CHAPTER 3

Monitoring and Backing Up the BTS

Revised: February 18, 2010, OL-16000-07

Introduction

This chapter includes overall BTS maintenance strategies.

Detecting and Preventing BTS Congestion

When congested the BTS automatically does the following:

- Detects internal messaging congestion caused by traffic overload or other extraordinary events.
- Takes preventive action to avoid system failure (including shedding of traffic).
- Generates alarms when it detects internal messaging.
- Clears the alarms when congestion abates.
- Places the access control list (ACL) parameter (indicating congestion) into release messages sent to the SS7 network when the BTS internal call processing engine is congested.
- Routes emergency messages. Exact digit strings for emergency calls differ, specify up to ten digit strings (911 and 9911 are included by default). Contact Cisco TAC to do this, it involves a CA restart.
- Generates a SS7 termination cause code 42 for billing.
- Generates the cable signaling stop event with cause code “resource unavailable” for billing.

See the *Cisco BTS 10200 Softswitch Troubleshooting Guide, Release 6.0.1* for congestion alarms.

Monitoring BTS Hardware

BTS tracks devices and facilities that exceed their settings.

- A process exceeds 70 percent of the CPU.
- The Call Agent CPU is over 90 percent busy (10 percent idle).
- The load average exceeds 5 for at least a 5-minute interval.
- Memory is 95 percent exhausted and swap is over 50 percent consumed.

- Partitions consumed:
  - A partition 70 percent consumed generates a minor alarm.
  - A partition 80 percent consumed generates a major alarm.
  - A partition 90 percent consumed generates a critical alarm.

Table 3-1 Managing Hardware

Task	Sample Command
Running node reports	`report node node=prica42;` **Note** Results may take a few minutes to display.
Viewing nodes	`status node node=prica42;`
Rebooting the host machines	`control node node=prica42; action=REBOOT;` ⚠ **Caution** Use this command with extreme caution.
Setting the host machine for maintenance	`control node node=prica42; action=HALT;` ⚠ **Caution** Use local consoleaccess or a power cycle to restart the node.

Checking BTS System Health

Do the following tasks as listed or more frequently if your system administrator recommends it.

Table 3-2 BTS System Health Checklist

Tasks		Frequency
☐	Moving Core Files	as alarms are receieved
☐	Using BTS System-Health Reports	Daily
☐	Checking BTS System Time	Daily
☐	Checking Traffic Measurements See Chapter 6, "Using Measurements."	Daily
☐	Checking Event and Alarm Reports See *Cisco BTS 10200 Softswitch Troubleshooting Guide, Release 6.0.1*.	Daily
☐	Checking the OS Log of Each Host Machine	Daily
☐	Backing up the EMS Database	Daily
☐	Checking Disk Mirroring on Each Host Machine	Weekly

Table 3-2 BTS System Health Checklist (continued)

☐	Auditing Databases and Tables	Monthly
☐	Cleaning Filters See equipment manufacturer's documentation.	Monthly
☐	Archiving Your Database	See your system administrator
☐	Backing Up the Software Image	Monthly
☐	Examining Heap Usage	Quarterly
☐	Running Diagnostic Procedures on Trunk Groups See Chapter 5, "Managing External Resources"	Quarterly
☐	Running Diagnostic Procedures on Subscriber Terminations See Chapter 5, "Managing External Resources"	Quarterly
☐	Running Network Loopback Tests for NCS/MGCP Endpoints See equipment manufacturer's documentation.	Quarterly
☐	Creating Numbering Resource Utilization/Forecast (NRUF) Reports	Biannually

Using BTS System-Health Reports

The BTS allows you to gather data and create a report on its overall state. Use this data to find problems like hardware failures or traffic congestion.

Table 3-3 Using BTS System-Health Reports

Task	Sample Command
Viewing scheduled reports	`show scheduled-command verb=report; noun=system_health`
Viewing reports by ID number	`show scheduled-command ID=1`
Scheduling reports	`add scheduled-command verb=report; noun=system_health; start-time=2003-10-01 12:22:22; recurrence=DAILY; keys=period; key-values=<1 ... 720>;` where: **`start-time`**—When BTS creates report, yyyy-mm-dd hh:mm:ssss. **`recurrence`**—How often to run report (**`none`** (only once), **`daily`**, **`weekly`**, **`monthly`** **`keys=period; key-values=<1 ... 720>;`**—How many hours back to collect data. If not specified, BTS uses default of 24 (last 24 hours worth of data).
Changing reports	`change scheduled-command id=881958666704177006; start-time=2003-10-01 14:14:14; recurrence=DAILY; keys=period; key-values=24;`

Table 3-3 Using BTS System-Health Reports (continued)

Task	Sample Command
Deleting reports	`delete scheduled-command id=881958666704177006;`
Viewing completed reports	In a web browser enter `https://<active EMS IP addr or FQDN>:/report/system_health`
Generating a report immediately	`report system-health period=<1 ... 720>;` **Note** Results may take a few minutes to display.

Checking BTS System Time

BTS clocks must be accurate to 2 seconds.

Caution Do not change the date or time in your BTS host machines while CA, FS, EMS, and BDMS are running. Instead allow the Solaris OS to get the time automatically through NTP services.

Step 1 Log in to the primary and secondary EMSs as `root`.

Step 2 Enter `<hostname># date`.

Step 3 On each EMS ensure the following are correct:

a. The time does not deviate more than +/- 2 seconds.

b. Day, month, year, time zone

Step 4 Log in to both the primary and secondary CA as `root`.

Step 5 Enter `<hostname># date`.

Step 6 On each CA ensure the following are correct:

a. The time is accurate to within +/-2 seconds of the correct time.

b. Day, month, year, time zone

Checking the OS Log of Each Host Machine

Monitor the OS logs on all four host machines (primary and secondary EMS, primary and secondary CA) for errors or warnings. This report shows you recent messages like memory hits, disk errors, and frequent process restarts.

Step 1 Log in as `root`.

Step 2 Enter `dmesg`.

Step 3 For more history edit the /var/adm/messages file.

Checking Disk Mirroring on Each Host Machine

Each procedure takes about 30 minutes.

CA/FS Side A

Before doing this procedure, ensure your BTS platform is connected to controller 1 or controller 0.

Step 1 Log in as **root** to CA/FS side A using telnet.

Step 2 Enter one of the following:

```
<hostname># metastat | grep c0
```

Or:

```
<hostname># metastat | grep c1
```

Step 3 Verify the return matches the following:

```
c1t0d0s1          0     No            Okay   Yes
c1t1d0s1          0     No            Okay   Yes
c1t0d0s5          0     No            Okay   Yes
c1t1d0s5          0     No            Okay   Yes
c1t0d0s6          0     No            Okay   Yes
c1t1d0s6          0     No            Okay   Yes
c1t0d0s0          0     No            Okay   Yes
c1t1d0s0          0     No            Okay   Yes
c1t0d0s3          0     No            Okay   Yes
c1t1d0s3          0     No            Okay   Yes
c1t1d0   Yes    id1,sd@SSEAGATE_ST373307LSUN72G_3HZ9JG7800007518H8WV
c1t0d0   Yes    id1,sd@SSEAGATE_ST373307LSUN72G_3HZ9JC9N00007518Y15K
```

If the results differ synchronize the disk mirroring:

```
<hostname># cd /opt/setup
<hostname># sync_mirror
```

Verify the results using Step 1 through Step 3.

Caution In case of a mismatch, synchronize once. If the mismatch continues, contact Cisco TAC.

CA/FS Side B

Step 1 Log in as **root** to CA/FS side B using telnet.

Step 2 Enter **<hostname># metastat | grep c0**.

Step 3 Verify the return matches the following:

```
c0t0d0s6 0 No Okay
c0t1d0s6 0 No Okay
c0t0d0s1 0 No Okay
c0t1d0s1 0 No Okay
c0t0d0s5 0 No Okay
c0t1d0s5 0 No Okay
```

```
c0t0d0s7 0 No Okay
c0t1d0s7 0 No Okay
c0t0d0s0 0 No Okay
c0t1d0s0 0 No Okay
c0t0d0s3 0 No Okay
c0t1d0s3 0 No Okay
```

If the results differ synchronize the disk mirroring:

```
<hostname># cd /opt/setup
<hostname># sync_mirror
```

Verify the results using Step 1 through Step 3.

Caution In case of a mismatch, synchronize once. If the mismatch continues contact Cisco TAC.

EMS Side A

Step 1 Log in as **root** to EMS side A using telnet.

Step 2 Enter **<hostname># metastat | grep c0**.

Step 3 Verify the return matches the following:

```
c0t0d0s6 0 No Okay
c0t1d0s6 0 No Okay
c0t0d0s1 0 No Okay
c0t1d0s1 0 No Okay
c0t0d0s5 0 No Okay
c0t1d0s5 0 No Okay
c0t0d0s7 0 No Okay
c0t1d0s7 0 No Okay
c0t0d0s0 0 No Okay
c0t1d0s0 0 No Okay
c0t0d0s3 0 No Okay
c0t1d0s3 0 No Okay
```

If the results differ synchronize the disk mirroring:

```
<hostname># cd /opt/setup
<hostname># sync_mirror
```

Verify the results using Step 1 through Step 3.

Caution In case of a mismatch, synchronize once. If the mismatch continues contact Cisco TAC.

EMS Side B

Step 1 Log in as **root** to EMS side B using telnet.

Step 2 Enter **<hostname># metastat | grep c0.**

Step 3 Verify the return result matches the following:

```
c0t0d0s6 0 No Okay
c0t1d0s6 0 No Okay
c0t0d0s1 0 No Okay
c0t1d0s1 0 No Okay
c0t0d0s5 0 No Okay
c0t1d0s5 0 No Okay
c0t0d0s7 0 No Okay
c0t1d0s7 0 No Okay
c0t0d0s0 0 No Okay
c0t1d0s0 0 No Okay
c0t0d0s3 0 No Okay
c0t1d0s3 0 No Okay
```

If the results differ synchronize the disk mirroring:

```
<hostname># cd /opt/setup
<hostname># sync_mirror
```

Verify the results using Step 1 through Step 3.

Caution In case of a mismatch, synchronize once. If the mismatch continues contact Cisco TAC.

Auditing Databases and Tables

Audit either the complete database or entries in every provisionable table in both the Oracle database and shared memory. See the *Cisco BTS 10200 Softswitch Troubleshooting Guide, Release 6.0.1*.

Caution Audits are time-intensive. Do only during a maintenance window. Completion time varies with database or table entries.

Table 3-4 Auditing Databases and Tables

Task	Sample Command
Auditing individual tables	**audit trunk type=row-count;**
Auditing every entry in each provisionable table	**audit database;**
Auditing provisionable tables based on **type**	**audit database type=row-count;** **Note** **type** defaults to **full**
Auditing provisionable tables based on **platform state**	**audit database platform-state=active;** **Note** **platform-state** defaults to **active**

Table 3-4 Auditing Databases and Tables (continued)

Task	Sample Command
Auditing mismatches across network elements	1. Log in as **root**. 2. Enter: **bts_audit -ems priems01 -ca prica01 -platforms CA146,FSAIN205 -tables SUBSCRIBER,MGW_PROFILE** **Note** bts_audit cannot work in certain scenarios, for example, when a termination record points to an invalid mgw
Resolving mismatches across network elements	If a table references a missing row, the mismatch is not resolved. Only synchronize data mismatches between active network elemens. 1. Audit mismatches using **bts_audit**. 2. Enter: **bts_sync /opt/ems/report/Audit_CA146_root.sql** **bts_sync applies updates directly to the databases.**

Exporting Provisioned Data

The CLI Native Data Export feature enables the export of all provisioning data from the BTS 10200 system by the use of a CLI command. Execution of the CLI command stores the exported data in a user-named output file in text format in the export directory. The exported file contains all provisioning data from the BTS 10200. The provisioning data is written into the export file using **add** and **change** commands for all supported nouns.

The key attributes of the CLI Native Data Export feature are

- The user can run the CLI command to export the BTS 10200 provisioning data.
- The provisioning data for all the nouns, which enables the use of verbs as “add” and “change” is exported in text format.
- The list of all the nouns related to provisioning is kept in an input file (xml format). Upon execution of the **export** command, the xml input file reads the nouns and their corresponding verbs (operation type, whether add or change), and exports the provisioning data from the BTS 10200.

The CLI export command is:

```
CLI > export database outfile = <whatever>
```

Where the noun is database and the verb is export. Execution of the command exports all of the provisioning data from the BTS 10200. All of the exported data is written in the output file as specified by the user. The output file contains all the **add** and **change** commands for the existing native data in the BTS 10200. The exported output file is stored in the /opt/ems/export directory.

The result of the **export** command is a text file that contains add/change CLI commands. The following is an example output text file:

```
# BTS Config Export
# EMS Server: priems26-ora
# User: optiuser
# Export Start Time : Tue Jan 22 17:23:54 CST 2008

#########################
##### Add clli_code #####
```

```
##########################
add clli_code ID=ABCD1234567;


############################
##### Add call_agent #####
############################
add call_agent id=CA146;tsap_addr=CA146.A.12345678901234567890123456789012345678
901234567890123456;mgw_monitoring_enabled=N;clli=ABCD1234567;

##############################
##### Add feature_server #####
##############################
add feature_server ID=FSAIN205;TSAP_ADDR=FSAIN.A.12345678901234567890123456789012
345678901234567890123456;TYPE=AIN;DESCRIPTION=12345678901234567890123456789012345
4567890123456789012345678904BCD;EXTERNAL_FEATURE_SERVER=N;
add feature_server ID=FSPTC235;TSAP_ADDR=FSPTC.A.12345678901234567890123456789012
345678901234567890123456;TYPE=POTS;DESCRIPTION=12345678901234567890123456789012345
6789012345678901234567890ABCD;EXTERNAL_FEATURE_SERVER=N;

####################################
##### Change billing_acct_addr #####
####################################

################################
##### Change billing_alarm #####
################################

####################################
##### Change report_properties #####
####################################
change report_properties TYPE=EVENT_LOGSIZE;VALUE=30000;
change report_properties TYPE=ALARM_LOGSIZE;VALUE=30000;
change report_properties TYPE=EVENT_LEVEL;VALUE=INFO;

############################
##### Change sup_config #####
############################
change sup_config TYPE=refresh_rate;VALUE=86400;
change sup_config TYPE=priority;VALUE=5;
change sup_config TYPE=subterm_mgw_block;VALUE=5;
change sup_config TYPE=subterm_block_pause;VALUE=9000;
change sup_config TYPE=subterm_status_pause;VALUE=0;
change sup_config TYPE=trunkterm_tg_block;VALUE=5;
change sup_config TYPE=trunkterm_block_pause;VALUE=9000;
change sup_config TYPE=trunkterm_status_pause;VALUE=0;
change sup_config TYPE=trunkterm_range_block;VALUE=1000;
change sup_config TYPE=trunkterm_range_pause;VALUE=20000;
```

```
##############################################
##### Change command_throttle_threshold #####
##############################################
change command_throttle_threshold SESSION_TYPE=CLI;THRESHOLD=100;ENABLE=Y;
change command_throttle_threshold SESSION_TYPE=CORBA;THRESHOLD=100;ENABLE=Y;
change command_throttle_threshold SESSION_TYPE=FTP;THRESHOLD=1000;ENABLE=Y;
change command_throttle_threshold SESSION_TYPE=MNT;THRESHOLD=100;ENABLE=Y;
change command_throttle_threshold SESSION_TYPE=SNMP;THRESHOLD=100;ENABLE=Y;
change command_throttle_threshold SESSION_TYPE=SOAP;THRESHOLD=100;ENABLE=Y;

##################################
##### Change config_interval #####
##################################
change config_interval CONFIG_TYPE=THROTTLE;INTERVAL=15;

# Export End Time : Tue Jan 22 17:24:14 CST 2008
```

Limitations

Currently the **export** command is supported only from the CLI interface. The **export** command is currently not supported from other interfaces such as CORBA and SOAP.

There is a limitation on the size of the /opt/ems/export directory. Currently the size of the export directory is defined in /opt/ems/etc/bts.properties as 7500000 ~ 700 MB. During the first run of the **export** command, if the size of the export file is beyond the threshold limit, a warning message is shown to the user after export is finished. The warning message indicates that the export file size has exceeded the threshold and that the user needs to clean up the export directory before running the command again. During additional runs of the **export** command, if the export directory size is more then the threshold size, a warning is shown to the user that the space of export directory is insufficient for the export and that the user has to clear the export directory before rerunning the **export** command.

Creating Numbering Resource Utilization/Forecast (NRUF) Reports

The North American Numbering Plan Association (NANPA) collects, stores, and maintains how telephone numbers are used by 19 countries. Companies, like carriers, that hold telephone numbers must report to NANPA twice a year using the NRUF report. Go to http://www.nanpa.com for more information and job aids on submitting reports.

The BTS creates an NRUF report using the Number Block table. This table:

- Is a single table that is the sole reference for NANPA audits
- Can be customized
- Can be updated from data imported from other tables, changes from office-code updates, or manually
- Has the following fields:
  - Number Block: NPA to NPA-NXX-XXXX—For FCC-required NANPA audit compliance, the report input is NPANXX. In markets outside of NANPA, the input can be based on either the combination of the national destination code (NDC) and the exchange code (EC), or just the EC.
  - Code Holder = Y/N
  - Block Holder = Y/N
  - Native = Y/N

  - Non-Native = Y/N

To generate the following reports, use **`report dn-summary`**:

- All DNs in NDC and EC
- Thousands group in NDC and EC
- Operating company number (OCN)
- Switch Common Language Location Identifier (CLLI) code
- OCN + CLLI code—entries must match LERG data

Creating Reports for Nonrural Primary and Intermediate Carriers

NRUF reporting for nonrural primary and intermediate carriers:

- Occurs at a thousands-block level (NPA-NXX-X)
- Applies only to NANP

The report returns the following based on the DN2SUBSCRIBER table's STATUS token:

Table 3-5 NRUF Report Data for Nonrural Carriers

Data Groups	Matching Data from the DN2SUBSCRIBER Table
Assigned DNs	• Individual DNs: **ndc=<npa>; ec=<nxx>; DN=[0-9][0-9][0-9]; (status=assigned) AND ADMIN-DN=N** **ndc=<npa>; ec=<nxx>; DN=[0-9][0-9][0-9]; (status=ported-out) AND ADMIN-DN=N** • DID DNs: **ndc=<npa>; ec=<nxx>; DN=xxxx; (status=assigned) AND ADMIN-DN=N; X 10000** **ndc=<npa>; ec=<nxx>; DN=xxxx; (status=ported-out) AND ADMIN-DN=N; X 10000** **ndc=<npa>; ec=<nxx>; DN=[0-9]xxx; (status=assigned) AND ADMIN-DN=N; X 1000** **ndc=<npa>; ec=<nxx>; DN=[0-9]xxx; (status=ported-out) AND ADMIN-DN=N; X 1000** **ndc=<npa>; ec=<nxx>; DN=[0-9][0-9]xx; (status=assigned) AND ADMIN-DN=N; X 100** **ndc=<npa>; ec=<nxx>; DN=[0-9][0-9]xx; (status=ported-out) AND ADMIN-DN=N; X 100** **ndc=<npa>; ec=<nxx>; DN=[0-9][0-9][0-9]x; (status=assigned) AND ADMIN-DN=N; X 10** **ndc=<npa>; ec=<nxx>; DN=[0-9][0-9][0-9]x; (status=ported-out) AND ADMIN-DN=N; X 10** • PORTED-OUT DNs
Intermediate Telephone Directory Numbers	0
Reserved DNs	0

Table 3-5 NRUF Report Data for Nonrural Carriers (continued)

Data Groups	Matching Data from the DN2SUBSCRIBER Table

Aging DNs	• DISC DNs:
	`ndc=<npa>; ec=<nxx>; DN=[0-9][0-9][0-9][0-9]; (status=DISC)`
	• Changed Number DNs:
	`ndc=<npa>; ec=<nxx>; DN=[0-9][0-9][0-9][0-9]; (status=CN)`
	• DISC DID DNs:
	`ndc=<npa>; ec=<nxx>; DN=xxxx; (status=DISC) X 10000`
	`ndc=<npa>; ec=<nxx>; DN=[0-9]xxx; (status=DISC) X 1000`
	`ndc=<npa>; ec=<nxx>; DN=[0-9][0-9]xx; (status=DISC) X 100`
	`ndc=<npa>; ec=<nxx>; DN=[0-9][0-9][0-9]x; (status=DISC) X 10`
	• Changed Number DID DNs:
	`ndc=<npa>; ec=<nxx>; DN=xxxx; (status=CN) X 10000`
	`ndc=<npa>; ec=<nxx>; DN=[0-9]xxx; (status=CN) X 1000`
	`ndc=<npa>; ec=<nxx>; DN=[0-9][0-9]xx; (status=CN) X 100`
	`ndc=<npa>; ec=<nxx>; DN=[0-9][0-9][0-9]x; (status=CN) X 10`

Administrative DNs	• Administrative DNs:
	`ndc=<npa>; ec=<nxx>; status=LRN;`
	`ndc=<npa>; ec=<nxx>; status=CLRN`
	`ndc=<npa>; ec=<nxx>; status=RACF-DN;`
	`ndc=<npa>; ec=<nxx>; status=ANNC;`
	`ndc=<npa>; ec=<nxx>; status=TEST-LINE;`
	`ndc=<npa>; ec=<nxx>; (ADMIN-DN=Y AND (status=ASSIGNED))`
	`ndc=<npa>; ec=<nxx>; (ADMIN-DN=Y AND (status=PORTED-OUT))`
	• Administrative DID DNs:
	`ndc=<npa>; ec=<nxx>; DN=xxxx; (ADMIN-DN=Y AND (status=ASSIGNED)) X 10000`
	`ndc=<npa>; ec=<nxx>; DN=xxxx; (ADMIN-DN=Y AND (status=PORTED-OUT)) X 10000`
	`ndc=<npa>; ec=<nxx>; DN=[0-9]xxx (ADMIN-DN=Y AND (status=ASSIGNED)) X 1000`
	`ndc=<npa>; ec=<nxx>; DN=[0-9]xxx (ADMIN-DN=Y AND (status=PORTED-OUT)) X 1000`
	`ndc=<npa>; ec=<nxx>; DN=[0-9][0-9]xx; (ADMIN-DN=Y AND (status=ASSIGNED)) X 100`
	`ndc=<npa>; ec=<nxx>; DN=[0-9][0-9]xx; (ADMIN-DN=Y AND (status=PORTED-OUT)) X 100`
	`ndc=<npa>; ec=<nxx>; DN=[0-9][0-9][0-9]x; (ADMIN-DN=Y AND (status=ASSIGNED)) X 10`
	`ndc=<npa>; ec=<nxx>; DN=[0-9][0-9][0-9]x; (ADMIN-DN=Y AND (status=PORTED-OUT)) X 10`
	• Changed Number administrative DNs

Creating Reports for Rural Primary and Intermediate Carriers

This section identifies the DN information that is reported at the NPA-NXX level when the service provider is a code holder. NRUF reporting at the “ndc, ec” level includes dn-groups of varying length. Some countries might support dn-groups of length 1, 2, 3 or 4.

- The Rural Primary Carrier (U2 form) NPA-NXX report has:
  - NPA-NXX (input as ndc, ec)
  - Rate Center (read from LERG)
  - State (read from LERG)
  - Number of Assigned DNs
  - Number of Intermediate DNs
  - Number of Reserved DNs
  - Number of Aging DNs
  - Number of Administrative DNs
  - Donated to Pool (always 0)

- The Rural Intermediate Carrier (U4 form) report has:
  - NPA-NXX (input as ndc, ec)
  - Rate Center (read from LERG)
  - State (read from LERG)
  - Number of Assigned DNs
  - Number of Intermediate DNs
  - Number of Reserved DNs
  - Number of Aging DNs
  - Number of Administrative DNs
  - Numbers Received (always 0)

The report returns the following based on the DN2SUBSCRIBER table's STATUS token:

Table 3-6 NRUF Report Data for Rural Carriers

Data Groups	Matching Data from the DN2SUBSCRIBER Table
Assigned DNs	• Individual DNs: **ndc=<npa>; ec=<nxx>; DN=[0-9][0-9][0-9]; (status=assigned) AND ADMIN-DN=N** **ndc=<npa>; ec=<nxx>; DN=[0-9][0-9][0-9]; (status=ported-out) AND ADMIN-DN=N** • DID DNs: **ndc=<npa>; ec=<nxx>; DN=xxxx; (status=assigned) AND ADMIN-DN=N; X 10000** **ndc=<npa>; ec=<nxx>; DN=xxxx; (status=ported-out) AND ADMIN-DN=N; X 10000** **ndc=<npa>; ec=<nxx>; DN=[0-9]xxx; (status=assigned) AND ADMIN-DN=N; X 1000** **ndc=<npa>; ec=<nxx>; DN=[0-9]xxx; (status=ported-out) AND ADMIN-DN=N; X 1000** **ndc=<npa>; ec=<nxx>; DN=[0-9][0-9]xx; (status=assigned) AND ADMIN-DN=N; X 100** **ndc=<npa>; ec=<nxx>; DN=[0-9][0-9]xx; (status=ported-out) AND ADMIN-DN=N; X 100** **ndc=<npa>; ec=<nxx>; DN=[0-9][0-9][0-9]x; (status=assigned) AND ADMIN-DN=N; X 10** **ndc=<npa>; ec=<nxx>; DN=[0-9][0-9][0-9]x; (status=ported-out) AND ADMIN-DN=N; X 10**
Intermediate Telephone Directory Numbers	0
Reserved DNs	0

Table 3-6 NRUF Report Data for Rural Carriers (continued)

Data Groups	Matching Data from the DN2SUBSCRIBER Table

Aging DNs	• DISC DNs:
	`ndc=<npa>; ec=<nxx>; DN=[0-9][0-9][0-9][0-9]; (status=DISC)`
	• Changed Number DNs:
	`ndc=<npa>; ec=<nxx>; DN=[0-9][0-9][0-9][0-9]; (status=CN)`
	• DISC DID DNs:
	`ndc=<npa>; ec=<nxx>; DN=xxxx; (status=DISC) X 10000`
	`ndc=<npa>; ec=<nxx>; DN=[0-9]xxx; (status=DISC) X 1000`
	`ndc=<npa>; ec=<nxx>; DN=[0-9][0-9]xx; (status=DISC) X 100`
	`ndc=<npa>; ec=<nxx>; DN=[0-9][0-9][0-9]x; (status=DISC) X 10`
	• Changed Number DID DNs:
	`ndc=<npa>; ec=<nxx>; DN=xxxx; (status=CN) X 10000`
	`ndc=<npa>; ec=<nxx>; DN=[0-9]xxx; (status=CN) X 1000`
	`ndc=<npa>; ec=<nxx>; DN=[0-9][0-9]xx; (status=CN) X 100`
	`ndc=<npa>; ec=<nxx>; DN=[0-9][0-9][0-9]x; (status=CN) X 10`

Administrative DNs	• Administrative DNs:
	`ndc=<npa>; ec=<nxx>; status=LRN;`
	`ndc=<npa>; ec=<nxx>; status=CLRN`
	`ndc=<npa>; ec=<nxx>; status=RACF-DN;`
	`ndc=<npa>; ec=<nxx>; status=ANNC;`
	`ndc=<npa>; ec=<nxx>; status=TEST-LINE;`
	`ndc=<npa>; ec=<nxx>; (ADMIN-DN=Y AND (status=ASSIGNED))`
	`ndc=<npa>; ec=<nxx>; (ADMIN-DN=Y AND (status=PORTED-OUT))`
	• Administrative DID DNs:
	`ndc=<npa>; ec=<nxx>; DN=xxxx; (ADMIN-DN=Y AND (status=ASSIGNED)) X 10000`
	`ndc=<npa>; ec=<nxx>; DN=xxxx; (ADMIN-DN=Y AND (status=PORTED-OUT)) X 10000`
	`ndc=<npa>; ec=<nxx>; DN=[0-9]xxx (ADMIN-DN=Y AND (status=ASSIGNED)) X 1000`
	`ndc=<npa>; ec=<nxx>; DN=[0-9]xxx (ADMIN-DN=Y AND (status=PORTED-OUT)) X 1000`
	`ndc=<npa>; ec=<nxx>; DN=[0-9][0-9]xx; (ADMIN-DN=Y AND (status=ASSIGNED)) X 100`
	`ndc=<npa>; ec=<nxx>; DN=[0-9][0-9]xx; (ADMIN-DN=Y AND (status=PORTED-OUT)) X 100`
	`ndc=<npa>; ec=<nxx>; DN=[0-9][0-9][0-9]x; (ADMIN-DN=Y AND (status=ASSIGNED)) X 10`
	`ndc=<npa>; ec=<nxx>; DN=[0-9][0-9][0-9]x; (ADMIN-DN=Y AND (status=PORTED-OUT)) X 10`

Backing Up the Software Image

To back up the software image do the following three procedures:

1. Full Database Auditing, page 3-16
2. Checking Shared Memory, page 3-16
3. Backing Up the Full BTS, page 3-18

Full Database Auditing

Step 1 Log in as CLI user on EMS side A.

Step 2 Enter **audit database type=full;**.

Step 3 Check the audit report and verify that there is no mismatch or error. If errors are found, try to correct the errors. If you cannot make the correction, contact Cisco TAC.

Checking Shared Memory

This task checks shared memory to detect potential data problems.

From CA/FS Side A

Step 1 Log in as **root**.

Step 2 Enter:

```
<hostname># cd /opt/OptiCall/CAxxx/bin
<hostname># ca_tiat data
```

Press **Enter**.

The result should match the following:

```
All tables are OK.
For details, see ca_tiat.out
```

Caution If the result is not"All tables are OK", stop and contact Cisco TAC. If the result is "All tables are OK", go to Step 3.

Step 3 Enter:

```
<hostname># cd /opt/OptiCall/FSPTCzzz/bin <Return>
<hostname># potsctx_tiat data <Return>
```

Press **Enter**.

The result should match the following:

```
All tables are OK.
For detail, see potsctx_tiat.out
```

Caution If the result is not"All tables are OK", stop and contact Cisco TAC. If the result is "All tables are OK", go to Step 4.

Step 4 Enter:

```
<hostname>#cd /opt/OptiCall/FSAINyyy/bin
<hostname>#ain_tiat data
```

Step 5 Press **Enter**.

The result should match the following:

```
All tables are OK.
For detail, see ain_tiat.out
```

Caution If the result is not"All tables are OK", stop and contact Cisco TAC.

From CA/FS Side B

Step 1 Log in as **root**.

Step 2 Enter:

```
<hostname>#cd /opt/OptiCall/CAxxx/bin
<hostname>#ca_tiat data
```

Step 3 Press **Enter**.

The result should match the following:

```
All tables are OK.
For detail, see ca_tiat.out
```

Caution If the result is not"All tables are OK", stop and contact Cisco TAC. If the result is "All tables are OK", go to Step 3.

Step 4 Enter:

```
<hostname>#cd /opt/OptiCall/FSPTCzzz/bin
<hostname>#potsctx_tiat data
```

Step 5 Press **Enter**:

The result match the following:

```
All tables are OK.
For detail, see potsctx_tiat.out
```

Caution If the result is not"All tables are OK", stop and contact Cisco TAC. If the result is "All tables are OK", go to Step 6.

Step 6 Enter:

```
<hostname>#cd /opt/OptiCall/FSAINyyy/bin
<hostname>#ain_tiat data
```

Step 7 Press **Enter**:

The result should match the following:

```
All tables are OK.
For detail, see ain_tiat.out
```

Caution If the result is not"All tables are OK", stop and contact Cisco TAC.

Backing Up the Full BTS

Do this before and after software upgrades or as routine, always during a maintenance window. Before starting the provisioning process ensure you have the following:

Pre-Provisioning Checklist	
☐	NFS server hostname or ip address
☐	Shared directory from NFS server
☐	Root user access
☐	Provisioning blocked

Backing Up the CA/FS

Perform the following steps to back up the secondary CA/FS. Then repeat the procedure on the primary CA/FS.

Step 1 Log in as **root** on the secondary CA/FS.

Step 2 Verify all platforms are in STANDBY mode, enter **<hostname>#nodestat**.

Step 3 Remove unnecessary files or directories like /opt/Build and application tar files.

Step 4 Mount the NFS server to the **/mnt** directory, enter **<hostname>#mount <nfs server ip or hostname>:/<share dire> /mnt**.

Step 5 Stop all platforms; enter **<hostname>#platform stop all**.

Step 6 Save all platforms data directory (shared memory) to nfs server

```
<hostname>#tar -cf - /opt/OptiCall/CAxxx/bin/data |gzip -fast - > /mnt/data.<hostname>.CA
<<hostname>#tar -cf - /opt/OptiCall/CAxxx/bin/data |gzip --fast - >
/mnt/data.<hostname>.CA.gz
<hostname>#tar -cf - /opt/OptiCall/FSAINxxx/bin/data |gzip --fast - >
/mnt/data.<hostname>.FSAIN.gz
<hostname>#tar -cf /opt/OptiCall/FSPTCxxx/bin/data |gzip --fast - >
/mnt/data.<hostname>.FSPTC.gz
```

where xxx is the instance number

Step 7 Start all platforms by entering **<hostname>#platform start**.

Step 8 Verify all platforms are in STANDBY mode, enter **<hostname>#nodestat**.

Step 9 Create an excluded directories file for the flash archive, enter:

```
<hostname>#vi /tmp/excluded_dir
/opt/OptiCall/CAxxx/bin/data
/opt/OptiCall/CAxxx/bin/logs
```

```
/opt/OptiCall/FSAINxxx/bin/data
/opt/OptiCall/FSAINxxx/bin/logs
/opt/OptiCall/FSPTCxxx/bin/data
/opt/OptiCall/FSPTCxxxx/bin/logs
```

where **xxx** is the instance number

Step 10 Back up the system, enter:

```
<hostname>#mv /bin/date /bin/date.archive
<hostname>#mv /bin/.date /bin/date
<hostname>#flarcreate -n <hostname> -X /tmp/excluded_dir -c /mnt/<hostname>.archive
<hostname>#mv /bin/date /bin/.date
<hostname>#mv /bin/date.archive /bin/date
```

Step 11 Unmount the NFS server, enter:

```
<hostname>#umount /mnt
```

Step 12 From the active EMS switch over all platforms, enter:

```
<hostname>#ssh optiuser@<hostname>
cli>control feature-server id=FSAINxxx;target-state=standby-active;
cli>control feature-server id=FSPTCxxx;target-state=standby-active;
cli>control call-agent id=CAxxx;target-state=standby-active;
```

where **xxx** is the instance number of each platform

Step 13 Repeat this procedure for the primary CA/FS.

Backing up the EMS/BDMS

Do the following to back up the STANDBY EMS/BDMS system.

Step 1 Log in as **root**.

Step 2 Verify all platforms are in STANDBY mode, enter **<hostname>#nodestat**.

Step 3 Remove unnecessary files or directories like /opt/Build and application tar files.

Step 4 Mount the NFS server to the **/mn**t directory, enter **<hostname>#mount <nfs server ip or hostname>:/<share dire> /mnt**.

Step 5 Stop all platforms, enter **<hostname>#platform stop all**.

Step 6 Save the Oracle database and MySQL directories, enter:

```
<hostname>#tar -cf - /data1/oradata |gzip --fast - >/mnt/oradata.<hostname>.gz
<hostname>#tar -cf - /opt/ems/db |gzip --fast - >/mnt/db.<hostname>.gz
```

Step 7 Create an excluded directories file for the flash archive, enter:

```
<hostname>#vi /tmp/excluded_dir
           /data1/oradata
```

Step 8 Start all platforms **<hostname>#platform start**.

Step 9 Verify all platforms are in STANDBY mode, enter **<hostname>#nodestat**.

Step 10 Back up the system, enter:

```
<hostname>#mv /bin/date /bin/date.archive
<hostname>#mv /bin/.date /bin/date
```

```
<hostname>#flarcreate -n <hostname> -X /tmp/excluded_dir -c /mnt/<hostname>.archive
<hostname>#mv /bin/date /bin/.date
<hostname>#mv /bin/date.archive /bin/date
```

Step 11 Unmount the NFS server, enter **<hostname>#umount /mnt**.

Step 12 From the active EMS switch over all platforms, enter:

```
<hostname>#ssh optiuser@<hostname>
cli>control bdms id=BDMS01;target-state=standby-active;
cli>control element-manager id=EM01;target-state=standby-active;
```

Step 13 Repeat the procedure starting with Step 3 to back up the PRIMARY EMS/BDMS.

Backing up the EMS Database

This procedure is for experienced UNIX users. It tells you how to save the provisioning database from the EMS to a remote server. The remote server must be:

- Connected to a corporate LAN.
- Backed up daily by default, the daily hot backup is not turned on at installation

The back up processes:

- ora_hot_backup.ks—Backs up database data files, control files, and archive logs
- ora_arch_backup.ksh—Backs up archive logs

The target backup directory on both primary and secondary EMS systems is **/opt/oraback**. Backup files in **/opt/oraback** directory are later transferred to the **/opt/backup** directory in a remote archive site. After the files are transferred, they are purged from **/opt/oraback**.

Step 1 Cross check the databases on the primary and secondary EMSs before backing up.

Caution Cross check before ora_hot_backup.ksh and ora_arch_backup.ksh are scheduled. This validates database and archived log files for RMAN processes.

a. Log in as **oracle**, or **su - oracle**.

b. Enter **dbadm -E backup_crosscheck**..

c. Ensure the log file has no errors (except the "validation failed for archived log" messages). Ignore these messages of the /data1/arch/opticalx_yyy.arc files because the validation directs RMAN not to look for *.arc files. ora_purge_archlog.ksh purges *.arc files.

```
RMAN-06157: validation failed for archived log
RMAN-08514: archivelog filename=/data1/arch/optical1_25.arc recid=1 stamp=461878656
```

Step 2 Remove the archive log purge process and schedule the backup processes.

Note Do this on the primary and secondary EMSs.

a. Disable the ora_purge_archlog.ksh process.

b. Enable the ora_hot_backup.ksh process.

c. Optional: Enable the ora_arch_backup.ksh process.

d. Log in as **oracle**, or **su - oracle**.

e. Enter **crontab -e**.

f. Modify the crontab file as follows. This is on the primary EMS site, database name *optical1*.

```
# Daily Oracle Hot backup - this also include archive log backup
#       Note: Set hot backup process to run at 2:00am every day.
#
0 2 * * * /opt/oracle/admin/scripts/ora_hot_backup.ksh optical1 > /opt/oracle/t
mp/ora_hot_backup.log 2>&1
#
# Oracle archive log backups, in addition to daily hot backup.
#       Note: Set one additional archive log backup to run at 6:00pm every day.
#
0 18 * * * /opt/oracle/admin/scripts/ora_arch_backup.ksh optical1 > /opt/
oracle/tmp/ora_arch_backup.log 2>&1
#
# Purge archive log files
#     Note: Delete or uncomment this line to stop purging archive log files.
#
#0 1,3,…,23  * * * /opt/oracle/admin/scripts/ora_purge_archlog.ksh optical1 >
/opt/oracle/tmp/ora_purge_archlog.log 2>&1
```

g. Repeat Step f by replacing *optical1* with *optical2* on the secondary EMS site.

Step 3 To setup daily file transfer to the remote archive site using FTP, see Using FTP to Setup File Transfer. To setup daily file transfer to the remote archive site using SFTP, see Using SFTP to Setup File Transfer.

Using FTP to Setup File Transfer

Step 1 Configure the remote site.

a. Verify the oracle user access and create backup directory on FTP server site.

```
Primary EMS hostname:           priems
Secondary EMS hostname:      secems
FTP server hostname:              ftpserver
FTP server Oracle password:  ora00
FTP server backup directory:    /opt/backup
```

First, test the connection to the remote FTP server using the *oracle* user access. If the password of *oracle* is not 'ora00', update the ORA_PW variable in the **/opt/oracle/admin/etc/dba.env** file.

b. Do this on the primary and secondary EMSs:

```
telnet ftpserver
```

c. Log in as **oracle** and enter the password (in this case, **ora00**).

d. Create the **/opt/backup** directory. Ensure the **oracle** user has write permission to this directory.

```
mkdir /opt/backup
```

Note It is your responsibility to archive backup files from the ftp server **/opt/backup** directory to a tape device or enterprise tape library.

Step 2 Schedule the FTP process.

a. Do this on the primary and secondary EMSs:

Log in as **oracle**, or **su - oracle** and enter the following command: **crontab -e**

b. Add the following line to the Oracle crontab on the primary EMS.

```
#
# FTP backup files from primary (optical1) to /opt/backup directory of ftpserver.
#
0 6 * * * /opt/oracle/admin/scripts/ora_ftp_backup.ksh optical1 ftpserver /opt/backup >
/opt/oracle/tmp/ora_ftp_backup.log 2>&1
```

c. Replace **ftpserver** with the correct host name of the remote FTP server. Replace /opt/backup with the correct target directory name, if they are different.

Note The **0 6 *** /opt/oracle/admin/scripts/ora_ftp_backup.ksh …… ora_ftp_backup.log 2>&1** are all typed in the same line.

d. Edit the oracle crontab on secondary EMS site by replacing *optical1* with *optical2*.

Step 3 Verify the backup files, enter:

```
cd /opt/oraback          | EMS systems
cd /opt/backup           | Remote FTP system
```

Using SFTP to Setup File Transfer

The following steps generate an SSH key from the primary EMS. Key files are copied to the secondary EMS and remote SFTP server. On the remote SFTP server the "oracle" user is created for login.

Step 1 Generate SSH secure key from primary EMS:

a. Login to the primary EMS:

```
#  su - oracle
#  /opt/BTSossh/bin/ssh-keygen -t rsa
```

b. Generating public/private rsa key pair.

c. Enter file in which to save the key (/opt/orahome/.ssh/id_rsa).

d. Enter passphrase (empty for no passphrase).

e. Enter same passphrase.
Your identification has been saved in /opt/orahome/.ssh/id_rsa.
Your public key has been saved in /opt/orahome/.ssh/id_rsa.pub.
The key fingerprint is: d8:4f:b1:8b:f4:ac:2f:78:e9:56:a4:55:56:11:e1:40 oracle@priems79

f. Enter:

```
#  ls -l /opt/orahome/.ssh
```

-rw-------1 oracleorainst1675 Mar 10 15:42 id_rsa
-rw-r--r--1 oracleorainst397 Mar 10 15:42 id_rsa.pub

Step 2 From the secondary EMS, sftp both "id_ssa" and "id_rsa.pub" files from the primary EMS to the secondary EMS **/opt/orahome/.ssh** directory. Make the files with "oracle:orainst" ownership.

Step 3 Login to the secondary EMS:

```
#  su - oracle
$  cd /opt/orahome/.ssh
$  sftp root@priems
sftp> cd /opt/orahome/.ssh
sftp> get id_rsa*
sftp> quit
$  ls -l /opt/orahome/.ssh/id_rsa*
 -rw-------1 oracleorainst1675 Mar 10 15:42 id_rsa
 -rw-r--r--1 oracleorainst397 Mar 10 15:42 id_rsa.pub
```

Now both primary and secondary EMSs have the same "id_rsa" and "id_rsa.pub" files in **/opt/orahome/.ssh** directory.

Step 4 Create an oracle user and **/opt/backup** directory on the remote SFTP server.

a. Login to remote SFTP server as root.

b. Create a user "oracle" with group "orainst" and home directory "/opt/orahome".

c. Create a repository directory "/opt/backup".

```
# mkdir -p /opt/orahome
 # groupadd orainst
 # useradd -g orainst -d /opt/orahome -s /bin/ksh oracle
 # chown oracle:orainst /opt/orahome
# passwd oracle
   New Password:   <Enter password>
   Re-enter new Password:   <Re-enter password>
# mkdir -p /opt/backup
 # chown oracle:orainst /opt/backup
# su - oracle
$ mkdir -p /opt/orahome/.ssh
 $ chmod 700 /opt/orahome/.ssh
 $ chown oracle:orainst /opt/orahome/.ssh
```

Step 5 Sftp the "id_rsa" and "id_rsa.pub" files generated in Step 1 to remote SFTP server /opt/orahome/.ssh directory. Make the file owned by "oracle:orainst" owner and group.

Login to remote SFTP server:

```
# su - oracle
$ cd .ssh
$ sftp root@priems
   sftp> cd /opt/orahome/.ssh
   sftp> get id_rsa*
   sftp> quit
$ cat id_rsa.pub >> authorized_keys
$ chmod 600 id_rsa* authorized_keys
$ ls -l
-rw-------1 oraoragrp788 Mar 10 16:52 authorized_keys
   -rw-------1 oraoragrp1675 Mar 10 16:48 id_rsa
```

-rw-------1 oraoragrp394 Mar 10 16:48 id_rsa.pub

Step 6 Sftp the "id_rsa" and "id_rsa.pub" files generated in Step 1 to remote SFTP server /opt/orahome/.ssh directory. Make the file owned by "oracle:orainst" owner and group.

Step 7 Test SSH and SFTP from both the primary and secondary EMSs to the remote SFTP server:

a. From BTS primary EMS:

```
#  su - oracle
$ sftp_ping oracle SFTPserverName
Connecting to SFTPserverName...
      sftp> quit
      SFTP_PING=OK
```

Note At the first login, the following message may display:"Warning: Permanently added the RSA host key for IP address '10.xx.xxx.xxx' to the list of known hosts."

Step 8 To schedule the ora_sftp_backup.ksh process to execute at 5:30am every day in oracle crontab on both the primary and secondary EMS:

a. Log in as oracle, or su - oracle and enter the following:

```
crontab -e
```

b. Add the following line to the Oracle crontab on the primary EMS:

```
#
# SFTP backup files from primary (optical1) to /opt/backup directory of SFTPserver.
#
0 6 * * * /opt/oracle/admin/scripts/ora_sftp_backup.ksh optical1 oracle SFTPserver
/opt/backup > /opt/oracle/tmp/ora_sftp_backup.log 2>&1
```

Note Enter 0 6 *** /opt/oracle/admin/scripts/ora_sftp_backup.ksh…ora_sftp_backup.log 2>&1 in the same line.

Step 9 Replace SFTPserver with the correct host name of the remote SFTP server.

Step 10 Replace **/opt/backup** with the correct target directory name, if different.

Step 11 Edit the oracle crontab on secondary EMS site by replacing optical1 with optical2.

Archiving Your Database

Step 1 Log in as **root.**

Step 2 Stop all platforms. If this is a primary node, use the CLI command to control the standby forced active.

Step 3 Verify that /var/yp exists. Enter `ls -l /var/yp`.

If the result is no such file or directory, enter mkdir -p /var/yp

Step 4 Mount the NFS server. Enter **mount <nfsserver hostname/ip>:/<share directory> /mnt**. Example:

```
mount 10.89.183.253:/opt/archive /mnt
```

Step 5 Back up all interfaces. Enter **tar -cvf /mnt/<local_hostname>.tar host***. Example:

```
<hostname>#tar -cvf bts-prica.tar host.*
```

Step 6 Restore the Solaris "**date**" command to create the system Flash Archive. Enter:

```
mv /bin/date /bin/date.orig
mv /bin/.date /bin/date
```

Step 7 Create the archive. Enter **<hostname>#flarcreate -n <archive name> -x /opt -S -c /mnt/<file name>**

Note Example archive name: flarcreate -n **CCPU-EMS** -x /opt -S -c /mnt/secems04.archive

Step 8 Back up the /opt directory. Enter **tar -cvf - /opt/* |gzip -c >/opt/<hostname_release>.tar.gz**

Step 9 Restore the original configuration. Enter:

```
mv /bin/date /bin/.date
mv /bin/date.orig /bin/date
```

Step 10 Unmount the NFS server. Enter **umount /mnt**

Examining Heap Usage

Heap is memory BTS reserves for data it creates as its applications execute. BTS audits heap usage of all the processes started by a platform, CA, AIN, POTS, EMS and BDMS. Heap auditing is added to the ADP process.

When heap usage of a process goes beyond certain threshold level, BTS generates an alarm. The alarm clears when heap usage goes below the threshold level.

Heap audit does the following:

- Monitors traces of heap usage in the last four periods for each process
- Measures heap usage of each process started by the platform once a day at 4 a.m
- Issues a minor alarm if the heap usage of a process exceeds 70% of its max heap size limit
- Clears a minor alarm if the heap usage of a process drops below 68% of its max heap size limit
- Issues a major alarm if the heap usage of a process exceeds 80% its max heap size limit
- Clears a major alarm if the heap usage of a process drops below 78% its max heap size limit
- Issues a critical alarm if the heap usage of a process exceeds 90% its max heap size limit
- Clears a critical alarm if the heap usage of a process drops below 88% its max heap size limit
- Reports, via trace logs, the last twenty heap measurements, including the time and the value for each process
- Clears heap usage alarms when process restarts

Checking the DNS Server

To check the DNS server, do this for all nodes.

Step 1 Log in as **root** on the active CA.

Step 2 Enter more /etc/resolv.conf.

Note nameserver <ip address>

Step 3 Enter **nslookup**

This defaults to the first DNS server.

Step 4 Enter a valid gateway name and press **Enter**.

An IP address associated to gateway appears.

Step 5 Enter **server <second dns server ip>**

Step 6 Enter a valid gateway name and press Enter.

An IP address associated to gateway appears.

Step 7 Enter **exit** to quit.

Log Archive Facility (LAF)

The LAF process in Cisco BTS 10200 transports the trace log files to a remote archive server for storage. LAF is a continuously running daemon process on all nodes (components) of the BTS 10200. It wakes up every minute when active and checks if there are any new log files.

The service provider can specify the external archive system, the target directory, host directory, and the disk quota for each trace log directory in the system. If any new log files are in these trace log directories, LAF transfers them by Secure FTP (SFTP) to an external archive server specified by the service provider.

Secure Transfer of Files

BTS 10200 uses Secure FTP to transfer trace log files to the external server. LAF opens an SFTP connection when its ready to transfer log file to the remote server. This connection is not closed even after the transfer is complete. If for some reason the connection closes, the LAF process re-establishes the connection during the next transfer. The connection is persistent till the LAF feature is disabled.

LAF operates on a single SFTP connection and transfer of files occurs one file at a time (using the SFTP put operation). The same connection is used to transfer multiple files. When the LAF process detects a bad connection, it terminates the SFTP session by closing the socket used to talk to the archive server.

The LAF process maintains a linked list for the files that need to be transferred. If the connection is lost during a transfer, the LAF process moves the unsuccessfully transferred file to the end of the list and raises Maintenance Alarm 108.

A re-attempt on a failed file depends on the number of files in the list and the time taken to transfer those files. When there is no file to be transferred (i.e. the list is empty), then there is a gap of 30 seconds before processing the list again.

The LAF process increments a counter, which is specifically used for the number of times the transfer was attempted for this file. If a counter is more than three, the log file is deleted from the list. That is, upon three failed attempts on the same file, the file entry is deleted from the list.

Other Capabilities

This section lists the additional capabilities of the LAF process.

- It performs disk space management when 90% of the disk space quota specified for the target directory is reached.
- It gracefully recovers from any abnormal conditions and re-initiates the process to continue the transfer of files.
- It generates alarms when any unsuccessful scenarios are encountered. These alarms are listed in the *Cisco BTS 10200 Troubleshooting Guide*.

Provisioning LAF

Caution The values provided by the user for the following parameters will be written into /etc/opticall.cfg file and transported to all the four BTS 10200 nodes.

The following parameters are associated with the LAF process. If they are left blank, the LAF process for a particular platform (such as, CA, FSPTC, FSAIN) is turned off.

To use this feature, you must provision the following parameters with the external archive system, the target directory, and the disk quota (in GB) for each platform.

CA*xxx*_LAF_PARAMETER

FSPTC*xxx*_LAF_PARAMETER

FSAIN*xxx*_LAF_PARAMETER

Note that *xxx* must be replaced with each platform's instance number.

Example 1

```
CA146_LAF_PARAMETER="yensid /CA146_trace_log 20"
```

Example 2

```
FSPTC235_LAF_PARAMETER="yensid /FSPTC235_trace_log 20"
```

Example 3

```
FSAIN205_LAF_PARAMETER="yensid /FSAIN205_trace_log 20"
```

To enable Log Archive Facility (LAF) process, refer to Enabling LAF Process section.

Enabling LAF Process

To enable the Log Archive Facility (LAF) feature, you must set up the authorization for non-interactive SSH login to the external archive server for the Cisco BTS 10200 system to access and turn the LAF processes to active state. (Immediately after the fresh installation and platform start, the LAF process is in a dormant state).

The steps to set up the authorization in external archive server and turn the LAF processes to active is listed below:

Setup Non-Interactive SSH Login to External Archive Server

Note The external archive system is recommended to be located such that it can be accessed by the management network. In such a case, the static routes in the CA system should be explicitly set so that the traffic to the external archive system is routed through the management network see section ("Adding Static Routes" section for more details). Otherwise, the traffic is routed through the default network (i.e. signaling network) and may not be able to reach the external archive system.

Step 1 Log in to the Cisco BTS 10200 primary EMS as **root**.

Step 2 From the EMS, login to the external archive server via ssh to get the external archive server added to the */.ssh/known_hosts* file.

Step 3 Log off from the external archive server.

Step 4 While still logged in on the primary EMS as **root**, generate an SSH key.

- **a.** Execute **cd /opt/BTSossh/bin**.
- **b.** Execute **ssh-keygen -t rsa**.
- **c.** Press Enter to accept the default file name for the key (**/.ssh/id_rsa**).
- **d.** Enter **y** if prompted to choose whether to overwrite the existing file.
- **e.** Press Enter when prompted to enter a passphrase (i.e. no passphrase).
- **f.** Transfer the resulting file (**/.ssh/id_rsa.pub**) to a temporary location on the external archive server.

Step 5 Set up the external archive server with the key generated in Step 4.

- **a.** Login to the external archive system as **root**.
- **b.** If a */.ssh/authorized_keys* file does not exist on the external archive system, rename the **id_rsa.pub** file (copied from the Cisco BTS 10200 EMS) to */.ssh/authorized_keys*. If the file does exist, append the **id_rsa.pub** file to it.

Step 6 On the primary EMS, execute

ssh root@abcd

where *abcd* is the IP address or fully-qualified domain name of the external archive server.

Step 7 Verify that login to the external archive server is successful and that no prompts for username or password are issued.

Step 8 Run **enableLAF** in EMS platform directories (i.e. */opt/ems/bin and /opt/bdms/bin*)

Step 9 Repeat Steps 1-8 for the secondary EMS, primary CA and secondary CA. (In CA, the platform directories are */opt/OptiCall/CAxxx/bin*, */opt/OptiCall/FSPTCyyy/bin*, */opt/OptiCall/FSAINzzz/bin*).

Note Billing has a similar mechanism/steps to SFTP their Call Detail Blocks (CDB) files to an external machine. If the LAF and Billing use the same target machine, then in both EMS, perform Steps 1-7 only once. You must still run Step 8 to enable LAF. And you must still run Steps 1 -9 in CA nodes.

Adding Static Routes

To add static routes to all Cisco BTS 10200 systems, perform the following steps:

Step 1 From the shell or window of the primary call agent, change directory to */opt/utils*.

```
cd /opt/utils
```

Step 2 Edit **S96StaticRoutes** using an editor.

Step 3 Add the subnet of NTP server, DNS server, external archive server and any other machine to the file, which user wants to have access to Cisco BTS 10200 system in the following format:

```
route add -net <destination network> <network gateway>
```

Note All NTP, DNS traffic, traffic to external archive server, and traffic from other machine to Cisco BTS 10200 system (eg. login), should all go through management networks. (i.e. network gateway in management network). This is particularly important in CA system because CA has both management and signaling network. If user does not specify explicitly in this file, those traffic will be directed to signaling network, because signaling network is the default one in CA/FS.

Step 4 Make sure there is a soft link pointing from */etc/rc3.d/S96StaticRoutes* to */opt/utils/S96StaticRoutes*.

```
ls -l /etc/rc3.d/S96StaticRoutes
```

Step 5 After editing, close the file, and run **S96StaticRoutes**.

```
/etc/rc3.d/S96StaticRoutes
```

Step 6 Repeat Step 1 to Step 5 on the secondary CA.

Step 7 Verify the connectivity by pinging the DNS server, NTP server, external archive server, or any machine that user just added in that file.

LAF Alarm Information

Refer to the following link to see the LAF alarm information.

Document Name	Link to the Document
Cisco BTS 10200 Troubleshooting Guide	*http://www.cisco.com/en/US/docs/voice_ip_comm/bts/6.0/troubleshooting/guide/07tg01.html#wp1938289*

Moving Core Files

BTS creates and stores core files in the bin directory for the binary executable that generated the core. Core files are large (2–4 GB) and eventually cause a disk full condition resulting in a switchover. When a BTS platform system generates a core file, the BTS creates an alarm. The Core File Present—Audit 25 (major) alarm indicates a core is present in the BTS. The primary cause of this alarm is that a network element process crashed.

The BTS automatically removes these core files when disk space is critically low or the core file has aged beyond a maximum allowable time. However, to ensure proper BTS performance move these core files off the BTS to another storage area as soon as they are generated. Refer to the Directory Containing Core Files dataword for the location of the core file.

Use the settings in the cfm.cfg file to configure how to monitor and manage core files.

Table 3-7 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 to true, the oldest core files are deleted when free file space is low. Default is true.