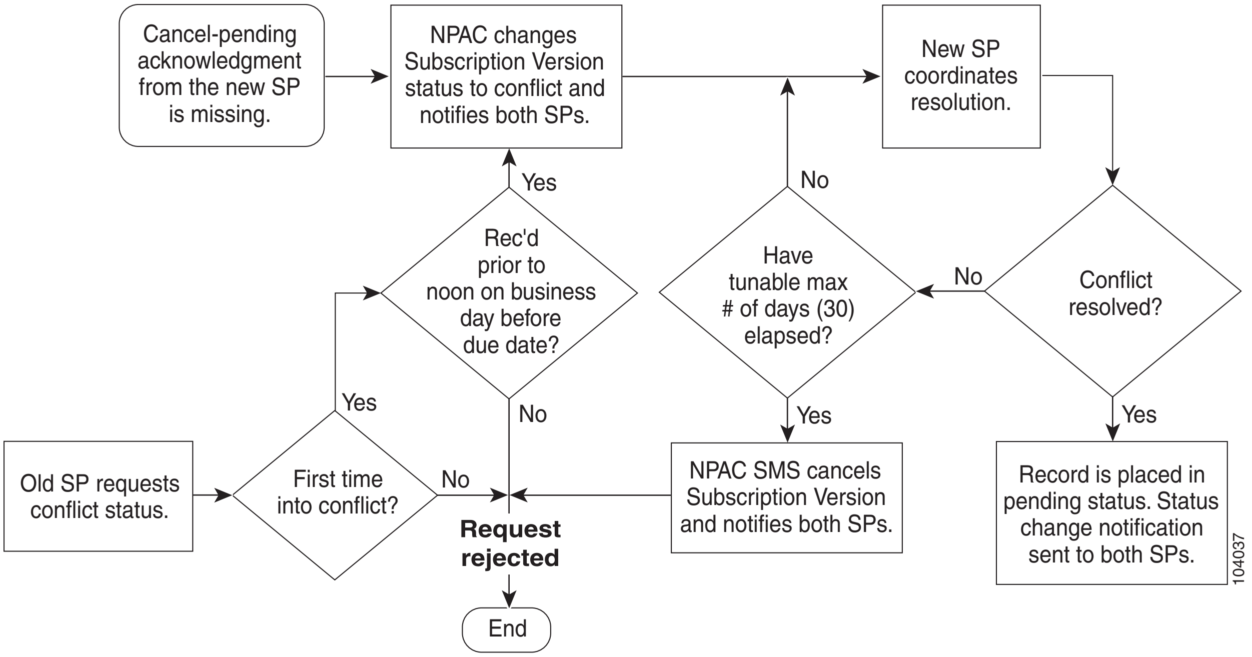
If either the old or new service provider did not send a notification to the NPAC SMS, the NPAC SMS notifies the service provider from which it did not receive a notification that it is expecting a notification. If the NPAC SMS receives the missing notification, and both notifications indicate agreement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


Cancel-pending acknowledgment from the new SP is missing.
NPAC changes Subscription Version status to conflict and notifies both SPs.
New SP coordinates resolution.
Yes
No
Rec'd prior to noon on business day before due date?
Have tunable max # of days (30) elapsed?
No
Conflict resolved?
Yes
No
Yes
Yes
Old SP requests conflict status.
First time into conflict?
No
NPAC SMS cancels Subscription Version and notifies both SPs.
Record is placed in pending status. Status change notification sent to both SPs.
Request rejected
End
104037

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 might 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) address, 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 that one of the following three cases, as applicable:

- Verify that the ALERT_NOTIFY feature 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 the ALERT_NOTIFY feature is included in the default office service ID (if the feature is intended to be offered 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 and the 3PTYFS.

Example:

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

The following details apply to the Signaling (12) alarm:

- For a 3PTYFS that is more than one hop away from the Cisco BTS 10200, Signaling (12) alarm is raised when communications between the Cisco BTS 10200 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 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 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, SS7 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 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 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 protocol problems.

Troubleshooting H.323 Problems

To troubleshoot H.323 problems, refer to the *Cisco BTS 10200 Softswitch H.323 Guide*.

Troubleshooting Integrated Services Digital Network Problems

To troubleshoot Integrated Services Digital Network (ISDN) problems, refer to the *Cisco BTS 10200 Softswitch ISDN Guide*.

Troubleshooting PacketCable Problems

To troubleshoot PacketCable problems, refer to the *Cisco BTS 10200 Softswitch PacketCable Guide*.

Troubleshooting SIP Problems

To troubleshoot SIP problems, refer to the *Cisco BTS 10200 Softswitch SIP Guide*.

Troubleshooting SS7 SIGTRAN Problems

To troubleshoot Signaling System 7 SIGTRAN problems, refer to the *Cisco BTS 10200 Softswitch SS7 SIGTRAN Guide*.

File Configuration—bts.properties

This section provides instructions for editing and configuring the bts.properties file. The default content of the /opt/ems/etc/bts.properties file is in listed in Table 14-1.

Note Modification of the bts.properties file should not be attempted without Cisco TAC support or supervision.

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

Parameter	Variable
reportDir=	/opt/ems/report
reportDirSize=	50000000
reportSuffix=	.html
logDefLevel=	Information
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
invalidChars=	‘‘’; # spaces or other white space characters are considered invalid.
LERGDuration=	86400000
throttleEnable=	N

Editing—bts.properties

Note Modification of the bts.properties file should not be attempted without Cisco TAC support or supervision.

Use the following instructions to edit the bts.properties file:

Step 1 Edit the /opt/ems/etc/bts.properties file to change the desired parameter(s).

Step 2 Shut down and restart the affected processes.

Edit Example—bts.properties

The following instructions show how to configure the bts.properties file to enable debugging.

Note Modification of the bts.properties file should not be attempted without Cisco TAC support or supervision.

Step 1 Open the /opt/ems/etc/bts.properties file.

Step 2 Set logDefLevel=debug.
//valid logging options are: info, debug, error, warning, fatal

Step 3 Start a new CLI session.
//su - btsuser

Step 4 Look for the log information in the /opt/ems/log/<username>.log. It is //btsuser.log in this case.

Privacy Screening Troubleshooting

This section lists several privacy screening troubleshooting symptoms and solutions.

Symptom 1

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

Solution 1

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 2

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

Solution 2

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

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

Symptom 3

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

Solution 3

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

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

Symptom 4

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

Solution 4

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 with which the subscriber is associated.

Call Agent Controlled Mode for RFC 2833 DTMF Relay Troubleshooting

This section describes general troubleshooting procedures related to the call agent controlled mode for RFC 2833 DTMF relay.

General Troubleshooting Procedures

This section explains how to troubleshoot the following conditions:

- Basic Call Cannot Be Established
- No DTMF Relay Involving H.323 Endpoints

Basic Call Cannot Be Established

Problem: A basic call cannot be established through the MGW.

Symptom: The CRCX message sent to the MGW results in failure.

Diagnosis: Determine whether the MGW supports CA-controlled RFC 2833 DTMF relay. (See the MGW vendor documentation for information on MGW features.)

Resolution: If the MGW does not support CA-controlled RFC 2833 DTMF relay, set dtmf-telephone-event-enabled=N in the QoS table associated with the endpoint.

No DTMF Relay Involving H.323 Endpoints

Problem: RFC 2833 DTMF relay does not work on the H.323 gateway or endpoint.

Symptom: DTMF tones do not go through.

Diagnosis: Determine whether the RFC 2833 payload configured on the H.323 gateway or endpoint matches the payload configured on the Cisco BTS 10200.

Resolution: Ensure that the value of rfc2833-payload in the applicable h323-tg-profile or h323-term-profile table is set to the same value as that on the H.323 gateway or endpoint.

NCS I10 and Audit Connection Troubleshooting

This section explains how to troubleshoot the following conditions:

- General Troubleshooting Information
- Troubleshooting the Timeout Queue
- Troubleshooting QoS
- Troubleshooting Audit Connection

General Troubleshooting Information

Call Agent (CA) log files are located in /opt/OptiCall/CA[XYZ]/bin/logs directory, where XYZ is the CA instance (for example CA146). If you need to call Cisco TAC regarding a call-processing issue, first collect the log files from this directory if possible.

Troubleshooting the Timeout Queue

Problem: Due to a change in NCS protocol specifications, MGCP command timeout has increased by a factor of 2.

Symptoms: Increased memory usage on slow networks and during major outages of MGCP devices.

Diagnosis: Memory usage returns to normal when network connectivity to MGCP devices is restored.

Resolution: Great care needs to be taken when MGCP-T-HIST and MGCP-T-MAX parameters are provisioned in the ca-config table. If necessary, reduce the values of MGCP-T-HIST and/or MGCP-T-MAX parameters. Note that MGCP-T-HIST must be greater than or equal to MGCP-T-MAX + 10 seconds; otherwise the provisioned settings are ignored by the system (the system reverts to the default values for these parameters).

Note For a detailed discussion of keepalive timeout parameters, see Appendix B, "System Usage of MGW Keepalive Parameters."

Troubleshooting QoS

Problem: Endpoint does not support silence suppression and/or echo cancellation.

Symptom: Silence suppression and/or echo cancellation parameters provisioned on the Cisco BTS 10200 are not reflected in MGCP device behavior.

Diagnosis:

1. Through CLI commands, take the MGCP device out of service. Make sure to take the entire MGCP device out of service (control mgw...) because disabling the terminations is not sufficient.
2. Put the MGCP device back in service.

Use network packet analysis software to observe the response to an AUEP command. Look through each "A:" (capabilities) line and verify that "s:on" (silence suppression supported) and/or "e:on" (echo cancellation supported) are not present.

Resolution:

- If the endpoint reports “e:on” in its capabilities, but provisioned echo cancellation settings are ignored, verify that EC-SUPP is enabled for the MGCP device in the mgw-profile table.
- Upgrade the MGCP device firmware.
- Contact the device manufacturer if the MGCP device advertises support for silence suppression/echo cancellation but does not report it to the CA.

Troubleshooting Audit Connection

Problem: Stray connections have not been removed after failover.

Symptoms: Endpoint(s) unable to place feature calls, dropped active calls after a Cisco BTS 10200 failover.

Diagnosis: Place a call through the endpoint. Use network packet analysis software to observe any negative CreateConnection (CRCX) ACK responses from the MGCP device. Check whether error messages in the negative ACK responses indicate that connection resources are not available (which suggests that the resources are not being cleaned up).

Resolution: Enable AuditConnection support for MGCP profile corresponding to MGCP device.

Multi-Lingual Support Troubleshooting

This section describes general troubleshooting procedures.

Ensure the subscriber has MLS using report billing_record:

```
DIALEDDIGITS=*56
CALLTERMINATIONCAUSE=NORMAL_CALL_CLEARING
```

*56 is the VSC entered by the subscriber to start MLS. NORMAL_CALL_CLEARING shows the IVR successfully completed its service.

If NORMAL_CALL_CLEARING does not return, check both the service and subscriber_service_profile tables:

```
btsadmin> show service id=mlstest
ID=mlstest
FNAME1=MLS
btsadmin>show subscriber_service_profile sub-id=2212437211
SUB_ID=2212437211
SERVICE_ID=mlstest
```

If you hear a reorder-tone from a SIP phone, ensure the status of the Cisco BTS 10200 announcement table is all of the following:

```
btsadmin> status tt tgn-id=889;cic=all
889 1   ADMIN_INS     TERM_ACTIVE_IDLE      ACTV   IDLE   NON_FAULTY
```

If you hear a click from an MGCP phone, ensure the status of the Cisco BTS 10200 announcement table is all of the following:

```
btsadmin> status tt tgn-id=889;cic=all
889 1   ADMIN_INS     TERM_ACTIVE_IDLE      ACTV   IDLE   NON_FAULTY
```

If you hear a reorder tone instead of audio, ensure the release_cause table routes to correct MS:

```
btsadmin> show release_cause
ID=1
ANNC_ID=18
btsadmin> show announcement
...
ANNOUNCEMENT_FILE=ann_id_18.au
ROUTE_GUIDE_ID=10013
```

Ensure that the IVR script points to the correct MS and that the MLS has an FNAME:

```
btsadmin> show ivr_script_profile
FNAME=MLS
IVR_ACCESS_MODE=IVR
IVR_ROUTE_GUIDE_ID=10013
IVR_SCRIPT_PKG_TYPE=BAU
```

Ensure that the annc-tg-profile table is correct:

```
ANNC_LANG_FORMAT_SUPPORTED=N for IPUnity
ANNC_LANG_FORMAT_SUPPORTED=Y for Cognitronics
```

Turn on trace in the Cisco BTS 10200 Call Agent (CA) for MLS, set MGCP on the CA to info5 level, and examine the BAU code from the MS:

```
TC_11.3.1_CA.log:..            MGA    00-00.           |<<<< RECV FROM: 10.1.31.2
FROM-PORT=2427 TO-PORT=2727 <<<<|
TC_11.3.1_CA.log-..            MGA    00-00.           |ntfy 717
annc/1@sj-ms1-s4.sjc-devtest.com MGCP 1.0 NCS 1.0^M|
TC_11.3.1_CA.log-..            MGA    00-00.           |X: 2B00000007^M|
TC_11.3.1_CA.log-..            MGA    00-00.           |O: A/of(rc=601)^M|
TC_11.3.1_CA.log-..            MGA    00-00.           ||snd_rcv.c:260
```

Error: Need

Explanation: The mls-annc-mult-factor token value is lower than the number of announcements existing on the MS.

Recommended Action: Provision the mls-annc-mult-factor token value greater than the number of announcements on the MS.

Error: Return Code 601: File not found

Explanation: MSs are limited to 40-character filenames. These 40 characters include the extension (typically a wav) and the announcement-file-prefix: for example fra_, eng_ and spa_.

Recommended Action: Change the filename length to less than 40 characters.

Viewing Trace Logs for Throttled Flood of MGCP Messages From Specific Endpoint

The Cisco BTS 10200 can detect an incoming flood of messages from an individual MGCP-based MGW or endpoint. When such a flood occurs, the Cisco BTS 10200 automatically throttles messages coming from that specific resource. If the flood condition stops, the system releases the throttle. The system also deletes wild-carded messages (for example, RSIP <tid> *@mgw.net) received from any MGW. This detection and throttling mechanism is not customer configurable.

The system displays one of the following traces in logs at the INFO3 level:

- Message dumped for termIdx=<term id> due to high incoming message rate.
- Message dumped for mgIdx=<mg id> due to high incoming message rate.

Note Log info levels are listed in the "Logs" section on page C-15 in Appendix C, "Overload Control."

Platform Core File Alarm

The Cisco BTS 10200 core file monitor feature provides Cisco BTS 10200 customers with an alarm notification whenever a core file is generated on a Cisco BTS 10200 platform system. The Cisco BTS 10200 core file monitor feature also removes core files automatically when disk space is critically low or when the core file has aged beyond a maximum allowable time.

Core files are generated and stored in the bin directory for the binary executable which generated the core. The normal procedure to be followed by the operator is to move the core files as they are generated to another storage area. The monitoring of core files with alarm notification will remind the system operator to perform this process.

The Cisco BTS 10200 core file monitor enhancement is driven by the problem that core files are huge (2–4 GB) and eventually cause a disk full condition resulting in a switchover. In the field, operators rely on a process crash alarm to alert them that a core file is present. The core file monitor alarm provides an additional periodic reminder that operator action must be taken to move core files from the system.

Note See the *Cisco BTS 10200 Softswitch Network and Subscriber Feature Descriptions* guide for a complete list of subscriber features supported by the Cisco BTS 10200.

Planning

This section provides information on prerequisites and limitations applicable to the Cisco BTS 10200 core file monitor feature:

- Prerequisites—Tasks or conditions (outside the immediate scope of this document) that are required before these new Cisco BTS 10200 features can work as specified
- Restrictions and limitations for this feature—Special conditions or scenarios for which these features might not work, or might behave in an unexpected manner

Prerequisites

The Cisco BTS 10200 must be upgraded to Release 5.0 and above for the Cisco BTS 10200 core file monitor feature to be active.

Restrictions and Limitations

The Cisco BTS 10200 must be upgraded to Release 5.0 and above for the Cisco BTS 10200 core file monitor feature to be active.

Configuring

The configuration of the Cisco BTS 10200 core file monitor feature is dependent upon the settings in the cfm.cfg file. Table 14-2 lists the parameters and conditions within the cfm.cfg file for configuring the Cisco BTS 10200 core file monitor feature.

Table 14-2 Core File Monitor Configuration File Parameters and Conditions

Parameter	Condition
CORE_FILE_MONITOR_DISABLE	If set to true, the core file monitor audit is not performed. Default setting is false.
CORE_FILE_ALARM_ENABLE	If set to false, the core file monitor alarm is not issued when a core file is found in the network element bin directory. Default setting is true.
CORE_FILE_MINIMUM_SPACE	This is the minimum free file space in megabytes which will trigger the automatic deletion of the oldest core files. Default is 5 GB.
CORE_FILE_AGE_TO_DELETE	This is the maximum time in hours that a core file can exist before it is automatically deleted. Default is 72 hours.
CORE_FILE_AGE_DELETE_ENABLE	If set to true, core files are deleted automatically when their maximum age is reached. Default is true.
CORE_FILE_SPACE_DELETE_ENABLE	If set to true, the oldest core files are deleted when free file space is low. Default is true.

For details on troubleshooting the “Core File Present” condition, refer to Core File Present—Audit (25), page 2-20.