



# Core and Billing Manager 850 Fault Management

---

## Fault Management Strategy

The Core and Billing Manager 850 (CBM 850) uses self-testing, automated diagnostics, and reporting systems to support maintenance and to manage faults. These systems raise alarms and generate logs when the following types of software and hardware events occur:

- one or more CBM 850 applications have failed
- the CBM 850 is reporting an in-service trouble condition
- a system software resource has exceeded its alarm threshold
- a hardware device failure has been reported
- communication with the core has failed
- correction of a fault or failure condition

## Alarms

Alarms provide notification that a system hardware or software-related event has occurred that requires attention. Alarms are generated when problems or conditions are detected that can change the performance or operating state of the CBM 850 and its connections.

Fault conditions on the CBM 850 are indicated through the customer's office alarm unit, through hardware LEDs, or through alarms displayed on the Integrated EMS (IEMS) alarm management system. Alarms are also displayed on the CBM maintenance interface (CBMMTC) alarm banner.

Routine CBM 850 administration requires monitoring for alarms and alarm status, and checking that functions continue without interruption.

## Logs

A log report is a record of a message generated whenever a significant event on the system has occurred. Log reports include status and activity reports, as well as reports on hardware or software faults, test

results, changes in state, or other temporary events or conditions likely to affect the performance of the system. A system action or a manual action can generate a log report.

In the CBM 850, applications and CBM base software generate logs to identify status changes and to notify the operator about events requiring attention. Logs are also generated on the core, in response to the loss of heartbeat between the core and CBM 850. Core-side CBM application software also generates logs on the core. The Log Delivery application, included as part of the base software on the CBM 850, collects the logs generated by the CBM 850 and by the core in order to provide a single fault feed to the operational support systems (OSS).

A list of the CBM 850 logs can be found in [CBM 850 logs on page 1](#).

### **Fault clearing procedures**

The basic strategy for clearing CBM 850 faults is outlined in [Strategy for clearing a CBM 850 fault condition on page 21](#).

## **Tools and utilities**

It is important to note that CBM 850 application maintenance is separated from the maintenance of the platform on which the CBM 850 resides. Thus, CBM 850 application maintenance function is performed through the CBM maintenance interface (CBMMTC) and through the command line. Maintenance for the SSPFS platform and for the Sun Netra240 hardware platform is performed through a suite of SSPFS tools.

### **CBMMTC**

The CBMMTC includes a hierarchical set of screens or levels and a dynamic alarm banner that provides state information, for the following functional areas:

- CBM product state (aggregated from all subcomponent states), that includes the state of the inactive server in the cluster configuration
- application state (aggregated from all individual application states)
- core connectivity status
- Network Time Protocol (NTP) service health status
- platform status, including computing resources, and file system resources and health

Each of the functional areas, except for CBM product state, has individual screens or levels that provide an aggregated state for its own sub-components. Thus, for example, the applications level aggregates

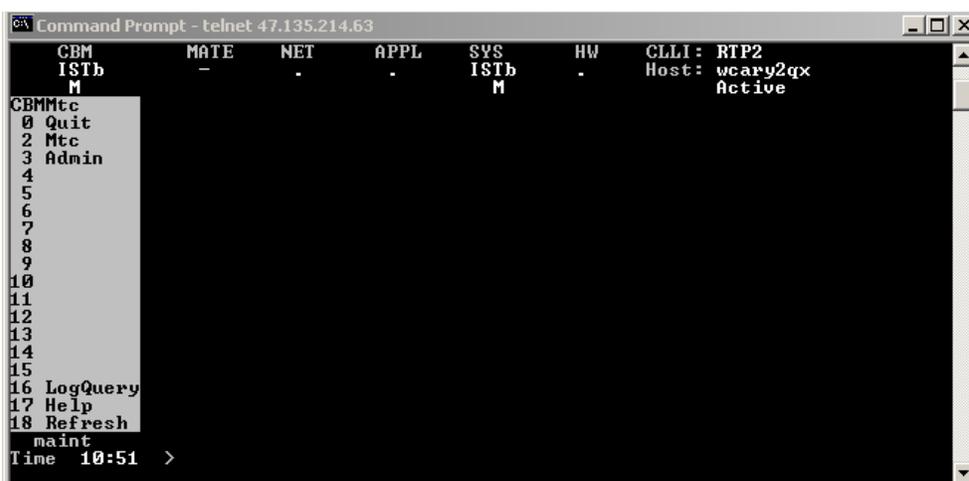
the state of each application into the general application state. Additional levels provide administration functions such as:

- user pass-through functionality, which allows user to pass directly to the core for terminal access for file transfer operations
- access configuration to set the level of terminal access
- software installation and maintenance

The individual component states reflect the state of the local server where the cbmmtc tool is being run. Each screen in the cbmmtc tool provides context-sensitive help text and fault reporting.

A sample CBMMTC screen is shown below.

**Figure 1 Sample CBMMTC screen**



```
Command Prompt - telnet 47.135.214.63
  CBM   MATE   NET   APPL   SYS   HW   CLLI: RTP2
  ISTb  -      -      -      ISTb  .   Host: wcarv2qx
  M                                           Active

CBMMtc
0 Quit
2 Mcc
3 Admin
4
5
6
7
8
9
10
11
12
13
14
15
16 LogQuery
17 Help
18 Refresh
  maint
Time 10:51 >
```

The alarm banner categories include:

- CBM - status the CBM
- MATE - status of the mate of the active CBM in a CBM 850 cluster
- NET - network status
- APPL - CBM application status
- SYS - system status
- HW - hardware status

The alarm banner states for the categories are shown in the table below.

State	Description
-	unequipped
.	standby
.	in-service
ISTb	in-service trouble
SysB	system-made busy
ManB	manually-made busy
OffL	offline
CBsy	c-side busy
Fail	failure

The alarm status indicators that appear below the alarm banner states are shown in the table below.

Alarm Indicator	Description
	cleared
	warning
	minor
M	major
*C*	critical
?	indeterminate

### SSPFS / Sun Netra240 services

The SSPFS common OAM platform provides the system monitoring and maintenance procedures for the platform on which the CBM 850 runs. The platform provides the basic resources necessary for the CBM 850 and its applications. The SSPFS platform is maintained using SSPFS-provided tools and procedures built on standard Sun/Solaris

administration tools and commands. The procedures and capabilities provide functions such as:

- procedures for diagnosing all platform faults
- procedures for upgrading SSPFS platform hardware and software
- procedures for field-replaceable-unit (FRU) hardware replacement, such as disk drives, DVD drives, and the server itself
- creating and modifying file systems (or logical volumes) and their characteristics, including size, capacity, permissions, alarm threshold, type
- user interfaces to maintain the HA cluster, including the ability to switch activity (SwAct), query which unit is active, and state of HA services
- interface to determine the active or inactive node
- ability to duplicate synchronize the program store and configuration from the active unit to the inactive unit in the cluster (image copy)

## **CBM 850 maintenance procedures**

This document contains the procedures used for maintaining the CBM 850 and for responding to fault conditions that arise on the CBM 850. The procedures are performed primarily in response to alarms and logs that are raised. The log and alarm description and text generally provide you with the direction needed to determine which procedure to perform.

To assist you in locating the correct procedure when specific instructions are not provided in an alarm or log, the following tables group procedures by the general functional areas, "CBM 850 application", "SuperNode Billing Application (SBA)", and "SSPFS / Sun Netra 240 services".

**CBM 850 application fault clearing procedures**

The following table contains the fault clearing procedures for CBM 850 applications.

<b>CBM 850 application</b>
<a href="#">Strategy for clearing a CBM 850 fault condition</a>
<a href="#">Clearing a CBM application alarm</a>
<a href="#">Clearing a GDD logical volume size threshold violation on page 29</a>
<a href="#">Collecting DEBUG information using the CBMGATHER command</a>
<a href="#">Displaying or storing log records using logreceiver</a>
<a href="#">Retrieving and viewing log records</a>
<a href="#">Troubleshooting Log Delivery problems on a CBM</a>
<a href="#">Verifying the file transfer protocol</a>
<a href="#">Verifying the FTP Schedule</a>

## SuperNode Billing Application (SBA) fault clearing procedures

The following table contains procedures used for clearing faults related to the SuperNode Billing Application (SBA). The type of alarm or log you receive in response to a fault will contain the information that will normally direct you to the appropriate procedure to use. If no specific SBA fault clearing procedure is apparent in the alarm or log, refer to [SBA alarm troubleshooting on page 41](#).

SuperNode Billing Application (SBA)
<a href="#">SBA alarm troubleshooting</a>
<a href="#">Displaying SBA log reports</a>
<a href="#">Displaying SBA alarms</a>
<a href="#">Controlling the SDM Billing Application</a>
<a href="#">Troubleshooting AFT alarms</a>
<a href="#">Troubleshooting RTB problems</a>
<a href="#">Troubleshooting problems with scheduled billing file transfers</a>
<a href="#">Clearing a BAK50 alarm</a>
<a href="#">Clearing a BAK70 alarm</a>
<a href="#">Clearing a BAK90 alarm</a>
<a href="#">Clearing a BAKUP alarm</a>
<a href="#">Adjusting disk space in response to SBA backup file system alarms</a>
<a href="#">Clearing a CDRT alarm</a>
<a href="#">Clearing a DSKWR alarm on a CBM</a>
<a href="#">Clearing an FTPW alarm</a>
<a href="#">Clearing an inbound file transfer alarm</a>
<a href="#">Clearing an LODSK alarm</a>
<a href="#">Clearing a NOBAK alarm</a>
<a href="#">Clearing a NOCLNT alarm</a>
<a href="#">Clearing a NOFL alarm</a>

**SuperNode Billing Application (SBA)**

[Clearing a NOREC alarm](#)

[Clearing an NOSC alarm](#)

[Clearing a NOSTOR alarm](#)

[Clearing a NOVOL alarm](#)

[Clearing an RTBCF alarm](#)

[Clearing an RTBER alarm](#)

[Clearing an RTBFM alarm](#)

[Clearing an RTBPD alarm](#)

[Clearing an RTBST alarm](#)

[Clearing a major SBACP alarm](#)

[Clearing a minor SBACP alarm](#)

[Clearing an SBAIF alarm](#)

**SSPFS / Sun Netra 240 services fault clearing procedures**

The following table shows selected SSPFS procedures that are used during CBM fault clearing. If you do not find a procedure that you need to use, contact your next level of support for assistance.

<b>SSPFS / Sun Netra 240 services</b>
<a href="#">Clearing a major Heartbeat alarm</a>
<a href="#">Replacing a failed power supply</a>
<a href="#">Replacing failed Ethernet interfaces</a>
<a href="#">Accessing TCP and TCP-IN log devices from a remote location</a>
<a href="#">Accessing the MATE</a>
<a href="#">Clearing the MATE alarm</a>
<a href="#">Replacing one or more failed disk drives on an SSPFS-based server</a>
<a href="#">Shutting down an SSPFS-based server</a>
<a href="#">Preparing a CD-RW or DVD-RW for use</a>
<a href="#">Increasing the size of a file system on an SSPFS-based server</a>
<a href="#">Performing a backup of file systems on an SSPFS-based server</a>
<a href="#">Verifying disk utilization on an SSPFS-based server</a>
<a href="#">Replacing a DVD drive on an SSPFS-based server</a>
<a href="#">Initiating a manual failover on a Sun Netra 240 server pair</a>
<a href="#">Viewing customer logs on an SSPFS-based server</a>

## CBM 850 logs

The following is a list of the CBM 850 logs, with high-level summaries of causes for the logs, and general descriptions of actions to be taken in response. The logs are arranged in two categories:

- SDM logs - logs pertaining to CBM
- SDMB logs - logs pertaining to SBA (SuperNode Billing Application)

The comprehensive listing of all Carrier VoIP logs is found in NN10275-909, *Carrier Voice over IP Fault Management Logs*. The NN10275-909 document should always be consulted for complete information about CBM logs and the actions to be taken in response.

## SDM logs

The following table lists SDM logs.

Log	Trigger	Action
SDM303	A core manager application or process has failed more than three times in a day, or has declared itself to be in trouble.	Users with root permissions can examine the log files in /usr/adm to determine the cause of the process failure. If required, contact your next level of support for assistance.
SDM304	The Log Delivery application cannot deliver logs to the specified UNIX file.	Use the Log Delivery online commissioning tool (logroute) to verify the existence and validity of the device name. Refer to the following procedures for more information: <ul style="list-style-type: none"> <li>• “Configuring a core manager for log delivery” in the Configuration Management document</li> <li>• “Deleting a device using logroute” in the Configuration Management document</li> </ul> If required, contact your next level of support for assistance.

Log	Trigger	Action
SDM306	The Table Access Service application on the core manager has detected that the software load on the Core is incompatible with the software load on the core manager.	Upgrade the CM software to a version that is compatible with the SDM software.  <b>Note:</b> The software on the core manager must not be at a lower release level than the software on the Core.
SDM315	The Table Access Service application on the core manager has detected corruption in the Data Dictionary on the Core.	Contact your next level of support with the information provided in the log. The log information contains essential information for identifying the Data Dictionary type that is corrupt.
SDM318	An operational measurements (OM) report was not generated. (The OM report failed to complete within one report interval.)	Contact your next level of support.
SDM325	Indicates a lost connection to a Preside network management component.	No action required.
SDM330	Indicates a communication problem between two mated nodes on a CBM850 HA cluster	Use the description field to determine necessary action.
SDM331	OMDD audit deleted files from the OMDD storage volume to free up space.	No action required.
SDM333	OMD audit discovers that the OMDD storage usage has gone above 60%	Delete the old OM reports from the volume reported by the log. Otherwise, older files will get deleted in the next audit if the usage has gone up to above 70%.
SDM336	No heartbeat response received	Use the logs command from the hw level of the cbmmtc display to check for Ethernet link faults on the CBM. Check on core mapci;mtc;xac level for Ethernet connectivity faults.

Log	Trigger	Action
SDM375	OMDD discovered a problem while performing outbound file transfer and could not ensure that the OM report got transferred downstream.	Contact your next level of support.
SDM603	A fault on a core manager application or process has cleared.	No action required.
SDM604	The Log Delivery Application generates this log when the Core generates logs at a higher rate than can be transferred to the Log Delivery Service and the device buffer on the core is too full to accept more logs.	<p>Increase office parameter PER_OPC_LOGDEV_BUFFER_SIZE to its maximum size of 32,000. (For more information about this parameter, refer to the <i>SuperNode Data Manager Log Report Reference Manual</i>, 297-5051-840.)</p> <p>If you still continue to receive SDM604 logs after you have increased the size of the parameter, or if large numbers of logs are lost, contact your next level of support for assistance.</p>
SDM619	The OM Access Server has detected a corrupt OM Group during an OM Schema download.	No action required.
SDM622	The SDM log delivery application generates this log when the file device reaches its maximum size.	Check if you have configured enough space for the file device. If there is a software error causing the increase of logs, contact your next level of support for help.
SDM625	Indicates a re-established connection to a Preside network management component.	No action required.
SDM636	Heartbeat alarm cleared	No action required.
SDM700	Log report SDM700 reports a Warm, Cold, or Reload restart or a norestartswact on the core	No action required.

Log	Trigger	Action
SDM739	This log prints the ftp user's log-in status.	No action required.
SDMO 375	Indicates that OMDD discovered a problem while performing an outbound file transfer and could not ensure that the OM report was transferred downstream.	Contact your next level of support.

## SDMB logs

SDMB logs describe events related to the operations of the SuperNode Billing Application (SBA) and the SDM Billing System that resides on the core manager. The following table lists SDMB logs.

### SDM Billing Application (SBA) logs

Log	Trigger	Action
SDMB300	Memory allocation has failed.	Contact your next level of support.
SDMB310	A communication-related problem has occurred.	Determine the reason that the core manager is not communicating with the Core. Determine whether the core manager, the Message switch (MS) and the Frame Transport bus (FBus) are in service (InSv) or in-service trouble (ISTb). If the core manager is InSv or ISTb, return the billing stream to service.
SDMB315	A general software-related problem has occurred.	Contact your next level of support.
SDMB316	A billing-related process has been manually "killed".	Restart the process.
SDMB320	A billing backup-related problem occurred, which affects more than one file.	Ensure that the backup volumes configured for the stream have enough available space.
SDMB321	A billing backup-related problem occurred, which affects one file.	Ensure that the backup volume is not busy or full.

**SDM Billing Application (SBA) logs**

<b>Log</b>	<b>Trigger</b>	<b>Action</b>
SDMB330	The configuration of a billing stream failed.	Configure the billing stream using the procedure "Configuring a billing stream" in the Accounting document.
SDMB350	An SBA process has reached a death threshold and made a request to restart. A death threshold occurs after a process has died more than 3 times less than 1 minute apart.	SBA will automatically restart. What for logs that indicate that SBA is in normal operation. If the system generates this log more than once, contact your next level of support.

**SDM Billing Application (SBA) logs**

<b>Log</b>	<b>Trigger</b>	<b>Action</b>
SDMB355	<p>A problem with a billing disk has occurred, which can consist of any one of the following problems:</p> <ul style="list-style-type: none"> <li>• Records cannot be written to file (by stream). When this occurs, alarm DSKWR is raised.</li> <li>• The Record Client/File Manager is unable to write to the disk.</li> <li>• The disk use is above the critical threshold specified in the MIB in parameter. When this occurs, alarm LODSK is raised.</li> <li>• The disk use is above the major threshold specified in the MIB in parameter. When this occurs, alarm LODSK is raised.</li> <li>• The disk use is above the minor threshold specified in the MIB in parameter. When this occurs, alarm LODSK is raised.</li> <li>• Reached limit for disk space or for the number of files that can reside on the system for a particular stream.</li> <li>• The SBA cannot close or open a file.</li> <li>• Flush file failed</li> </ul>	<ul style="list-style-type: none"> <li>• Check the disk space on the core manager. You may need to FTP files or may need to clean up the disk.</li> <li>• Check the disk space on the core manager. You may need to FTP files or may need to clean up the disk.</li> <li>• Check to see if files are being sent FTP. If not, set the system up to FTP files or back up files.</li> <li>• Check to see if files are being sent FTP. If not, set the system up to FTP files or back up files.</li> <li>• Check to see if files are being sent FTP. If not, set the system up to FTP files or back up files.</li> <li>• Check to see if files are being sent FTP. If not, set the system up to FTP files or back up files.</li> <li>• Check to see if files are being sent FTP. If not, set the system up to FTP files or back up files. Also check file permission for the destination directories.</li> <li>• Contact your next level of support.</li> </ul>
SDMB360	<p>SBA has lost the connection to the Persistent Store System (PSS) and cannot restore it. When this occurs alarm SBAIF is raised.</p>	<p>Contact your next level of support.</p>

**SDM Billing Application (SBA) logs**

<b>Log</b>	<b>Trigger</b>	<b>Action</b>
SDMB365	A serious problem is preventing the creation of a particular stream. Generated when a new version of SBA does not support a stream format on an active stream that was present in a previous load.	Revert to the previous running version of the SBA. If you removed the support for the stream format in the new release, turn off the stream before installing the new version. If the new version is supposed to support all existing streams, contact your next level of support for the latest appropriate software.
SDMB366	Indicates that a problem exists on the SDM. If the installed SBA supports multiple stream record formats, you can continue to process streams of the unlogged formats.	Contact your next level of support.
SDMB367	A trapable Management Information Base (MIB) object was set. The modification of some MIB objects provides notification of failures to the System Manager by way of a trap. Because there is no System Manager, the system logs messages. While most SDM logs report the stream, the logs associated with the MIB do not. Consideration for separate streams is not built into the Automatic Accounting Data Networking System (AMADNS) MIB specification.	Contact your next level of support.
SDMB370	The CDR-to-BAF conversion encountered a problem that prevents it from converting CDR to BAF. When this occurs, alarm NOSC is raised because the BAF record was not generated.	Clear the alarm.

**SDM Billing Application (SBA) logs**

Log	Trigger	Action
SDMB375	<p>A problem occurred during the transfer of a file to the Data Processing Management System (DPMS). When this occurs, alarm FTP is raised. The error text can be any of the following:</p> <p><b>Note:</b> The system may escalate these logs and minor alarms to critical status when the DPMS transmitter exhausts all possible retries. The MIB parameter SessionFtpMaxConsecRetries specifies the condition.</p>	<p>Contact your next level of support if log indicates any one of the following errors:</p> <ul style="list-style-type: none"> <li>• insufficient storage space in system</li> <li>• exceeded storage allocation on downstream DPMS</li> <li>• unable to fork child process</li> <li>• unable to open pseudo terminal master</li> <li>• unable to setsid in child process</li> <li>• unable to open pseudo terminal slave in child process</li> <li>• unable to set stdout of child process to pseudo terminal slave</li> <li>• unable to set stderr of child process to pseudo terminal slave</li> <li>• unable to set stdin of child process to pseudo terminal slave</li> <li>• local error in processing</li> <li>• DPMS FTP service not available</li> <li>• DPMS FTP connection closed</li> <li>• requested file action not taken: &lt;command&gt;. File unavailable</li> </ul> <p>Verify FTP if the log indicates any one of the following errors:</p> <ul style="list-style-type: none"> <li>• not logged in while executing command: &lt;command&gt;</li> <li>• unable to exec FTP process</li> </ul>
SDMB380	<p>The file transfer mode for the specified stream has an invalid value</p>	<p>Set the file transfer mode to either Inbound or Outbound.</p>

**SDM Billing Application (SBA) logs**

<b>Log</b>	<b>Trigger</b>	<b>Action</b>
SDMB390	A schedule-related problem has occurred. When this occurs, alarm SBAIF is raised.	Clear the alarm and any alarms related to failure.
SDMB400	This log is generated for every active stream every hour and lists all of the current active alarms.	Clear alarms immediately using the corresponding procedure in the Fault section.
SDMB530	A change in the configuration or status of a stream has occurred.	No action required.
SDMB531	The configuration for backup volumes has been corrected.	No action required.
SDMB550	The SBA has shut down either because the core manager was busied or the SBA was turned off.	Determine the reason SBA shut down.
SDMB600	This generic log provides information for billing system problems.	No action required.
SDMB610	A communication-related problem with the SBA has been resolved.	No action required.
SDMB615	A software-related condition has been resolved.	No action required.
SDMB620	A backup-related problem with the SBA has been resolved.	No action required.
SDMB621	A new backup file has been started.	No action required.
SDMB625	Recovery has started on a backup file.	No action required.
SDMB650	The SBA is restarting one or more of its processes.	No action required.

**SDM Billing Application (SBA) logs**

<b>Log</b>	<b>Trigger</b>	<b>Action</b>
SDMB655	<ul style="list-style-type: none"> <li>• The state of a billing file has changed.</li> <li>• Disk utilization for a particular stream has dropped below a threshold.</li> <li>• A billing file could not be moved to closedSent.</li> </ul>	Contact your next level of support.
SDMB660	A problem related to communications with other SBA features was resolved.	No action required.
SDMB665	A software problem on the Core that prevents the synchronization (downloading) of FLEXCDR data at the core manager.	Restart the Core with a load that supports the SBA enhancements for CDR on the core manager.
SDMB670	Either a CDR-to-BAF conversion process used default values to create a BAF field because a CDR field was missing, or the problem was corrected.	For the missing CDR field(s), determine which are needed to generate the BAF field. Use the BAF field displayed in the log report and refer to the applicable Billing Records Application Guide for a list of the CDR fields associated with each BAF field. Update the CDR to include the missing field.
SDMB675	A problem related to file transfer was resolved.	No action required.
SDMB680	The file transfer mode has changed value.	No action required.
SDMB690	Indicates that an SBAIF alarm has cleared.	No action required.

**SDM Billing Application (SBA) logs**

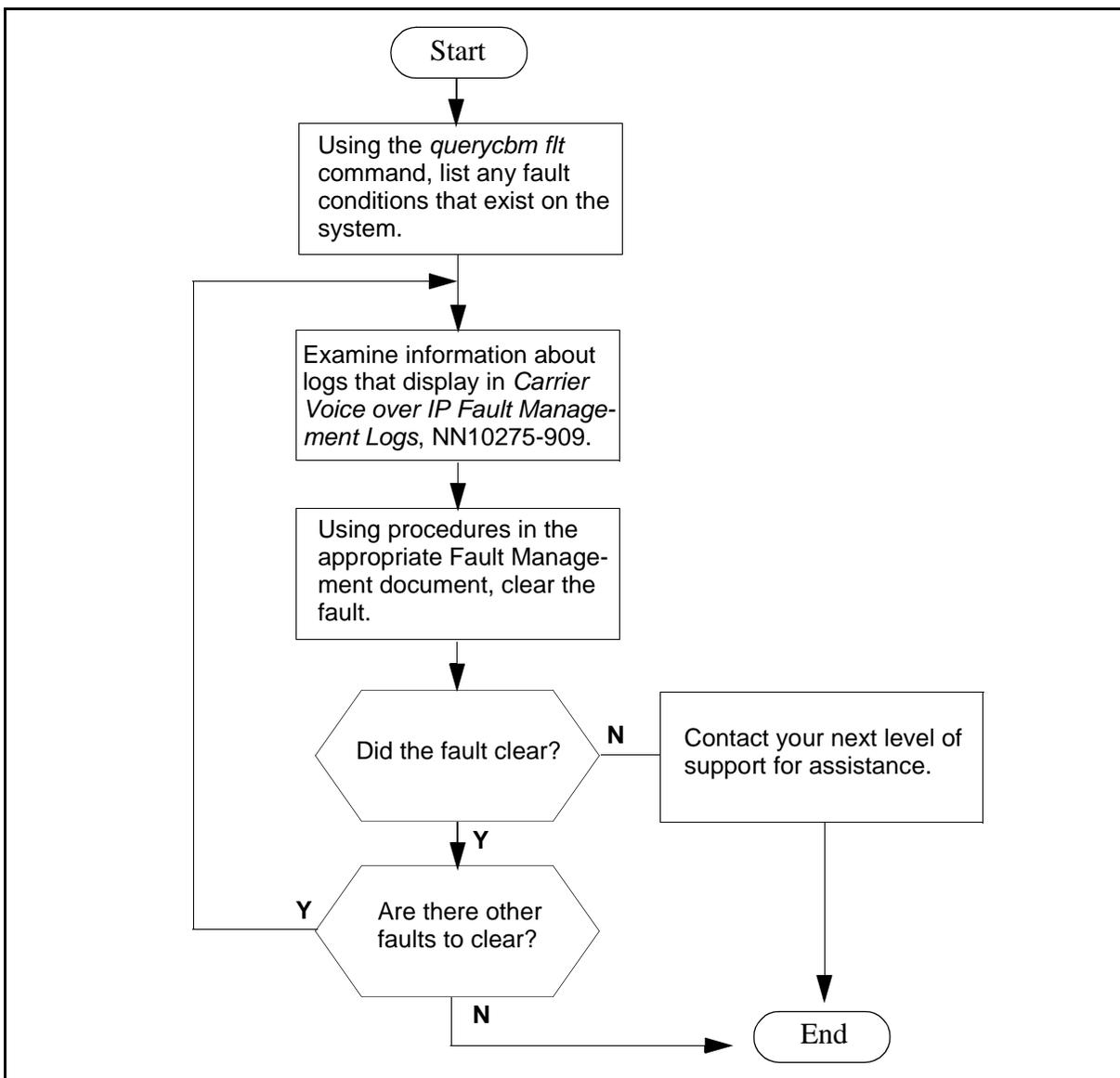
<b>Log</b>	<b>Trigger</b>	<b>Action</b>
SDMB691	Identifies events related to the scheduled transfer of billing files.	For the version of this alarm that displays the message, "Unable to initialize file transfer schedule for stream <stream>", make sure the system is free of faults. When the system is free of faults, the SBA will resume the scheduled transfer of billing files.
SDMB820	Minimal backup space is available.	Increase the size of backup volumes.

## Strategy for clearing a CBM 850 fault condition

The following procedure shows the basic steps to be performed to clear a CBM 850 fault. The procedure is designed to provide you with a fault-clearing strategy to follow. Specific procedures in this document and in other documents in the Carrier VoIP document collection provide you with the detailed steps used to actually clear a fault.

The steps required to clear a CBM 850 fault are outlined in the following flowchart.

### Basic task flow for clearing faults on the CBM 850



## Procedure

### Strategy for clearing a CBM 850 fault condition

#### At your CBM 850

- 1 Log into the CBM 850 as a maint class user, or root user, and list any fault conditions that exist on the system:

```
querycbm flt
```

- 2 Use the table below to determine the type of fault indicated by the response. Note the log type and the reason for use in later steps.

Fault type	log number	Description
Application	SDM303	Exceeded failure threshold Package: <package> Process: <process>  Trouble condition asserted Package: <package> Process: <process> <reason>
Communication	SDM336	Heartbeat alarm. No heartbeat response received.
Billing related	SDMBxx	Specific to the SBA
Network Time Protocol	SDM327	NTP alarm. Synchronization started, can take up to 30 minutes.
Platform related	SPFSxx	Specific to the platform, such as a hardware fault or resource exceeded threshold

- 3 For any logs that display, read and understand any information available about the logs in NN10275-909, *Carrier Voice over IP Fault Management Logs*. Record the relevant details for the fault condition, such as the network element name, time that the log was raised, severity, and category.

- 4 Use the following table to determine the appropriate response to the fault condition.

If the fault is	Do
Platform related (SPFSxxx) problem	Refer to <a href="#">SSPFS / Sun Netra 240 services fault clearing procedures on page 9</a>
Communication problem with the Core (SDM336)	Refer to <a href="#">Clearing a major Heartbeat alarm on page 31</a>
Network Time Protocol problem (SDM327)	First verify with your system administrator that the NTP server is not in a fault condition. If the fault condition is not in the NTP server and can be isolated to the CBM 850, contact your next level of support for assistance.
Application problem (SDM 303)	<a href="#">Clearing a CBM application alarm on page 24</a>
SBA related (SDMBxx)	Refer to <a href="#">SuperNode Billing Application (SBA) fault clearing procedures on page 7</a>

- 5 Refer to the alarm indicator that informed you about the fault condition and check to see that the fault has now been cleared.

If	Do
the fault has cleared	step <a href="#">6</a>
the fault has not cleared	Contact your next level of support for assistance

- 6 Check to see if all fault conditions have now cleared:

**querycbm flt**

If	Do
any fault conditions still exist	step <a href="#">3</a>
no fault conditions exist	step <a href="#">7</a>

- 7 You have completed this procedure.

---

## Clearing a CBM application alarm

---

### Purpose

Use this procedure to clear a minor or major or critical CBM alarm for a CBM application.

**Note:** Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or \$, displayed by the system through a GUI or on a command line.

### Action

#### Clearing a CBM application alarm

##### *At the local or remote VT100 terminal*

- 1 Log into the CBM as a maint class user, or root user, and access the maintenance interface:

```
cbmmtc
```

- 2 Access the application (Appl) menu level of CBMMTC:

```
appl
```

*Example response:*

```
Group: CBM                               State: ISTb
# Application                             State
1 Generic Data Delivery                   .
2 OSS Comms Svcs                          ManB
3 Log Delivery Service                     .
4 Table Access Service                     .
5 OM Access Service                        .
6 OM Delivery                              .
7 GR740 Pass Through                       .
8 Passport Log Streamer                    ISTb
9 Base Maintenance Utility                  .
10 FTP Proxy                               .
                                           Applications showing: 1 to 10 of 10
```

- 3 Refer to the following table to determine your next step.

If you	Do
receive a Generic Data Delivery (GDD) threshold alarm	refer to procedure <a href="#">Clearing a GDD logical volume size threshold violation on page 29</a>
do <i>not</i> receive a GDD threshold alarm	<a href="#">step 4</a>

- 4 Determine the affected application from the display and note its key number, shown under the header "#".
- 5 Proceed depending on the state of the application.

If the state is	Do
ManB	<a href="#">step 6</a>
ISTb	<a href="#">step 7</a>
SysB	<a href="#">step 9</a>
Fail	<a href="#">step 10</a>

- 6 Determine from office records or other personnel why the application was manually removed from service. When permissible, return the application software package to service:

**rts <key>**

where

**<key>**

is the key number of the application, shown under the header "#"

*Example response:*

```
RTS Application - Command initiated.
Please wait...
```

**Note:** When the RTS command is finished, the "Please wait..." message disappears. The word "initiated" also changes to "complete" as follows:

```
RTS Application Command complete.
```

If	Do
the application returns to service	<a href="#">step 13</a>

If	Do
the application does not return to service	<a href="#">step 5</a>

- 7 The ISTb state can result from one of the following reasons:
- a recent change of state
  - this application is dependent on another application that has not completed initialization

If	Do
either reason is applicable	wait 10 minutes for the applications to complete initializing
either reason is <i>not</i> applicable	use the value in the reason field to resolve the problem

- 8 Refer the following table to determine your next step.

If you	Do
can resolve the ISTb problem	<a href="#">step 13</a>
cannot resolve the ISTb problem	Contact your next level of support.

- 9 Use the reason given to resolve the SysB problem.

If you	Do
can resolve the SysB problem	<a href="#">step 13</a>
cannot resolve the SysB problem	Contact your next level of support.

- 10 The specified application software package was set to Fail state because it failed for one of the following reasons:

- the system cannot restart the package
- the application has restarted and failed three times within 10 minutes

At the application menu level of the RMI, manually busy the affected application software package:

**bsy** <key>

*where*

**<key>**

is the key number of the application, shown under the header “#”

*Example response:*

```
Bsy Application - Command initiated.
Please wait...
```

**Note:** When the Bsy command is finished, the “Please wait...” message disappears. The word “initiated” also changes to “complete” as follows:

```
Bsy Application - Command complete.
```

**11** Return the application to service:

**rts <key>**

where

**<key>**

is the key number of the application, shown under the header “#”

*Example response:*

```
RTS Application - Command initiated.
Please wait...
```

**Note:** When the RTS command is finished, the “Please wait...” message disappears. The word “initiated” also changes to “complete” as follows:

```
RTS Application - Command complete.
```

**12** Proceed depending on the state of the application.

If the application	Do
remains in a Fail state	refer to the configuration or installation information modules in the Configuration or Upgrades documents specific to that application
changes to InSv state	go to <a href="#">step 13</a>

- 13** Obtain the fault status information from the CBM:

**querycbm flt**

<b>If</b>	<b>Do</b>
more faults are reported	<a href="#">step 2</a>
all faults are cleared	<a href="#">step 14</a>

- 14** You have completed this procedure.

## Clearing a GDD logical volume size threshold violation

### Application

Use this procedure to clear the fault that results when the content of the Generic Data Delivery (GDD) logical volume exceeds its designated content size threshold.

### Indication

The system operation is unpredictable when a logical volume reaches 100% disk full, and CBM applications can fail as a result.

### Action

#### Clearing a GDD logical volume size threshold violation

##### *At the local or remote VT100 terminal*

- 1 There are two choices when the GDD logical volume size threshold is exceeded:
  - increase the size of the logical volume
  - or
  - decrease the number of days to keep the logs

If you decide to	Do
Increase the size of the GDD logical volume	proceed to the SSPFS procedure <a href="#">Increasing the size of a file system on an SSPFS-based server on page 171</a>
Decrease the number of days to retain logs	<a href="#">step 2</a>

- 2 Log in to the CBM 850 and access the Logroute commissioning tool:

**logroute**

*Example response:*

```

Logroute                               Main Menu
                                         1 - Device List
                                         2 - Global Parameters
                                         3 - CM Configuration File
                                         4 - Gdd Configuration
  
```

```
5 - Help
6 - Quit Logroute
Enter Option ==>
```

**3** Access the GDD configuration menu:

**4**

*Example response:*

```
GDD Menu
1 - Number of days to keep log files in /gdd :30
2 - Help
3 - Return to Main Menu
Enter Option ==>
```

**4** Enter the option number for the number of days to keep log files in /gdd:

**Enter Option ==> 1**

**5** Enter the number of days to retain the log files:

**Enter number of days(range - 1 To 30) ==>**

**6** Confirm to save the changes by entering "y":

**Save GDD Value [Y/N] [N] :- Y**

*Example response:*

Warning: This would change the number of days to store logsin/gdd. Logfiles older than the day specified would be deleted.

Press the Enter key to acknowledge that the data was saved.

Example response

Save data completed -- press return to continue

**7** Press the Enter key to acknowledge that the data was saved.

**8** You have completed this procedure.

---

## Clearing a major Heartbeat alarm

---

### Application

Use this procedure to clear a major Heartbeat alarm on the CBM.

### Indication

At the net level of the cbm mtc display, the Core Heartbeat State indicates a SysB condition.

### Meaning

The CBM is not receiving responses from the Core.

### Impact

If the CBM is unable to communicate with the Core, the applications will also be unable to communicate with the Core.

### Action

#### Clearing a major Heartbeat alarm

##### *At the CBM*

- 1 Verify that the CBM Ethernet interface is in service.  
See [SSPFS / Sun Netra 240 services fault clearing procedures on page 9](#) for the procedure used to clear the fault.
- 2 Verify that the Core Ethernet interface is in service.  
Search the "North America - DMS" document collection (for North American Carrier Voice over IP networks) or "International DMS Global Services Platform" document collection (for International Carrier Voice over IP networks) in Helmsman for the appropriate procedures to use to clear this fault.
- 3 Verify that Ethernet packets are routed properly between the CBM and Core interfaces.  
Search the "North America - DMS" document collection (for North American Carrier Voice over IP networks) or "International DMS Global Services Platform" document collection (for International Carrier Voice over IP networks) in Helmsman for the appropriate procedures to use to clear this fault.



## Replacing a failed power supply

---

### Application

Use the following procedure to replace a power supply on a CBM server.

### Action

The power supply is a field replaceable unit (FRU). It can be replaced while the server is powered up and in-service.

#### Replacing a power supply on a CBM server

- 1 Refer to the manufacturer documentation for the procedure on how to replace the power supply.
- 2 You have completed this procedure.



---

## Replacing failed Ethernet interfaces

---

### Purpose

Use the following procedures to replace a failed Ethernet interface.

### Application

The Ethernet interface is not a field replaceable unit. The server must be put out of service and powered down before hardware can be removed from the shelf.

**Note:** Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or \$, displayed by the system through a GUI or on a command line.

### Action

#### Replacing failed Ethernet interfaces

##### *At the CBM*

- 1 Record the stream\_name for the stream you wish to busy as determined in the procedure "Preparing for SBA installation and configuration" in the *Accounting* NTP for your core manager.
- 2 Access the SDMBIL level:  

```
mapci;mtc;appl;sdbil;post <stream_name>
```

where  

```
<stream_name>
```

is the stream name value determined in [step 1](#).
- 3 Busy the stream at the SDMBIL level by typing:  

```
bsy
```
- 4 Proceed with busying the stream by typing:  

```
y
```
- 5 Ensure that the stream is in Backup mode by verifying the state is indicated as ManB by typing:  

```
mapci;mtc;appl;sdbil;post <stream_name>
```

where  

```
<stream_name>
```

is the stream name value determined in [step 1](#).
- 6 Follow the procedure "Sending billing files from disk" in the *Accounting* NTP for your core manager.

- 7 Go to the appl level of the cbmmtc tool by typing:

**cbmmtc appl**

*Example response:*

```

Group: CBM                               State: ISTb
# Application                               State
1 Generic Data Delivery                    .
2 DMS Maintenance Application              .
3 GR740 Pass Through                       OffL
4 FTP Proxy                                .
5 Log Delivery Service                     Fail
6 Passport Log Streamer                    OffL
7 Table Access Service                     .
8 OM Access Service                        .
9 Reach Through SPM                        .
10 OM Delivery                             .
                                           Applications showing: 1 to 10 of 15

```

- 8 Manually busy all the applications by entering:

**bsy group**

- 9 Confirm the BUSY operation:

**y**

*Example response:*

```

15      Bsy GROUP: The GROUP is in service.
16      This command will cause a service interruption.
17 Help  Do you wish to proceed?
18 Refresh Please confirm ("YES", "Y", "NO", or "N")

```

- 10 Offline each application by entering:

**offl <application number 1><application number 2><.....>**

**Note:** Application numbers are separated by spaces if multiple applications are expected to be offlined.

- 11 Offline the CBM group by entering:

**offl group**

### ***At the shelf***

- 12 Follow the procedure "Shutting down an SSPFS-based server" in *ATM/IP Solution-level Security and Administration*, NN10403-900.
- 13 Remove and replace the CBM server by following instructions provided by the hardware manufacturer.

**Note:** Remove both disk drives from the server being replaced and place them in the replacement server.

- 14 To bring the server back up, turn on the power to the server at the circuit breaker panel of the frame.

### At the CBM

- 15 Go to the appl level of the cbmmtc tool by typing:

**cbmmtc appl**

*Example response:*

```

Group: CBM                               State: ISTb
# Application                             State
1 Generic Data Delivery                   .
2 DMS Maintenance Application             .
3 GR740 Pass Through                      offL
4 FTP Proxy                               .
5 Log Delivery Service                   Fail
6 Passport Log Streamer                  SysB
7 Table Access Service                   .
8 OM Access Service                      .
9 Reach Through SPM                      .
10 OM Delivery                           .
                                           Applications showing: 1 to 10 of 15

```

- 16 Proceed depending on the state of the application. If the CBM group state is Offl go to [step 17](#); otherwise, go to [step 19](#).

- 17 Manually busy all the applications by entering:

**bsy group**

- 18 Confirm the BUSY operation:

**y**

- 19 Proceed depending on the state of the application. If the applications you want to RTS are in the Offline state, go to [step 20](#); otherwise, go to [step 21](#).

- 20 Manually busy all the applications which are in the Offl state:

**bsy <application number 1><application number 2><.....>**

**Note 1:** The Bsy command can take multiple application numbers, each separated by a space, to manually busy multiple applications at the same time.

**Note 2:** Do not apply the Bsy command to the applications you do not want to RTS.

- 21 If the CBM group state is in ManB state, go to [step 22](#); otherwise, go to [step 23](#).

- 22**    RTS all the applications which are in the ManB state by typing:  
**rts group**  
Go to [step 24](#).
- 23**    RTS each application by typing:  
**rts <application number 1><application number 2><.....>**
- 24**    Ensure that the stream is in Recovery mode by verifying the state is indicated as Rcvy by typing:  
**mapci;mtc;appl;sdbil;post <stream\_name>**  
where  
    **<stream\_name>**  
    is the stream name value determined in [step 1](#).
- Note 1:** Rcvy indicates that the stream is in-service and also sending previously created backup files to the CS2000 Core Manager.
- Note 2:** The state may also be InSv, which indicates that the stream is in a normal working state if recovery has already completed.
- 25**    Clear any application and system alarms if they are present.
- 26**    You have completed this procedure.

## Accessing TCP and TCP-IN log devices from a remote location

### Purpose

Use this procedure to access TCP and TCP-IN devices, from a remote location.

### Application

The TCP and TCP-In log devices can be accessed from either a local, or a remote location (console). The following procedures describe how to access these log devices from a remote location. These procedures can be used when you are performing the related procedures listed in the table [Remote access to log devices procedures on page 39](#).

### Remote access to log devices procedures

Log device	Procedure	Applies to
TCP	Accessing a TCP device from a remote location	“Configuring a core manager for log delivery” in the Configuration Management document  <a href="#">Displaying or storing log records using logreceiver on page 61</a>
TCP-IN	Accessing a TCP-IN device from a remote location	“Configuring a core manager for log delivery” in the Configuration Management document  “Deleting a device using logroute” in the Configuration Management document

**Note:** Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or \$, displayed by the system through a GUI or on a command line.

## Procedure

### Accessing a TCP device from a remote location

#### *At the remote workstation*

- 1 Start the logreceiver tool:

```
logreceiver <port_number>
```

where:

**<port\_number>**

is the port number used for the TCP device on the core manager

- 2 Continue with the desired procedure listed in the table [Remote access to log devices procedures on page 39](#).
- 3 You have completed this procedure.

### Accessing a TCP-IN device from a remote location

#### *At the remote workstation*

- 1 Use telnet to access the core manager:

```
telnet <ip_address> <port_number>
```

where:

**<ip\_address>**

is the address of the core manager

**<port\_number>**

is the number of the port of the device on the core manager

- 2 Log into the core manager either as maint or admin.
- 3 Start the logroute tool:  

```
logroute
```
- 4 Continue with the desired procedure from the table [Remote access to log devices procedures on page 39](#).
- 5 You have completed this procedure.

---

## SBA alarm troubleshooting

---

### Purpose

In the SBA environment, there are many conditions that can cause an alarm to be raised. While there is a log message associated with each alarm, the information that is supplied is not always enough to determine what raised the alarm.

**Note:** When alarms related to a filtered stream are sent to the CM, they are sent under the name of the associated CM billing stream. When this occurs, the name of the filtered stream is prepended to the text of the alarm.

### Application

The majority of the alarms raised on the SBA system that you can resolve can be traced back to one of two problem areas:

- a problem in the FTP process
- an insufficient amount of storage

#### A problem in the FTP process

If you receive numerous FTP and LODSK alarms, this can indicate a problem with either the SBA or the general FTP process on the core manager. LODSK generally indicates that your primary files (closedNotSent) are not being moved from the core manager to the downstream processor. Review any accompanying logs.

The downstream processor can be full with no space to write files to, which can cause an FTP error. When this happens, you see core SDMB logs, which indicate that the file is not sent. In addition, if you do not receive an FTP alarm, it is possible that scheduling is turned off, which prevents FTP alarms from being sent.

#### Insufficient amount of storage

If you receive numerous alarms for the backup system without receiving an FTP or LODSK alarm, this indicates a communication problem. The core is not communicating with the core manager.

Use the following procedures to clear alarms based on the FTP process:

- [Verifying the file transfer protocol on page 144](#)
- [Verifying the FTP Schedule on page 151](#)

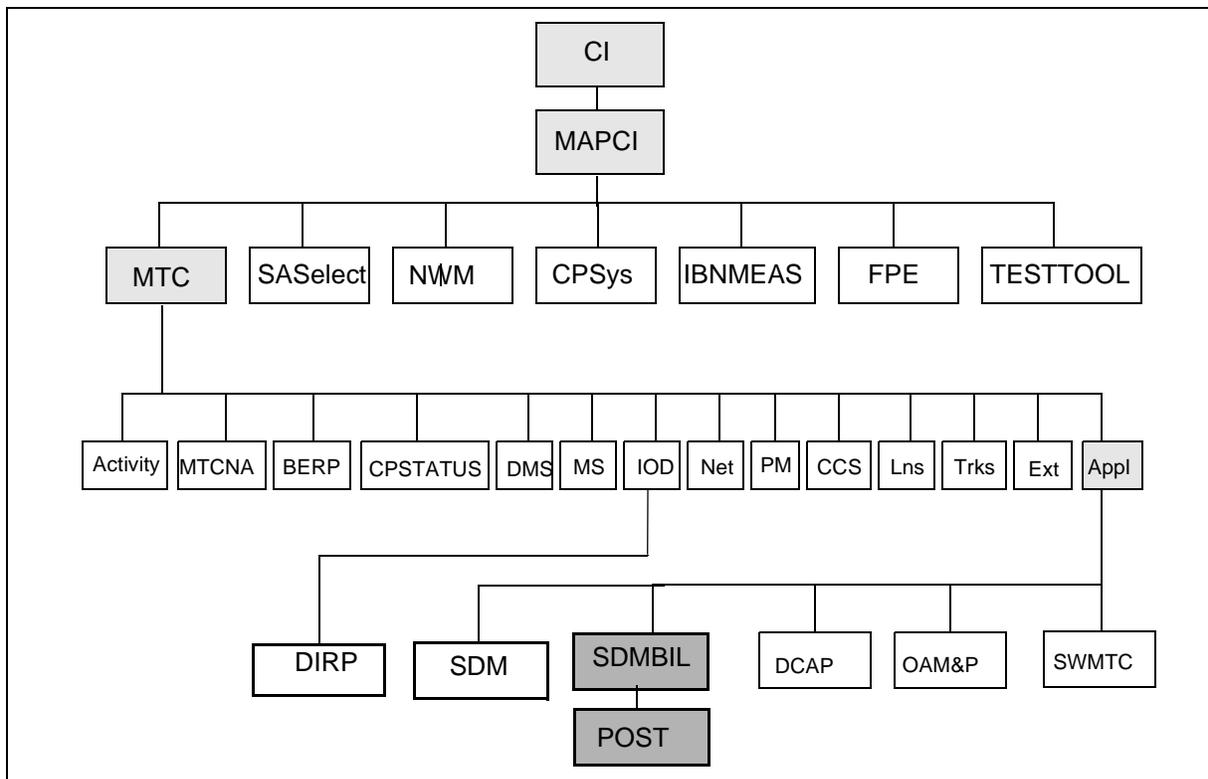
Use the following procedures to clear alarms based on communication problems between the core and the core manager:

- [Clearing a DSKWR alarm on a CBM on page 99](#)
- [Clearing a NOCOM alarm](#) (Applicable to the CS 2000 Core Manager and the Core and Billing Manager 800)
- [Clearing a major SBACP alarm on page 136](#)
- [Clearing a minor SBACP alarm on page 139](#)

## APPL Menu level alarms

Because SBA processing takes place in both the CM and the core manager environment, the SBA program displays core manager-generated alarms in the MAPCI;MTC window at the CM. The figure [Alarms layout](#) shows the SBA alarms that are displayed under the APPL Menu level at the MAPCI;MTC level on the CM side.

### Alarms layout



## Maintenance for SBA

Maintenance for SBA on the CM side centers around the following entities:

- table SDMBILL
- MAP level SDMBIL
- logs
- states
- alarms

Maintenance for SBA on the core manager side is performed using the interface on the SBA RMI. For example, you perform maintenance on the core manager side of SBA by using commands in the billing level (billmtc) of the core manager RMI display.

You can also display the alarms raised by the core manager side for the SBA by using the DispAl command from the billmtc level. The DispAl command displays the alarm criticality, stream, and text of the alarms.

## Alarm severity

There are three levels of severity for SBA alarms:

- Critical:  
a severe problem with the system that requires intervention
- Major:  
a serious situation that can require intervention
- Minor:  
a minor problem that deserves investigation to prevent it from evolving to a major problem

When multiple alarms are raised, the alarm with the highest severity is the one displayed under the SDM header of the MAP banner. If multiple alarms of the same severity (for example, critical) are raised, the first alarm that is raised is the one displayed under the SDM header of the MAP banner. For example, if a NOBAK critical alarm is raised before a NOSTOR critical alarm, the NOBAK alarm is the one that is displayed. Use the DispAl command to view all outstanding alarms, and use the associated procedure to clear each outstanding alarm.

## CM MAP states

In the SBA environment, an SBA stream can have different state values due to some action or condition on the SBA system. You can view the state of a stream from the CM by entering:

```
mapci;mtc;appl;sdbil;post <stream_name>
```

*where*

**<stream\_name>** is the name of the stream

The possible state values and their definition are as follows:

- Offline pending (OffP):  
the stream has been turned off and is waiting for the core manager to complete processing its data
- Offline (OffL):  
the stream is offline
- Manual busy (ManB):  
the stream has been manually busied by a user from the CM; data is being written to backup files
- System busy (SysB):  
the stream has been busied by the SBA system due to a communications or internal software error; data is being written to backup files
- Remote busy (RBsy):  
the stream has been busied by the SBA system due to a communications or internal software error; data is being written to backup files
- Backup (Bkup):  
the stream is writing data to backup files due to performance and communication problems
- Recovery (Rcvy):  
the stream is in service and is also sending backup files previously created to the core manager
- In-service (InSv):  
the stream is in a normal working state
-

## Common procedures

There are a few procedures that are common to all of the alarm clearing procedures. These common procedures include the following:

- [Verifying the file transfer protocol on page 144](#) helps you determine that the FTP process is configured correctly and is able to transfer files
- [Verifying the FTP Schedule on page 151](#) helps you determine that the system is able to send FTP files on a regular basis
- “Configuring SBA backup volumes on the core” in the core manager Accounting document is used to create and activate alternative backup volumes for a stream

Use the following procedures to clear alarms based on insufficient storage capacity:

- [Clearing a BAK50 alarm on page 79](#)
- [Clearing a BAK70 alarm on page 83](#)
- [Clearing a BAK90 alarm on page 87](#)
- [Clearing a BAKUP alarm on page 91](#)
- [Clearing a NOBAK alarm on page 112](#)
- [Clearing a NOREC alarm on page 121](#)
- [Clearing a NOSTOR alarm on page 123](#)
- [Clearing a NOVOL alarm on page 127](#)

## Accessing the MATE

### Purpose

Use this procedure to access the MATE.

### Procedure

Use the following procedure to access the MATE.

**Note:** Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or \$, displayed by the system through a GUI or on a command line.

#### Accessing the MATE

**At the workstation UNIX prompt or VT-100 terminal prompt:**

- 1 Log onto the CBM.
- 2 Get the current hostname by entering:

**GetCurrentHostName**

*Example response:*

<CBM hostname>-<unit0 / unit1>

- 3 Access the Report Registration Menu:

If	Then
the hostname returned in <a href="#">step 2</a> contains "unit0"	the MATE hostname is "unit1"
the hostname returned in <a href="#">step 2</a> contains "unit1"	the MATE hostname is "unit0"

- 4 Determine if the MATE is running by entering:

**ping <mate hostname>**

**Note:** The <mate hostname> is the one determined in [step 3](#).

- 5

If	Do
<a href="#">step 4</a> indicates the MATE is Active	<a href="#">step 6</a>
otherwise	<a href="#">step 8</a>

- 6 Access the MATE using SSH by typing:

```
ssh root@ <mate hostname>
```

where

**Note:** You can log into the MATE without a password. To exit the MATE, type > exit to return to the local system.

- 7 You have completed this procedure.
- 8 You need to access the MATE through a local VT100 terminal.

---

## Clearing the MATE alarm

---

### Purpose

Use this procedure to clear the MATE alarm.

**Note:** Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or \$, displayed by the system through a GUI or on a command line.

### Procedure

Use the following procedure to clear the MATE alarm.

**At the workstation UNIX prompt or VT-100 terminal prompt:**

- 1 Log onto the CBM.
- 2 Start the cbmmtc tool by typing:

**cbmmtc**

**Note:** Check the MATE column on the banner. If the state is not "." (dot), this indicates the presence of an alarm.

- 3 Access the MATE by performing the procedure [Accessing the MATE on page 46](#).
- 4 Clear the alarms by performing the procedure [Clearing a CBM application alarm on page 24](#).
- 5 Log out of the MATE.
- 6 You have completed this procedure.



---

## Displaying SBA log reports

---

### Purpose

Use this procedure to display the current logs raised by the core manager for the SuperNode Billing application (SBA) that have not been acknowledged by the Core.

### Application

The MIB parameter “sendBillingLogsToCM” affects the displogs command.

The displogs command does not display logs generated by the Core.

### Prerequisites

#### Logging on to the CS 2000 Core Manager

You must be a user authorized to perform fault-admin actions in order to perform this procedure.

For information on how to log in to the CS 2000 Core Manager as an authorized user or how to display other information about a user or role group, review the procedures in the following table.

Procedure	Document
Logging in to the CS 2000 Core Manager	<i>CS 2000 Core Manager Security and Administration</i> , NN10170-611
Displaying information about a user or role group	<i>CS 2000 Core Manager Security and Administration</i> , NN10170-611

#### Logging on to the Core and Billing Manager 850

You must have the root user ID and password to log into the server.

**Note:** Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or \$, displayed by the system through a GUI or on a command line.

## Procedure

### Displaying SBA logs

#### *At any workstation or console*

- 1 Log into the core manager. Refer to [Prerequisites](#) for details.
- 2 Access the billing maintenance interface:

```
billmtc
```

- 3 Display the logs:

```
displogs
```

The logs are displayed in the format of name, number, event type, alarm status, label, and body. If there are no logs to display, the message `No unsent logs` is displayed.

- 4 You have completed this procedure.

## Displaying SBA alarms

### Purpose

Use this procedure to display the current alarms raised by the core manager for the SuperNode Billing application (SBA).

### Application

The MAP CI displays the status (critical, major, minor), the stream, and the text of the alarm.

This command displays alarms that have not been sent to the computing module (CM). However, the dispal command does not display Core-side alarms, such as the BAK50, BAK70, BAK90, NOBAK, NOSTOR, and BAKUP alarms.

### Prerequisites

#### Logging on to the CS 2000 Core Manager

You must be a user authorized to perform fault-admin actions in order to perform this procedure.

For information on how to log in to the CS 2000 Core Manager as an authorized user or how to display other information about a user or role group, review the procedures in the following table.

Procedure	Document
Logging in to the CS 2000 Core Manager	<i>CS 2000 Core Manager Security and Administration</i> , NN10170-611
Displaying information about a user or role group	<i>CS 2000 Core Manager Security and Administration</i> , NN10170-611

#### Logging on to the Core and Billing Manager 850

You must have the root user ID and password to log into the server.

**Note:** Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or \$, displayed by the system through a GUI or on a command line.

## Procedure

### Displaying SBA alarms

#### *At any workstation or console*

- 1 Log into the core manager. Refer to [Prerequisites](#) for details.
- 2 Access the billing maintenance interface:

```
billmtc
```

- 3 Display the alarms:

```
dispal
```

The alarms are displayed in the format of alarm status (critical, major, minor), stream, alarm short text, and alarm long text. If there are no alarms to display, the message, "No alarms" is displayed.

- 4 You have completed this procedure.

---

## Collecting DEBUG information using the CBMGATHER command

---

### Purpose

Use this procedure to collect DEBUG information from the core manager.

### Application

Use either of these procedures to collect the following DEBUG information from the core manager:

- the output of `cbmgather`
- the content of `/var/adm` directory

It is important to collect DEBUG information from the system in case of a failure (before recovery). The information assists in discovering the root cause of the problem and in preventing similar problems in the future.

**Note:** Instructions for entering commands in the following procedure do not show the prompting symbol, such as `#`, `>`, or `$`, displayed by the system through a GUI or on a command line.

### Procedure

#### *At the core manager command line (UNIX prompt) of the active node*

- 1 Run the utility to collect the output:

```
cbmgather
```

The output file from this command is located under `/var/adm` and has a name in the format:

```
cbmgather_<machine>_<date_and_time>.tar.Z
```

#### **Example**

```
/var/adm/cbmgather_hadry2_20050221141300.tar.Z
```

- 2 Tar and compress the content of directory `/var/adm`:

```
cd /var/adm
```

```
tar cvf varadm_active.tar *.day* *.log
```

```
compress varadm_active.tar
```

The output of the compressed tar file in the example is called `varadm_active.tar.Z`.

- 3 Move the files generated by commands executed in steps [1](#) and [2](#) out the system to a secure location using FTP (in BINary mode).

- 4 Remove the gathered output/files from the system:

```
rm -f
/var/adm/cbmgather_<machine>_<date_and_time>
.tar.Z
```

**Note:** The command shown above is entered on a single line. When entering the command, ensure that there is a single space between -f and /var, and that there is no space between time> and .tar.

```
rm -f /varadm_active.tar.Z
```

If	Do
your system is a CBM 850 cluster configuration	<a href="#">step 5</a>
your system is not a CBM 850 cluster configuration	<a href="#">step 9</a>

**At the core manager command line (UNIX prompt) of the inactive node**

- 5 Run the utility to collect the output:

```
cbmgather
```

- 6 Tar and compress the content of directory /var/adm:

```
cd /var/adm
tar cvf varadm_inactive.tar *.day* *.log
compress varadm_inactive.tar
```

*Example response:*

The output of the compressed tar file in the example is called varadm\_inactive.tar.Z.

- 7 Move the files generated by commands executed in steps [5](#) and [6](#) out the system to a secure location using FTP (in BINary mode).

- 8 Remove the gathered output/files from the system:

```
rm -f
/var/adm/cbmgather_<machine>_<date_and_time>
.tar.Z
```

**Note:** The command shown above is entered on a single line. When entering the command, ensure that there is a single

space between -f and /var, and that there is no space between time> and .tar.

```
rm -f /varadm_inactive.tar.Z
```

- 9** You have completed this procedure.

## Controlling the SDM Billing Application

### Purpose

Use the following procedure to busy the SDM Billing Application (SBA) or return the SBA to service.

### Prerequisites

You must establish communications between the core manager and the core for SBA to run successfully.

**Note:** Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or \$, displayed by the system through a GUI or on a command line.

### Procedure

#### *At any workstation or console*

- 1 Log in to the CBM.
- 2 Access the Application level:

```
cbmmtc appl
```

The system displays a list of applications.

**Note:** Use the up and down commands to scroll through the list of applications.

If you want to	Do
busy the SBA	<a href="#">step 3</a>
return the SBA to service	<a href="#">step 5</a>

3

	<p><b>CAUTION</b></p> <p>Busying the SBA causes SBA to go into backup mode, and triggers an SBACP (major) alarm under the SDMBIL banner at the MAP terminal.</p>
---	--

Busy the SDM Billing Application:

```
bsy <x>
```

*where:*

<x>

is the number next to the CBM Billing Application

*Example response:*

```
The application is in service.
This command will cause a service interruption.
Do you wish to proceed?
Please confirm ("YES", "Y", "NO", or "N"):
```

**4** Confirm the busy command:

**y**

If the SBA	Do
busied successfully and you want to return the SBA to service	<a href="#">step 5</a>
busied successfully but you do not want to return the SBA to service at this time	<a href="#">step 13</a>
did not busy successfully	contact your next level of support

**5** Return the CBM Billing Application to service:

**rts <x>**

where:

<x>

is the number next to the CBM Billing Application

**Note 1:** This command causes SBA streams to go into a recovery mode.

**Note 2:** Any streams configured for real-time billing (RTB) are also returned to service. Log report SDMB375 is generated when a stream configured for RTB fails to return to service.

If the SBA	Do
returned to service successfully	<a href="#">step 6</a>
did not return to service successfully	contact your next level of support

- 6 Determine if log SDMB375 was generated.

If the system	Do
generates log SDMB375	<a href="#">step 7</a>
does not generate log SDMB375	you have completed this procedure

- 7 Return the RTB streams to service. Exit the Application level:

**quit all**

- 8 Access the billing maintenance level:

**billmtc**

- 9 Access the schedule level:

**schedule**

- 10 Access the real-time billing level:

**rtb**

- 11 Busy the stream:

**bsy <stream name>**

*where:*

**<stream name>**

is the name of the billing stream configured for RTB (for example OCC)

- 12 Return the stream to service:

**rts <stream name>**

*where:*

**<stream name>**

is the name of the billing stream configured for RTB (for example OCC)

If the billing stream configured for RTB	Do
returns to service successfully	<a href="#">step 13</a>
does not return to service successfully	contact your next level of support

- 13 Quit the billing maintenance level:

**quit all**

**14** You have completed this procedure

---

## Displaying or storing log records using logreceiver

---

### Purpose

Use this procedure to display or store log records on a workstation using the logreceiver tool.

### Application

The commands that you enter to display or store log records on a workstation must include a port number. The port number must be the same as the port number used to configure the TCP device on the core manager. The port number must not be used for any other purpose on the workstation, otherwise the following error message appears:

```
Failed to listen for connection request on port
<port_number>, exiting
```

You must change the port number used to configure the TCP device on the core manager.

### Storage file

If the storage file does not exist, it is created automatically. The logs from the core manager are stored in this file.

If the file exists, the logs from the core manager are added to it provided its UNIX access permissions allow writing to the file. In either case, a message 'Accepted connection request from host <hostname>' is displayed on the screen just before the first log received is written to the file. Press ctrl -c and press the Enter key to terminate execution of the logreceiver tool.

If the file exists, but its permissions do not allow writing to it, an error message 'Failed to open <filename>' displays on the screen. Press ctrl -c, and press the Enter key to terminate execution of the logreceiver tool.

The file continues to fill up until either the logreceiver execution terminates or all free storage in the file system is exhausted. In the latter case, the logreceiver execution terminates automatically. The error message 'Failed to open <filename>' displays on the screen and you must remove the file or free up some storage.

**Note:** Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or \$, displayed by the system through a GUI or on a command line.

## Procedure

### Checking the port numbers in use on a workstation

#### *At the client workstation*

- 1 Check the port numbers in use:

```
more/etc/services
```

The list of port numbers in use is displayed. Scroll through the display by pressing the Enter key again.

### Storing logs in a file

#### *At the client workstation*

- 1 Start the logreceiver tool to store logs in a file:

```
logreceiver <port> -f <filename>
```

*where*

**<port>** is the port number used when configuring the TCP device on the core manager

**<filename>** is the name of the file

### Displaying log records on a workstation

#### *At the client workstation*

- 1 Start the logreceiver tool to display the log records on the screen:

```
logreceiver <port>
```

*where*

**<port>** is the port number used when configuring the TCP device on the core manager

- 2 You have completed this procedure.

---

## Retrieving and viewing log records

---

### Purpose

Use this procedure to retrieve and view CM and core manager log records using the core manager log query tool.

### Application

When you enter the log query tool, the system automatically displays the log records using the following default settings:

- log type: all
- format: std
- date: current date
- time: midnight of current date
- display of log records: page by page
- arrangement of logs displayed: show latest log first

**Note:** Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or \$, displayed by the system through a GUI or on a command line.

### Procedure

#### Retrieving and viewing logs

*At a terminal or terminal session connected to the core manager*

- 1 Log into the core manager.

- 2 Start the log query tool using the default settings:

**logquery**

*Example response:*

```

                                SDM Log Query
Category: CUSTLOG                Type: ALL
RTEC02CR   C7UP105 MAR12 14:58:55 7365 INFO UNSUCCESSFUL CALL ATTEMPT
          CKT RLGHNCECBDS1LSA   10
          REPORTED BY CKT RLGHNCECBDS1LSA   10
          REASON = UNALLOCATED NUMBER
          ROUTESET = EC_B_RS
          CLDNO =                 3579972019

RTEC02CR   * BOOT201 MAR12 14:58:44 7364 INFO Bootp log report
Mac Address : 006038381f87
          MAC addr to node_id lookup failure : 13
          INM permission to boot failure   : 0
          Core IP address lookup failure   : 0
          SEND_UDP_MSG failure             : 0

RTEC02CR   * BOOT201 MAR12 14:58:44 7363 INFO Bootp log report
Mac Address : 52415320c011
          MAC addr to node_id lookup failure : 19
          INM permission to boot failure   : 0
[Warning: log too big for screen; truncated...]

Command:
```

- 3 Access a list of available parameters and variables to view logs:  
**logquery -help**
- 4 Enter the applicable command.
- 5 When you are finished, exit the log query tool:  
**quit**
- 6 You have completed this procedure.

## Troubleshooting AFT alarms

### Purpose

Use this procedure to clear alarms generated by the Automatic File Transfer (AFT) application.

### Application

Use the following procedures to resolve AFT alarms that are specific to the SuperNode Billing Application (SBA).

**Note:** Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or \$, displayed by the system through a GUI or on a command line.

### Indication

At the SDBIL level of the MAP, "AFT" and the alarm level indicators for critical (\*C\*) and major (M) alarms appear in the alarm banner under the SDBIL header.

### Meaning

An AFT alarm is generated under the conditions listed in the table [AFT alarms](#).

#### AFT alarms

Alarm	Occurs when:
Critical (*C*)	<ul style="list-style-type: none"><li>an AFT session network connection has been disrupted during file transfer</li><li>the retry count has been exceeded on a file</li><li>the message transfer protocol (MTP) timer has expired</li></ul>
Major (M)	an AFT session has been stopped using the AFT level Stop command

### Impact

When conditions exist for a critical or major AFT alarm, billing records are not being transferred to the downstream collector.

### Procedure

This section describes the methods for clearing critical and major AFT alarms.

### Clearing critical alarms

To clear a critical alarm, use one of the following methods:

- correct the network connection disruption
- manually clear the alarm through the Alarm command at the AFT level of the BILLMTC remote maintenance interface (RMI)
- delete the AFT session

Critical alarms also are cleared when the network connection disruption is corrected.

### Clearing major alarms

To clear a major alarm, use one of the following methods:

- restart the session using the Start the command available at the AFT level of the BILLMTC RMI
- manually clear the alarm through the Alarm command available at the AT level of the BILLMTC RMI
- delete the tuple from the automaticFileTransferTable table

### Procedure

Use the following procedure to clear an AFT alarm manually.

#### Clearing an AFT alarm manually

##### *At the core manager*

- 1 Access the BILLMTC level:  
**billmtc**
- 2 Access the Application (APPL) level:  
**appl**
- 3 Access the Automatic File Transfer (AFT) level:  
**aft**
- 4 Clear the alarm:  
**alarm cancel <session\_name>**

*where:*

**<session\_name>** is the unique name of the network connection for which you want to clear the alarm

*Example response:*

```
*** WARNING: Alarm(s) will be cancelled for AFT
session <session_name> Do you want to continue?
(Yes or No)
```

- 5 To cancel the alarms, enter:

**yes**

*Example response:*

```
Cancelled alarms for AFT session:
<session_name>
```

- 6 You have completed this procedure.

### Deleting a tuple from automaticFileTransferTable



#### CAUTION

An AFT session must be stopped before it can be deleted. When an AFT tuple is deleted, billing files are no longer being transferred downstream.

#### *At the core manager*

- 1 Access the BILLMTC level:  
**billmtc**
- 2 Access the APPL level:  
**appl**
- 3 Access the AFT level:  
**aft**
- 4 Access the AFTCONFIG level:  
**aftconfig**

- 5 Delete the tuple from the automaticFileTransferTable:  
**delete <session\_name>**  
*where:*  
    **<session\_name>** is the unique name of the network connection that generated the alarm  
*Example response:*  
\*\*\* WARNING: Alarm(s) will be cancelled for AFT session <session\_name> Do you want to continue? (Yes or No)
- 6 To delete the table entry (tuple), enter:  
**yes**  
*Example response:*  
Deleted table entry for AFT session:  
<session\_name>
- 7 You have completed this procedure.

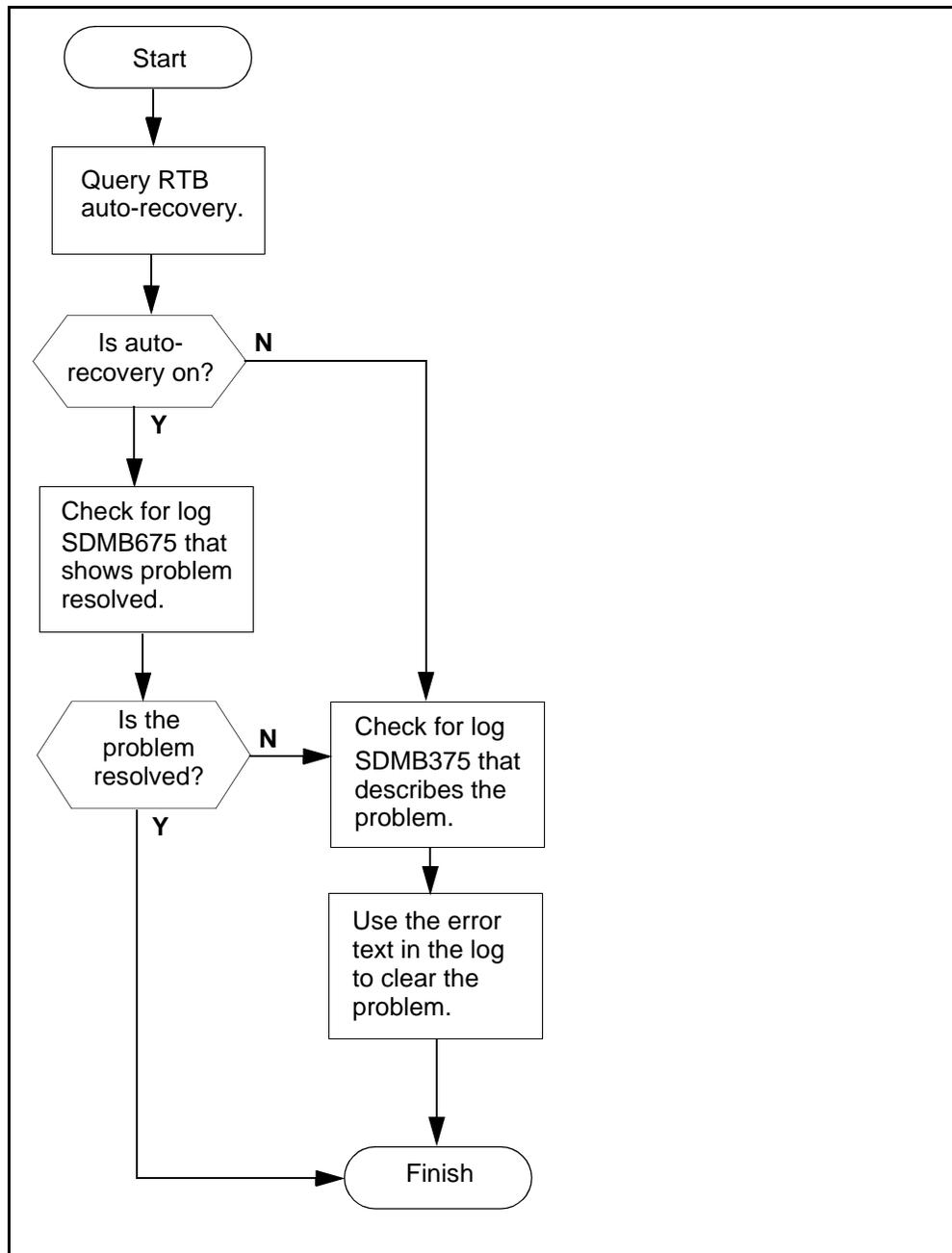
### Restarting an AFT session

#### *At the core manager*

- 1 Access the BILLMTC level:  
**billmtc**
- 2 Access the APPL level:  
**appl**
- 3 Access the AFT level:  
**aft**
- 4 Restart the AFT session that generated the alarm:  
**start <session\_name>**  
*where:*  
    **<session\_name>** is the unique name of the network connection that generated the alarm  
*Example response:*  
\*\*\* WARNING: Started AFT session:  
<session\_name>
- 5 You have completed this procedure.

## Troubleshooting RTB problems

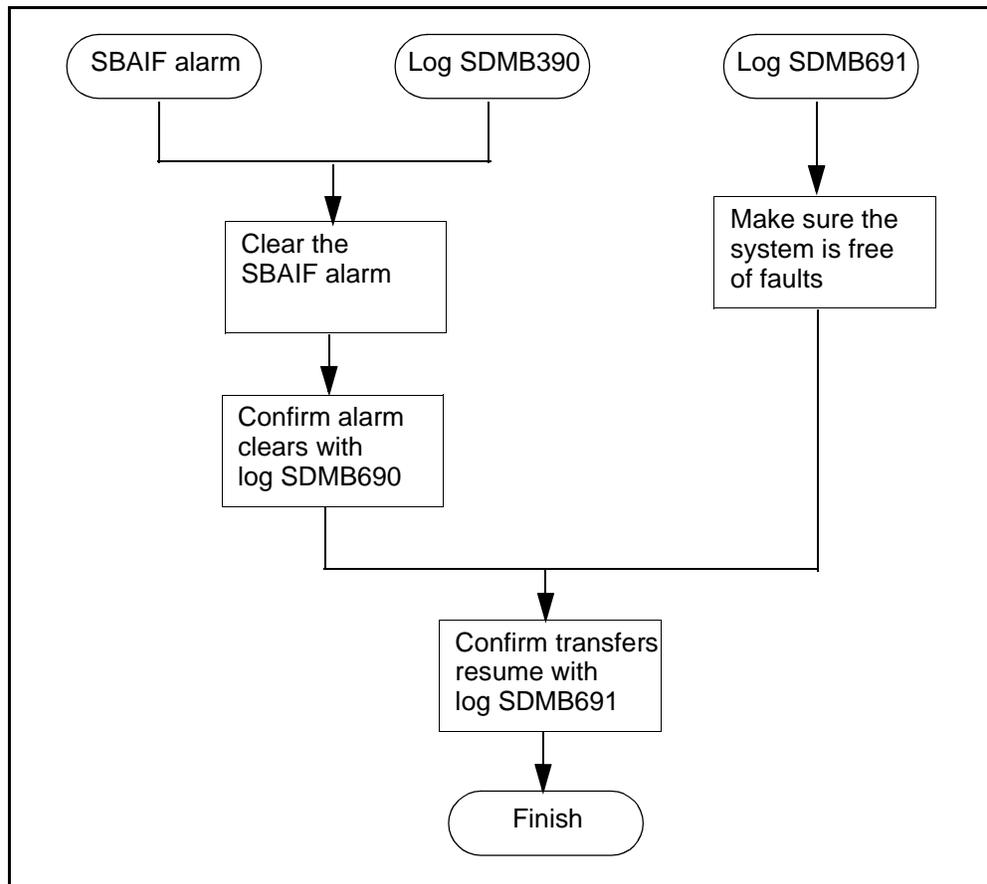
Use the following flowchart, and the procedures in your documentation for this product, to troubleshoot problems related to real time billing (RTB).





## Troubleshooting problems with scheduled billing file transfers

Use the following flowchart, and the procedures in your product documentation, to troubleshoot problems related to the scheduled transfer of billing files from the core manager to a downstream destination.



**Note:** The length of time for the SuperNode Billing Application (SBA) to resume transferring billing files depends on the following configured parameters:

- the number of active scheduled tuples
- the time interval to transfer files



---

## Troubleshooting Log Delivery problems on a CBM

---

### Purpose

Use the procedure to:

- troubleshoot the ISTb state of the log delivery application
- isolate and clear faults
- change the state of the log delivery application from ISTb to InSv

**Note:** Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or \$, displayed by the system through a GUI or on a command line.

### Fault conditions affecting Log Delivery

#### Lost logs

When the system detects that logs are being lost, an internal report indicating the number of logs lost is sent to all client output devices.

To clear the problem:

- 1 Access the Log Delivery commissioning tool
- 2 Select the Global Parameters menu, and
- 3 Increase the buffer size

Refer to procedure “Configuring Log Delivery global parameters” in the CBM Configuration Management document.

#### No logs being received at a Log Delivery client

If no logs are being received at a Log Delivery client, do the following at the Device List menu of the Log Delivery commissioning tool:

- verify that the client is defined
- verify that the log stream for the client is defined

Refer to procedure “Modifying a log device using logroute” in the CBM Configuration Management document.

### Logs not formatted properly

If the log reports at a Log Delivery client device are not formatted correctly, access the Log Delivery commissioning tool and check the following:

- at the Device menu, verify that the correct log format has been commissioned for the device (STD, SCC2, STD\_OLD, SCC2\_OLD)
- at the Global Parameters menu, check that the parameters for start and end of line, and start and end of log, are set correctly.

For more information, refer to procedure “Modifying a log device using logroute” in the CBM Configuration Management document.

### Log devices on the computing module are full

If a CBM cannot detect computing module (CM) logs, it is possible that there are no free log devices on the CM. In the event that all the log devices on the CM are full, the Log Delivery application generates an alarm. The application state changes to ISTb, and generates an SDM303 log at the RMI.

The log delivery alarm can be cleared when any log device on the CM/Core is freed, and the Log Delivery application is manually busied and returned to service.

## Interval

Perform this procedure when the state of the log delivery application in the Apply menu level of the cbmmtc user interface is ISTb.

## Procedure

### Troubleshooting the log delivery application when its state is ISTb

#### *At the local or remote VT100 console*

- 1 Log into the CBM as the root user.
- 2 Access the maintenance interface:  
**cbmmtc**
- 3 Access the application level (Appl):  
**appl**

If GDD is	Do
Offl	<a href="#">step 4</a>
ManB	<a href="#">step 5</a>

If GDD is	Do
InSv	<a href="#">step 6</a>

- 4 Busy the GDD application:

```
bsy <fileset_number>
```

*where*

**<fileset\_number>**

is the number next to the GDD application

- 5 Return the GDD application to service:

```
rts <fileset_number>
```

*where*

**<fileset\_number>**

is the number next to the GDD application on the screen

**Note:** Wait at least one minute for the ISTb state to change to InSv.

If the Log Delivery application	Do
remains ISTb	<a href="#">step 6</a>
goes InSv	you have completed this procedure

- 6 Check the CBM for any faults:

```
querycbm flt
```

If	Do
a fault report indicates "log file is circulating (losing logs)"	<a href="#">step 7</a>
a fault report indicates "Core log device is not Configured"	<a href="#">step 20</a>
no fault report indicates "log file is circulating (losing logs)"	contact your next level of support

- 7 Exit the maintenance interface:

```
quit all
```

**Note:** You must be a root user of the CBM to continue with the procedure.

- 8 Access the /gdd directory:  
**cd /cbmdata/00/gdd**
- 9 Check all log files:  
**ls -l**
- 10 Determine if there are any files present that are not log files.

**Note:** Log files start with *LOGS.recorddata*.

If	Do
there are files present that do not start with LOGS.recorddata	<a href="#">step 11</a>
all files start with LOGS.recorddata	<a href="#">step 17</a>

- 11 Delete files that are not log files:  
**Note:** Once you remove the file, there is no way to restore it.

**rm <file>**

where

**<file>**

is the file in the /gdd directory that is not a log file.

- 12 Return to the maintenance interface:  
**cbmmtc**
- 13 Access the application level (Appl):  
**appl**
- 14 Determine if the state of the log delivery application is ISTb. Wait at least 1 min. for the ISTb state to change to InSv.

If the Log Delivery application	Do
remains ISTb	<a href="#">step 15</a>
goes InSv	you have completed this procedure

- 15 Exit the maintenance interface:  
**quit all**
- 16 Access the /gdd directory:  
**cd /cbmdata/00/gdd**

- 17 Check the log files:  
`ls -l`
- 18 Determine if the current log file (LOGS.recorddata) is much larger than the other log files.

If the current log file is	Do
larger than the other log files	contact your next level of support
the same size as the other log files	<a href="#">step 19</a>

- 19 Increase the size of the /cbmdata/00/gdd file system:
- Note:** Once you have increased the size of a file system, you cannot decrease it.
- ```
filesys grow -m /cbmdata/00/gdd -s <size>{m,g}
```
- where

**<size>**

is the size in megabytes (Mbytes) or gigabytes (g) by which you want to increase the current size of the file system

**Note 1:** Configure the size of the /cbmdata/00/gdd file system to be equal to the required capacity for 12 hours of log files, multiplied by 2 (for a 24 hour file size) then multiply the value by 50 days. This provides enough storage space to accommodate the required 30 days of log files, with excess capacity available.

**Example**

$3\text{Mb} \times 2 \times 50 \text{ days} = 300 \text{ Mb}$

where

300 Mb

is the average size of a 12 hour log file in the /gdd file system

**Note 2:** The default value for GDD is set for seven days. If needed, increase the value, but a corresponding increase in GDD size is required.

**At the MAP**

- 20** Verify that a log device on the core is available.

**logutil; listdevs**

If all 32 log devices are being used, free up one log device for the Log Delivery Service on the CBM to use.

For more information, refer to procedure “Deleting a log device using logroute” in the CBM Configuration Management document.

**At the local or remote VT100 console**

- 21** Busy the Log Delivery application:

**bsy <fileset\_number>**

*where*

**<fileset\_number>**

is the number next to the GDD application

- 22** Return the Log Delivery application to service:

**rts <fileset\_number>**

*where*

**<fileset\_number>**

is the number next to the GDD application

- 23** Determine if the state of the log delivery application is still ISTb. Wait at least 1 minute for the ISTb state to change to InSv.

| If the Log Delivery application | Do                                 |
|---------------------------------|------------------------------------|
| remains ISTb                    | contact your next level of support |
| goes InSv                       | <a href="#">step 24</a>            |

- 24** You have completed this procedure.

---

## Clearing a BAK50 alarm

---

### Purpose

Use this procedure to clear a BAK50 alarm.

### Indication

BAK50 appears under the APPL header of the alarm banner at the MTC level of the MAP display. The alarm indicates a critical alarm for the backup system.

### Meaning

The SBA backup system is using more than 50 percent of the total space on backup volumes on the DMS/CM. If the stream is configured as:

- both  
the alarm severity level is major
- on  
the alarm severity level is critical

**ATTENTION**

The option to configure a billing stream to both is only intended to be a temporary path while you are performing maintenance and alarm clearing tasks. The option to set a billing stream to the both mode on a permanent basis is not supported.

The core manager generates the SDMB820 log report when this alarm is raised.

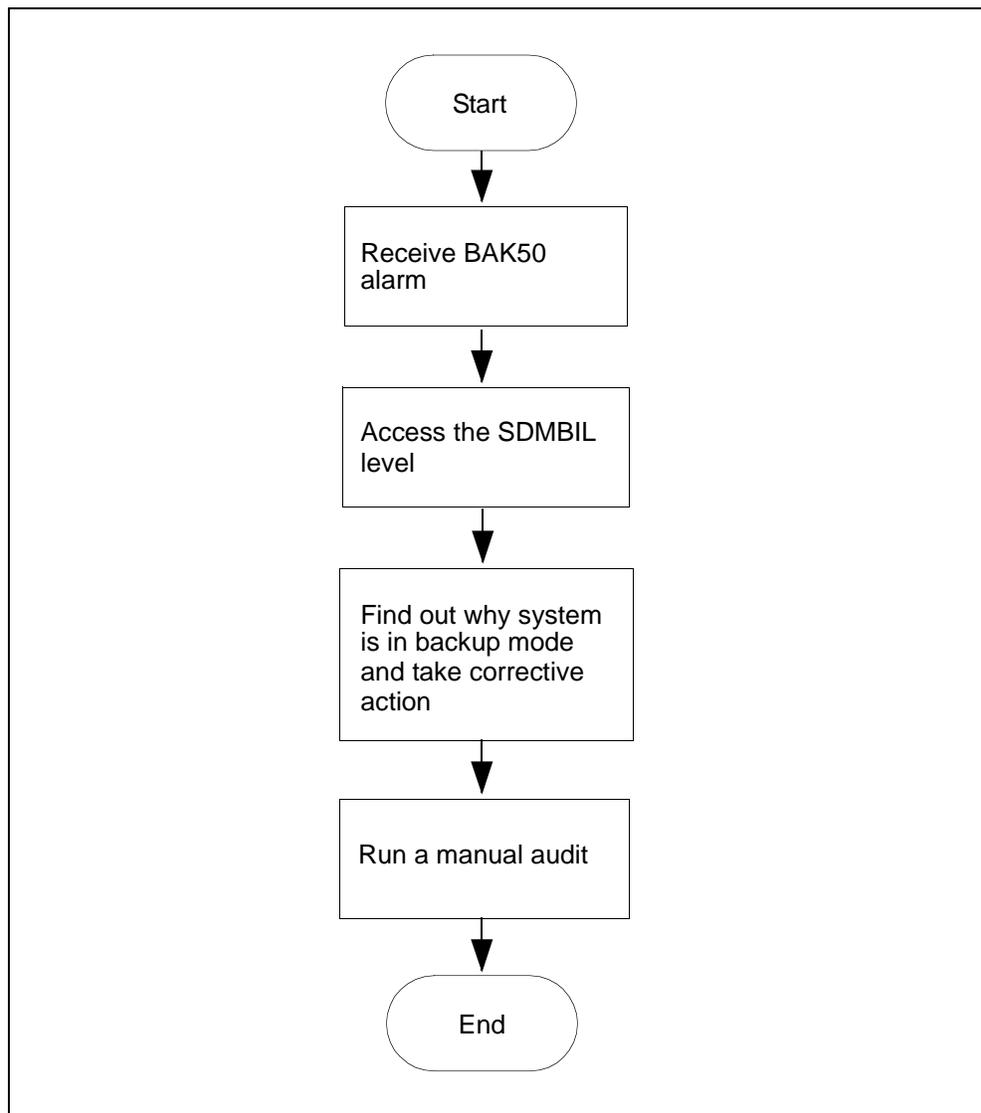
### Impact

If the disk usage for the SBA backup system reaches 100 percent of its capacity, data that is configured to go to backup storage is lost.

### Procedure

The following flowchart provides a summary of the procedure. Use the instructions in the procedure to clear the alarm.

## BAK50 alarm clearing flowchart



**Note:** Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or \$, displayed by the system through a GUI or on a command line.

### Clearing a BAK50 alarm

#### *At the MAP*

- 1 Post the billing stream:

```
mapci;mtc;appl;sdbil;post <stream_name>
```

where

<stream\_name> is the name of the billing stream.

- 2 Determine why the system is in backup mode.
- 3 Display all of the alarms that have been raised:  
**DispAL**
- 4 Determine the billing stream status.

| If the billing stream is | Perform the following steps                                                                                                                                                                                                                                                   |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SysB                     | perform the procedure for the alarm or the condition, and then return to step <a href="#">5</a> .                                                                                                                                                                             |
| RBsy                     | refer to <a href="#">Clearing a major SBACP alarm on page 136</a> , and then return to step <a href="#">5</a> .                                                                                                                                                               |
| ManB                     | RTS the billing stream.                                                                                                                                                                                                                                                       |
| Bkup                     | Go to step <a href="#">8</a> .                                                                                                                                                                                                                                                |
|                          | <b>Note:</b> The system may be in backup mode because communication between the core manager and CM has been lost. Adjusting disk space can temporarily remove the alarm. It is important, however, to determine why the system is in backup mode and take corrective action. |

- 5 Use Audit to clear the alarm.

| If the alarm  | Do                     |
|---------------|------------------------|
| cleared       | step <a href="#">6</a> |
| did not clear | step <a href="#">8</a> |

- 6 Ensure that the billing system is in recovery:  
**post <streamname>**
- 7 In the display, look for the status of the billing stream.

| If the billing system | Do                                 |
|-----------------------|------------------------------------|
| is in recovery (Rcvy) | step <a href="#">12</a>            |
| is not in recovery    | contact your next level of support |

- 8 Perform the procedure [Adjusting disk space in response to SBA backup file system alarms on page 95](#)

9 Use Audit to clear the alarm.

| If the alarm  | Do                                 |
|---------------|------------------------------------|
| cleared       | step <a href="#">10</a>            |
| did not clear | contact your next level of support |

10 Ensure that the billing system is in recovery:

**post <streamname>**

11 In the display, look for the status of the billing stream.

| If the billing system | Do                                 |
|-----------------------|------------------------------------|
| is in recovery (Rcvy) | step <a href="#">12</a>            |
| is not in recovery    | contact your next level of support |

12 You have completed this procedure.

---

## Clearing a BAK70 alarm

---

### Purpose

Use this procedure to clear a BAK70 alarm.

### Indication

BAK70 appears under the APPL header of the alarm banner at the MTC level of the MAP display, and indicates a critical alarm for the backup system.

### Meaning

The SBA backup system is using more than 70 percent of the total space on backup volumes on the DMS/CM. If the stream is set to:

- `both`  
the alarm severity level is major
- `on`  
the alarm severity level is critical

**ATTENTION**

The option to configure a billing stream to both is only intended to be a temporary path while you are performing maintenance and alarm clearing tasks. The option to set a billing stream to the both mode on a permanent basis is not supported.

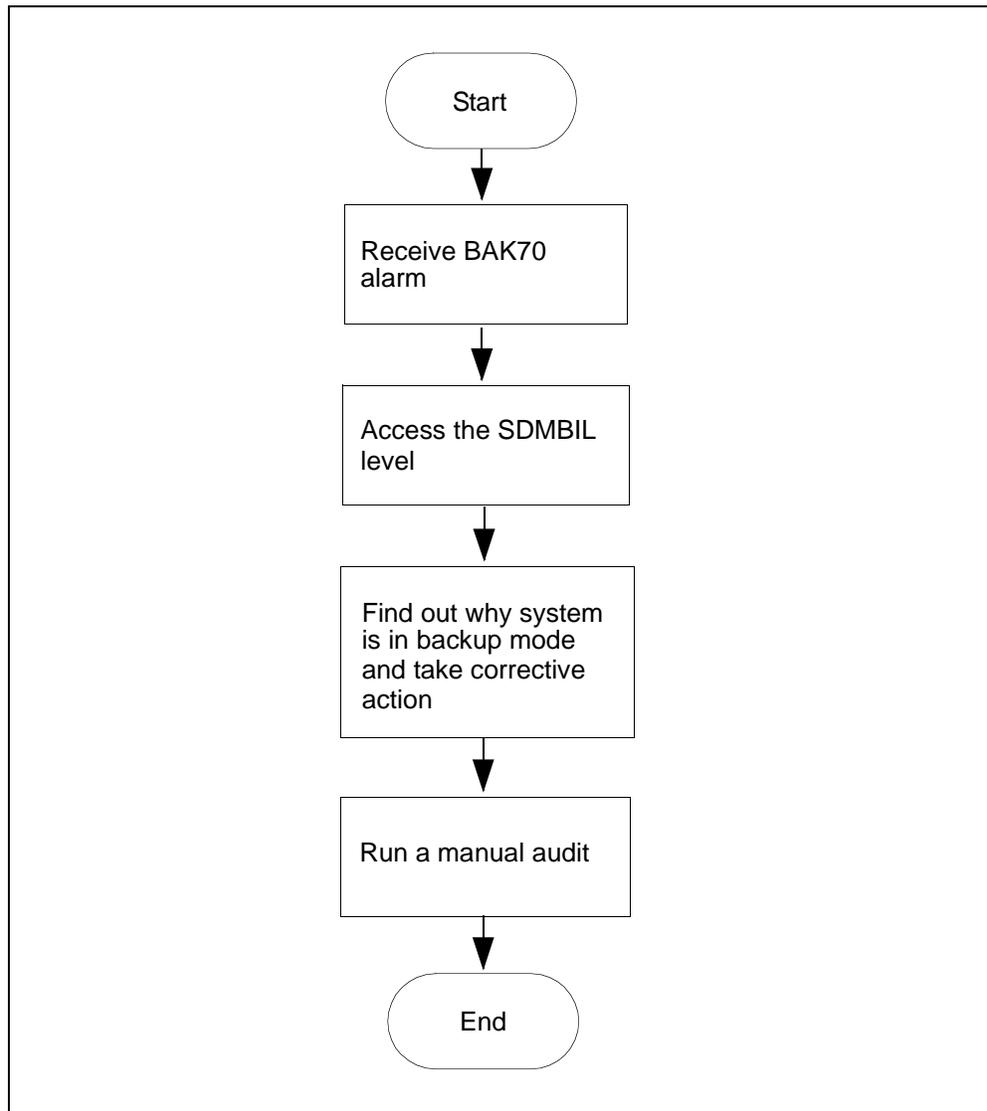
The core manager generates the SDMB820 log report when this alarm is raised.

### Impact

If the disk usage for the SBA backup system reaches 100 percent of its capacity, data that is configured to go to backup storage is lost.

### Procedure

The following flowchart provides a summary of the procedure. Use the instructions in the procedure to clear the alarm.

**BAK70 alarm clearing flowchart**

**Note:** Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or \$, displayed by the system through a GUI or on a command line.

## Clearing a BAK70 alarm

### At the MAP

- 1 Post the billing stream:

```
mapci;mtc;appl;sdbil;post <billing_stream>
```

where

<billing\_stream> is the name of the billing stream.

- 2 Determine why the system is in backup mode.
- 3 Display all of the alarms that have been raised:

```
DispAL
```

- 4 Determine the state of the billing stream.

| If the billing stream is | Perform the following steps                                                                                                                                                                                                                                                         |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SysB                     | perform the procedure for the alarm or the condition, and then return to step <a href="#">5</a> .                                                                                                                                                                                   |
| RBsy                     | refer to <a href="#">Clearing a major SBACP alarm on page 136</a> , and then return to step <a href="#">5</a> .                                                                                                                                                                     |
| ManB                     | RTS the billing stream. Go to step <a href="#">5</a>                                                                                                                                                                                                                                |
| Bkup                     | Go to step <a href="#">8</a>                                                                                                                                                                                                                                                        |
|                          | <p><b>Note:</b> The system may be in backup mode because communication between the core manager and CM has been lost. Adjusting disk space can temporarily remove the alarm. It is important, however, to determine why the system is in backup mode and take corrective action</p> |

- 5 Use Audit to clear the alarm.

| If the alarm  | Do                     |
|---------------|------------------------|
| cleared       | step <a href="#">6</a> |
| did not clear | step <a href="#">8</a> |

- 6 Ensure that the billing system is in recovery:

```
post <streamname>
```

7 In the display, look for the status of the billing stream.

| If the billing system | Do                                 |
|-----------------------|------------------------------------|
| is in recovery (Rcvy) | step <a href="#">12</a>            |
| is not in recovery    | contact your next level of support |

8 Perform the procedure [Adjusting disk space in response to SBA backup file system alarms on page 95](#)

9 Use Audit to clear the alarm.

| If the alarm  | Do                                 |
|---------------|------------------------------------|
| cleared       | step <a href="#">10</a>            |
| did not clear | contact your next level of support |

10 Ensure that the billing system is in recovery:

```
post <streamname>
```

11 In the display, look for the status of the billing stream.

| If the billing system | Do                                 |
|-----------------------|------------------------------------|
| is in recovery (Rcvy) | step <a href="#">12</a>            |
| is not in recovery    | contact your next level of support |

12 You have completed this procedure.

---

## Clearing a BAK90 alarm

---

### Purpose

Use this procedure to clear a BAK90 alarm.

### Indication

BAK90 appears under the APPL header of the alarm banner at the MTC level of the MAP display and indicates a critical alarm for the backup system.

### Meaning

The SBA backup system is using more than 90 percent of the total space on backup volumes on the DMS/CM. If the stream is configured as:

- both  
the alarm severity level is major
- on  
the alarm severity level is critical

**ATTENTION**

The option to configure a billing stream to both is only intended to be a temporary path while you are performing maintenance and alarm clearing tasks. The option to set a billing stream to the both mode on a permanent basis is not supported.

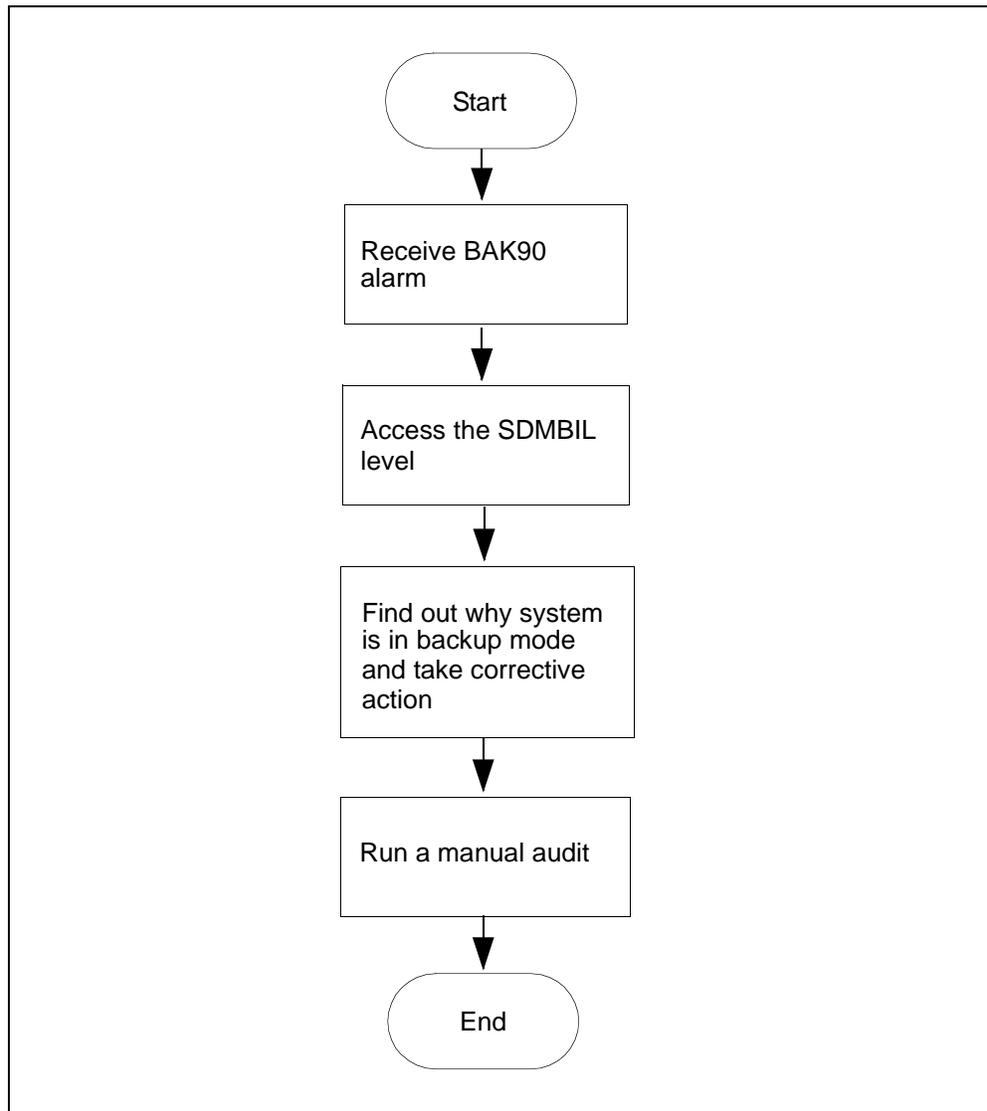
The core manager generates the SDMB820 log report when this alarm is raised.

### Impact

If the disk usage for the SBA backup system reaches 100 percent of its capacity, data that is configured to go to backup storage is lost.

### Procedure

The following flowchart is a summary of the procedure. Use the instructions in the procedure to clear the alarm.

**BAK90 alarm clearing flowchart**

**Note:** Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or \$, displayed by the system through a GUI or on a command line.

## Clearing a BAK90 alarm

### At the MAP

- 1 Post the billing stream:

```
mapci;mtc;appl;sdbil;post <billing_stream>
```

where

<billing\_stream> is the name of the billing stream.

- 2 Determine why the system is in backup mode.

- 3 Display all alarms that have been raised:

```
DispAL
```

- 4 Determine the state of the billing stream.

| If the billing stream is | Perform the following steps                                                                                                                                                                                                                                                  |
|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SysB                     | perform the procedure for the alarm or the condition, and then return to step <a href="#">5</a> .                                                                                                                                                                            |
| RBsy                     | refer to <a href="#">Clearing a major SBACP alarm on page 136</a> , and then return to step <a href="#">5</a> .                                                                                                                                                              |
| ManB                     | RTS the billing stream                                                                                                                                                                                                                                                       |
| Bkup                     | Go to step <a href="#">8</a>                                                                                                                                                                                                                                                 |
|                          | <b>Note:</b> The system may be in backup mode because communication between the core manager and CM has been lost. Adjusting disk space can temporarily remove the alarm. It is important, however, to determine why the system is in backup mode and take corrective action |

- 5 Use Audit to clear the alarm.

| If the alarm  | Do                     |
|---------------|------------------------|
| cleared       | step <a href="#">6</a> |
| did not clear | step <a href="#">8</a> |

- 6 Ensure that the billing system is in recovery:

```
post <streamname>
```

7 In the display, look for the status of the billing stream.

| If the billing system | Do                                 |
|-----------------------|------------------------------------|
| is in recovery (Rcvy) | step <a href="#">12</a>            |
| is not in recovery    | contact your next level of support |

8 Perform the procedure [Adjusting disk space in response to SBA backup file system alarms on page 95](#)

9 Use Audit to clear the alarm.

| If the alarm  | Do                                 |
|---------------|------------------------------------|
| cleared       | step <a href="#">10</a>            |
| did not clear | contact your next level of support |

10 Ensure that the billing system is in recovery:

```
post <streamname>
```

11 In the display, look for the status of the billing stream.

| If the billing system | Do                                 |
|-----------------------|------------------------------------|
| is in recovery (Rcvy) | step <a href="#">12</a>            |
| is not in recovery    | contact your next level of support |

12 You have completed this procedure.

---

## Clearing a BAKUP alarm

---

### Purpose

Use this procedure to clear a BAKUP alarm.

### Indication

BAKUP appears under the APPL header of the alarm banner at the MTC level of the MAP display, and indicates a critical alarm for the backup system.

### Meaning

Records are being stored on the DMS/CM backup volume for more than 10 minutes. If the stream is configured as:

- `both`  
the alarm severity level is major
- `on`  
the alarm severity level is critical

**ATTENTION**

The option to configure a billing stream as `both` is only intended to be a temporary path while you are performing maintenance and alarm clearing tasks. The option to set a billing stream to the `both` mode on a permanent basis is not supported.

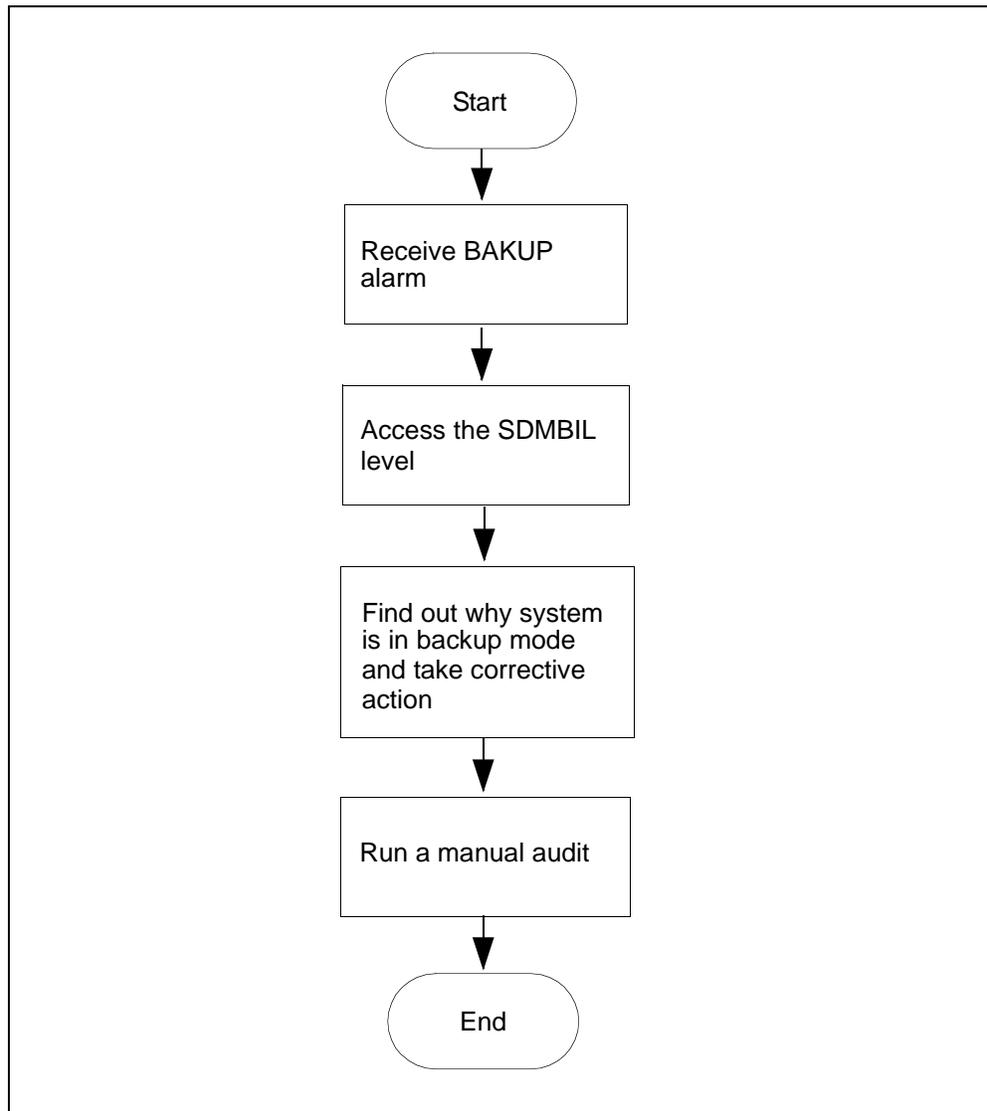
The core manager generates the SDMB820 log report when this alarm is raised.

### Impact

A problem with the SBA disk storage capacity can occur depending on the rate at which new data is sent to backup storage. BAK<sub>xx</sub> alarms provide storage notification (<sub>xx</sub> is the percentage of disk storage used).

### Procedure

The following flowchart provides a summary of the procedure. Use the instructions in the procedure to clear the alarm.

**BAKUP alarm clearing flowchart**

**Note:** Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or \$, displayed by the system through a GUI or on a command line.

## Clearing a BAKUP alarm

### At the MAP

- 1 Post the billing stream:

```
mapci;mtc;appl;sdbil;post <billing_stream>
```

where

<billing\_stream> is the name of the billing stream

- 2 Determine why the system is in backup mode.
- 3 Display all alarms that have been raised:

```
DispAL
```

- 4 Determine the state of the billing stream.

| If the billing stream is | Perform the following steps                                                                                                                                                                                  |
|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SysB                     | perform the procedure for the alarm or the condition, and then return to step <a href="#">5</a> .                                                                                                            |
| RBsy                     | refer to <a href="#">Clearing a major SBACP alarm on page 136</a> , and then return to step <a href="#">5</a> .                                                                                              |
| ManB                     | RTS the billing stream.                                                                                                                                                                                      |
| Bkup                     | <b>Note:</b> The system may be in backup mode because communication between the core manager and CM has been lost. It is important to determine why the system is in backup mode and take corrective action. |

- 5 Use Audit to clear the alarm.

| If the alarm  | Do                                  |
|---------------|-------------------------------------|
| cleared       | step <a href="#">6</a>              |
| did not clear | Contact your next level of support. |

- 6 Ensure that the billing system is in recovery:

```
post <streamname>
```

- 7 In the display, look for the status of the billing stream.

| If the billing system | Do                                 |
|-----------------------|------------------------------------|
| is in recovery (Rcvy) | step <a href="#">11</a>            |
| is not in recovery    | contact your next level of support |

**8** Use Audit to clear the alarm.

| <b>If the alarm</b> | <b>Do</b>                          |
|---------------------|------------------------------------|
| cleared             | step <a href="#">9</a>             |
| did not clear       | contact your next level of support |

**9** Ensure that the billing system is in recovery:

**post <streamname>**

**10** In the display, look for the status of the billing stream.

| <b>If the billing system</b> | <b>Do</b>                          |
|------------------------------|------------------------------------|
| is in recovery (Rcvy)        | step <a href="#">11</a>            |
| is not in recovery           | contact your next level of support |

**11** You have completed this procedure.

## Adjusting disk space in response to SBA backup file system alarms

### Purpose

Use this procedure to adjust disk space when SBA backup file system alarms are raised. The procedure enables you to either add logical volumes to a disk or to remove logical volumes from a disk.

**Note:** Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or \$, displayed by the system through a GUI or on a command line.

### Procedure

#### Adjusting disk space in response to SBA backup file system alarms

##### At the MAP

- 1 Post the billing stream:

```
mapci;mtc;appl;sdmbil;post <stream_name>
```

where

<stream\_name> is the name of the billing stream.

- 2 Display the names of the backup volumes configured for the stream:

```
conf view <stream_name>
```

where

<stream\_name> is the name of the billing stream.

| If the backup volumes are located on | Do                     |
|--------------------------------------|------------------------|
| DDU disks                            | step <a href="#">3</a> |
| IOP disks                            | step <a href="#">5</a> |
| SLM disks                            | step <a href="#">5</a> |
| 3PC disks                            | step <a href="#">5</a> |

- 3 Display and record the size of a volume and its number of free blocks:

```
diskut;sv <volume name>
```

where

**<volume name>**

is the name of one of the volumes that you obtained and recorded in step [2](#)

- 4 Repeat step [3](#) for each volume name that you recorded in step [2](#), and then proceed to step [5](#).
- 5 Display and record the size of a volume and its number of free blocks:

```
diskut;lv <volume name>
```

*where*

**<volume name>**

is the name of one of the volumes that you obtained and recorded in step [2](#).

- 6 Repeat step [5](#) for each volume name that you recorded in step [2](#).

| If the volumes                | Do                                                                                                               |
|-------------------------------|------------------------------------------------------------------------------------------------------------------|
| have enough disk space        | step <a href="#">7</a>                                                                                           |
| do not have enough disk space | perform procedure "Configuring SBA backup volumes on the core" in the Accounting document for your core manager. |

- 7 You have completed this procedure.

---

## Clearing a CDRT alarm

---

### Purpose

Use this procedure to clear a CDRT alarm.

### Indication

At the MTC level of the MAP display, CDRT appears under the APPL header of the alarm banner and indicates a core manager alarm.

### Meaning

The CDRT alarm indicates the value of the active template ID template on the DMS CM is not set to "0" (zero) or it does not match the value of the CurrentTpltID MIB parameter.

- Log report SDMB370 is generated when this alarm is raised
- log report SDMB670 is generated when this alarm is cleared

Valid template IDs are 0, 1, 2, or a template ID matching the value in the CDR MIB field currentTpltID.

### Impact

The CDR to BAF conversion process does not create BAF records.

### Action

If this alarm occurs:

- set the value of the CurrentTpltID MIB parameter to match the value (template ID) of the active template ID on the DMS/CM, or
- set the active template ID on the CM to "0" (zero)

The alarm is cleared when a valid template is received.

**Note:** Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or \$, displayed by the system through a GUI or on a command line.

#### ***At the MAP***

- 1 Determine the value of the active template ID on the DMS/CM:  
`CTMPLT "template all"`
- 2 Set the CurrentTpltID mib parameter to match the value of the active template ID:  
`mib cdr set CurrentTpltID <template_ID>`

*where*

**<template\_ID>** is the value of the active template on the DMS/CM.

- 3** If you change the CurrentTplID MIB parameter after you have turned on the stream, you must BSY and then `rts` the SBA application to activate the change.
- 4** If the alarm persists, contact your next level of support.

---

## Clearing a DSKWR alarm on a CBM

---

### Indication

At the MTC level of the MAP display, DSKWR appears under the APPL header of the alarm banner and indicates a critical disk alarm.

### Meaning

The system is unable to write records to the CBM disk because the disk is unavailable or the disk is full.

### Impact

The DMS/CM cannot send the billing records to the CBM. As a result, the DMS/CM send the billing records to backup storage. However, this backup storage is limited. As the backup storage becomes filled, alarms notify you as to how much of its capacity is used.

### Prerequisites

**ATTENTION**

If the NOBAK or NOSTOR alarm appears in addition to the DSKWR alarm, you must configure and activate alternative backup volumes before you clear the DSKWR alarm.

### Procedure

Use the following procedure to clear DSKWR alarm.

#### Clearing a DSKWR alarm

##### *At the MAP interface on the CM*

- 1 Access the SDBIL level:  

```
> mapci;mtc;appl;sdbil
```

- 2 Check to see if the NOBAK or NOSTOR alarm exists in addition to the DSKWR alarm on the alarm banner:

> **dispal**

| If the NOBAK or NOSTOR alarm        | Do                                                                                              |
|-------------------------------------|-------------------------------------------------------------------------------------------------|
| appears in the alarm banner         | perform the procedure "Configuring SBA backup volumes on the core" in the NN10363-811 document. |
| does not appear in the alarm banner | step <a href="#">3</a>                                                                          |

### *At your workstation*

- 3 Check to see if any logs have been raised that indicate a problem with the system's disks, by performing the procedure, [Viewing customer logs on an SSPFS-based server on page 195](#).
- 4 Determine whether the file system holding the billing files has adequate space by performing the procedure, [Verifying disk utilization on an SSPFS-based server](#).
- 5 If you want to back up the billing files, perform the procedure "Copying files to DVD" in the NN10363-811 document.
- 6 Using the information you obtained in step [4](#) determine whether the file system is full. The file system can be full if you have not sent the primary files downstream.

| If                                                                    | Do                                 |
|-----------------------------------------------------------------------|------------------------------------|
| you want to send the billing files downstream                         | step <a href="#">7</a>             |
| you feel that the capacity of the SBA file system requires adjustment | contact your next level of support |

- 7 Access the BILLMTC interface:

> **billmtc**

- 8 Access the FILESYS level:

> **filesys**

- 9 Send the primary billing files to the downstream processor:

```
> sendfile <stream_name>
```

where:

<stream\_name> is the name of the stream.

**Note:** The **sendfile** command sends the billing file to the billing collector.

| If the SENDFILE command | Do                                                                                                                                                                                                                                                              |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| is successful           | step <a href="#">10</a>                                                                                                                                                                                                                                         |
| is not successful       | refer to procedures <a href="#">Verifying the file transfer protocol</a> and <a href="#">Verifying the FTP Schedule</a> , then return to this procedure and repeat step <a href="#">9</a><br><br>If unsuccessful afterwards, contact your next level of support |

- 10 Use Audit to clear the alarm.

| If the alarm  | Do                      |
|---------------|-------------------------|
| cleared       | step <a href="#">17</a> |
| did not clear | step <a href="#">11</a> |

- 11 Quit the BILLMTC interface:

```
> quit all
```

- 12 At the prompt, check for orphan files and for files someone else copied to the logical volume of your billing stream:

```
> ls /<stream>/<stream_name>/orphan
```

where:

<stream> is the full pathname of the directory you have configured for the billing stream

**<stream\_name>** is the name of the billing stream.

| If billing files full because of accumulated orphan files                       | Do                                 |
|---------------------------------------------------------------------------------|------------------------------------|
| and you are unclear as to how to clean up the billing directory                 | contact your next level of support |
| and you have cleaned up the billing directory and are still incurring a problem | step <a href="#">13</a>            |

- 13** Verify the write permission and ownership for the directories in the billing stream:

```
ls -lrt /<stream>/<stream_name>
```

**<stream>** is the full pathname of the directory you have configured for the billing stream

**<stream\_name>** is the name of the billing stream

| If the                                                           | Do                                 |
|------------------------------------------------------------------|------------------------------------|
| permissions (rwx r-x r-x) and file ownership (maint) are correct | contact your next level of support |
| permissions for a directory are not rwx                          | step <a href="#">14</a>            |
| ownership for a directory is not maint                           | step <a href="#">15</a>            |
| the alarm fails to clear                                         | contact your next level of support |

- 14** Change the permissions for a directory:

```
> chmod 755 <directory>
```

*where:*

**<directory>** is the billing file directory in which you are changing permissions.

- 15** Change the ownership of a directory:

```
> chown maint:maint <directory>
```

*where:*

**<directory>** is the billing file directory in which you are changing ownership.

- 16** Use Audit to clear the alarm.

| <b>If the alarm</b> | <b>Do</b>                          |
|---------------------|------------------------------------|
| cleared             | step <a href="#">17</a>            |
| did not clear       | contact your next level of support |

- 17** You have completed this procedure.

## Clearing an FTPW alarm

### Purpose

Use this procedure to clear an FTPW alarm.

### Indication

At the MTC level of the MAP display, FTPW appears under the APPL header of the alarm banner and indicates an alarm for FTP.

### Meaning

The FTP process failed. The SDMB375 log report provides details about the FTP problem. Log report SDMB675 is generated when this alarm is cleared. This alarm can be either critical or major.

**Note:** The FTPW alarm can be present on the CM for a non-existent schedule. For example, the FTPW alarm is generated if an operator shuts down the server (making the ftp service unavailable to the core manager) without deleting the associated schedule tuple on the core manager first.

### Impact

The core manager cannot send files to the downstream destinations. The core manager will eventually reach its storage capacity, depending on the amount of storage and the volume of records. When this storage is full, the DMS switch/CM sends subsequent records to backup storage. When backup storage reaches capacity, billing records cannot be stored and will be lost.

### Action

#### Clearing an FTPW alarm

##### *At the core manager*

- 1 Complete procedure [Verifying the file transfer protocol on page 144](#) in this document.

| If                      | Do                            |
|-------------------------|-------------------------------|
| alarm fails to clear    | contact next level of support |
| schedule does not exist | step <a href="#">2</a>        |

- 2 Add a schedule tuple with the same stream name and destination defined by the alarm.

Use the procedure “Configuring the outbound file transfer schedule” in the Accounting document, then return to this procedure.

- 3** Once the alarm is cleared, delete the tuple that you added in [step 2](#).
- 4** You have completed this procedure.

## Clearing an inbound file transfer alarm

### Purpose

Use this procedure to clear an inbound file transfer (IFT) alarm.

### Indication

At the MTC level of the MAP display, inbound file transfer (IFT) appears under the APPL header of the alarm banner and indicates an alarm for the inbound file transfer connection.

### Meaning

The IFT alarm indicates the occurrence of an inbound file transfer. This alarm is raised if the link in the ftpdir directory of a stream cannot be managed or if an ftpdir directory is not accessible. This alarm can be minor, major, or critical.

Detailed information about the alarm condition is documented in log reports:

- SDMB375 or SDMB380 when the alarm is raised
- SDMB675 or SDMB680 after the alarm is cleared

### Prerequisites

#### Logging on to the CS 2000 Core Manager

You must be a user authorized to perform fault-admin actions in order to perform this procedure.

For information on how to log in to the CS 2000 Core Manager as an authorized user or how to display other information about a user or role group, review the procedures in the following table.

| Procedure                                         | Document                                                              |
|---------------------------------------------------|-----------------------------------------------------------------------|
| Logging in to the CS 2000 Core Manager            | <i>CS 2000 Core Manager Security and Administration</i> , NN10170-611 |
| Displaying information about a user or role group | <i>CS 2000 Core Manager Security and Administration</i> , NN10170-611 |

#### Logging on to the Core and Billing Manager 850

You must have the root user ID and password to log into the server.

## Impact

Inbound file transfer for the billing stream is not possible.

## Action

This alarm occurs only in rare situations. If this alarm occurs, ensure all other SBA alarms are cleared. The root user can check the following IFT alarm conditions:

- ftpdir directory has no write access
- storage for the billing stream has no space available
- <rcLogicalVolumeDirectory>/ftpdir directory does not exist

Determine what alarm is present by reading the log text and associating it to the appropriate alarm.

**Note:** Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or \$, displayed by the system through a GUI or on a command line.

### Clearing an IFT alarm

#### At the MAP

- 1 Log into the core manager. Refer to [Prerequisites](#) for details.

| If the                                                                      | Do                          |
|-----------------------------------------------------------------------------|-----------------------------|
| /home/maint/ftpdir directory has write permissions                          | no action is required       |
| /home/maint/ftpdir directory does not have write permissions                | step <a href="#">2</a> only |
| <rcLogicalVolumeDirectory>/ftpdir directory has write permissions           | no action is required       |
| <rcLogicalVolumeDirectory>/ftpdir directory does not have write permissions | step <a href="#">3</a> only |
| storage disk has sufficient space                                           | no action is required       |
| storage disk does not have sufficient space                                 | step <a href="#">4</a> only |

| If the                                                                                      | Do                                                                  |
|---------------------------------------------------------------------------------------------|---------------------------------------------------------------------|
| <rcLogicalVolumeDirectory><br>path is correct                                               | no action is required                                               |
| <rcLogicalVolumeDirectory><br>path is incorrect                                             | correct the<br><rcLogicalVolumeDirectory><br>path into the CONFSTRM |
| <rcLogicalVolumeDirectory>/<br>ftpdire is a directory                                       | no action is required                                               |
| <rcLogicalVolumeDirectory>/<br>ftpdire is not a directory                                   | step <a href="#">5</a> only                                         |
| IFT alarm persists once you<br>have performed the<br>appropriate steps in this<br>procedure | contact your next level of<br>support                               |

- 2 Change the permissions of the /home/maint/ftpdire directory:

```
chmod 777 /home/maint/ftpdire
```

- 3 Remove the <rcLogicalVolumeDirectory>/ftpdire directory:

```
rm /<rcLogicalVolumeDirectory>/ftpdire
```

where

**<rcLogicalVolumeDirectory>** is the logical volume that is assigned to the billing stream in the `confstrm`. The billing files are stored in the specified path.

**Note:** The next interval recreates the correct permissions and recreates all links.

- 4 Retrieve some *closed not sent* files and rename them to *closed sent*.

**Note 1:** Closed not sent files for DNS and DIRP have the file extensions of .pri and .unp respectively. When you rename them, change the file extensions to .sec and .pro respectively.

**Note 2:** The closed sent files are removed from the system to make available more disk space. If you continue to receive the IFT alarm, consider increasing the size of the logical volume.

- 5 Remove the <rcLogicalVolumeDirectory>/ftpdire directory:

```
rm /<rcLogicalVolumeDirectory>/ftpdire
```

**<rcLogicalVolumeDirectory>** is the logical volume that is assigned to the billing stream in the `confstrm`. The billing files are stored in the specified path.

**Note:** At the next transfer interval, the correct permissions and all links are re-created.

- 6 You have completed the procedure.

---

## Clearing an LODSK alarm

---

### Purpose

Use this procedure to clear a low disk storage (LODSK) alarm.

### Indication

**CAUTION****Possible Loss of Service**

If you receive a LODSK alarm, transfer (FTP) the billing files in the closedNotSent directory, or write to tape immediately. Refer to [Verifying the file transfer protocol on page 144](#) for more information.

At the `mtc` level of the `mapci`, LODSK appears under the APPL header of the alarm banner, and indicates a storage alarm.

### Meaning

The closedNotSent directory is reaching its capacity. The core manager generates the SDMB355 log report when this alarm is raised.

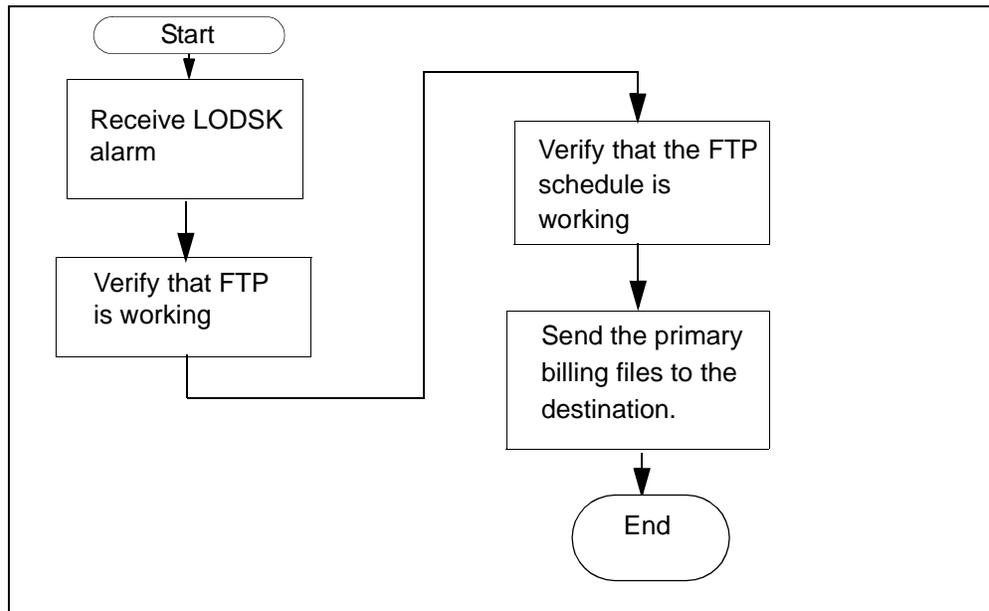
### Impact

As the storage becomes full, alarms notify you of how much capacity is used. In addition, there is a possibility that the DMS/CM does not go into backup mode when the core manager logical volume reaches 100 percent capacity.

### Action

The following flowchart is a summary of the procedure. Use the instructions in the procedure to clear the alarm.

### LODSK alarm clearing flowchart



### Clearing a LODSK alarm

#### At the MAP

- 1 Use the procedure [Verifying the file transfer protocol on page 144](#) to determine if the FTP is working properly.

| If the alarm   | Do                                                                                                                                         |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| clears         | you have completed this procedure                                                                                                          |
| does not clear | refer to procedure <a href="#">Verifying the FTP Schedule on page 151</a><br><br>if the alarm persists, contact your next level of support |

---

## Clearing a NOBAK alarm

---

### Purpose

Use this procedure to clear a no-backup (NOBAK) alarm.

### Indication

NOBAK appears under the APPL header of the alarm banner at the MTC level of the MAP display and indicates a critical alarm for the backup system.

### Meaning

This alarm only occurs if the volumes that are configured for backup are 100 percent full. If the stream is configured as

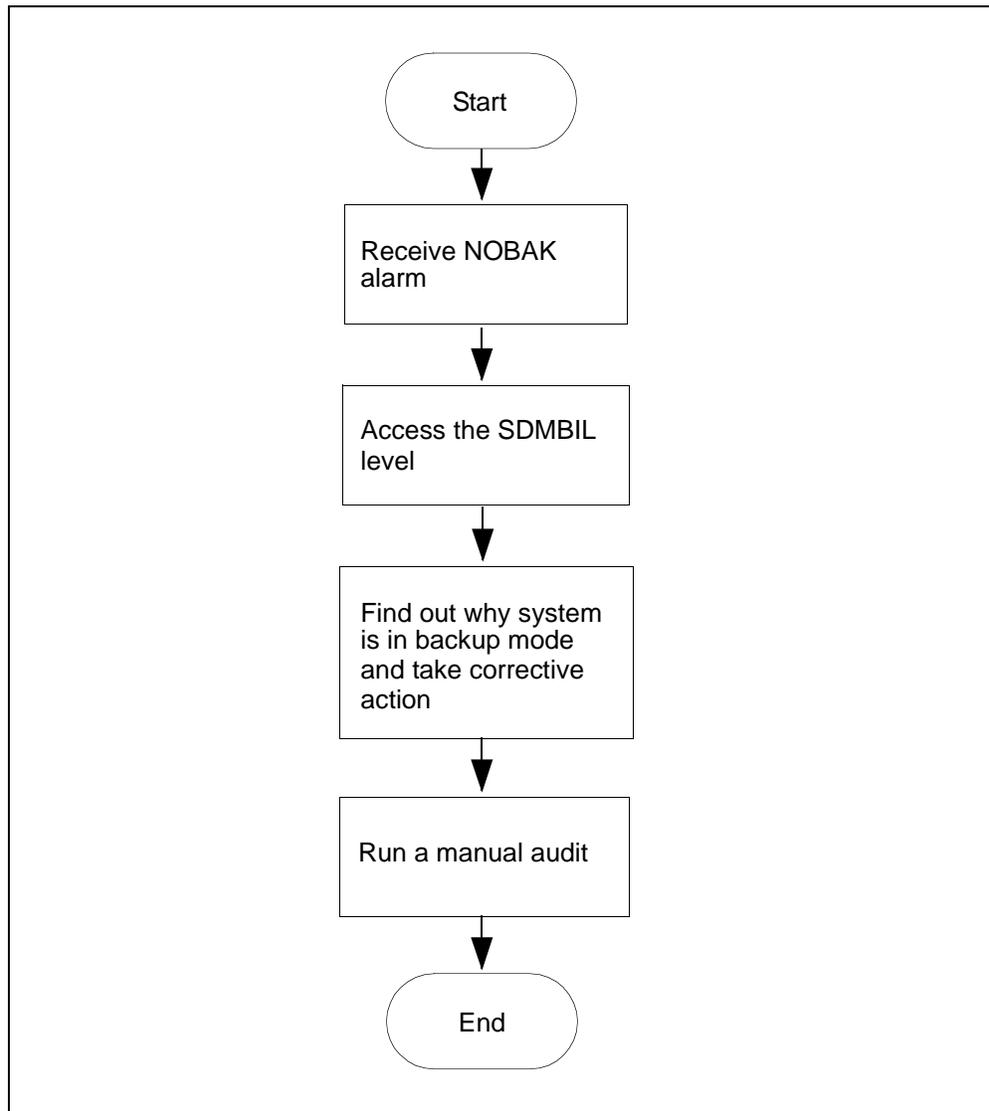
- `both`  
the alarm severity level is major
- `on`  
the alarm severity level is critical

**ATTENTION**

The option to configure a billing stream as “both” is only intended to be a temporary path while you are performing maintenance and alarm clearing tasks. The option to set a billing stream to the both mode on a permanent basis is not supported.

### Procedure

The following flowchart is a summary of the procedure. Use the instructions in the procedure to clear the alarm.

**NOBAK alarm clearing flowchart**

**Note:** Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or \$, displayed by the system through a GUI or on a command line.

## Clearing a NOBAK alarm

### At the MAP

- 1 Post the billing stream:

```
mapci;mtc;appl;sdbil;post <billing_stream>
```

where

<billing\_stream> is the name of the billing stream

- 2 Determine why the system is in backup mode.
- 3 Display all alarms that have been raised:

```
DispAL
```

- 4 Determine the state of the billing stream.

| If the billing stream is | Perform the following steps                                                                                                                                                                                                                                                   |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SysB                     | perform the procedure for the alarm or the condition, and then go to step <a href="#">5</a> .                                                                                                                                                                                 |
| RBsy                     | refer to <a href="#">Clearing a major SBACP alarm on page 136</a> , and then return to step <a href="#">5</a> .                                                                                                                                                               |
| ManB                     | RTS the billing stream                                                                                                                                                                                                                                                        |
| Bkup                     | Go to step <a href="#">8</a>                                                                                                                                                                                                                                                  |
|                          | <b>Note:</b> The system may be in backup mode because communication between the core manager and CM has been lost. Adjusting disk space can temporarily remove the alarm. It is important, however, to determine why the system is in backup mode and take corrective action. |

- 5 Use Audit to clear the alarm.

| If the alarm  | Do                     |
|---------------|------------------------|
| cleared       | step <a href="#">6</a> |
| did not clear | step <a href="#">8</a> |

- 6 Ensure that the billing system is in recovery:

```
post <streamname>
```

7 In the display, look for the status of the billing stream.

| If the billing system | Do                                 |
|-----------------------|------------------------------------|
| is in recovery (Rcvy) | step <a href="#">12</a>            |
| is not in recovery    | contact your next level of support |

8 Perform the procedure [Adjusting disk space in response to SBA backup file system alarms on page 95](#)

9 Use Audit to clear the alarm.

| If the alarm  | Do                                 |
|---------------|------------------------------------|
| cleared       | step <a href="#">10</a>            |
| did not clear | contact your next level of support |

10 Ensure that the billing system is in recovery:

```
post <streamname>
```

11 In the display, look for the status of the billing stream.

| If the billing system | Do                                 |
|-----------------------|------------------------------------|
| is in recovery (Rcvy) | step <a href="#">12</a>            |
| is not in recovery    | contact your next level of support |

12 You have completed this procedure.

---

## Clearing a NOCLNT alarm

---

### Purpose

Use this procedure to clear a NOCLNT alarm.

### Indication

At the MTC level of the MAP display, NOCLNT appears under the APPL header of the alarm banner and indicates an alarm.

### Meaning

The stream was activated by the SDMBCTRL command before initialization was complete. If the stream is set to

- `on`  
the alarm is critical
- `both`  
the alarm is major

**ATTENTION**

The option to set a billing stream to `both` is only intended to be a temporary path while you are performing maintenance and alarm clearing tasks. The option to set a billing stream to the `both` mode on a permanent basis is not supported.

### Impact

No data is buffered by the SBA system. As a result, no data is backed up or made available for delivery to the core manager.

If the stream is set to `both`, data is still being routed to DIRP. Therefore, you can send the billing records to the operating company collector through the previously-established network used by DIRP.

### Action

This alarm only occurs in rare cases during installation. If this alarm occurs, contact your next level of support.

---

## Clearing a NOFL alarm

---

### Purpose

Use this procedure to clear a no file (NOFL) alarm.

### Indication

NOFL appears under the APPL header of the alarm banner at the MTC level of the MAP display and indicates a critical alarm for the backup system.

### Meaning

On startup, the SBA backup file system is unable to create a file. If the stream is set to:

- `both`  
the alarm severity level is major
- `on`  
the alarm severity level is critical

**ATTENTION**

The option to configure a billing stream as both is only intended to be a temporary path while you are performing maintenance and alarm clearing tasks. The option to configure a billing stream to the both mode on a permanent basis is not supported.

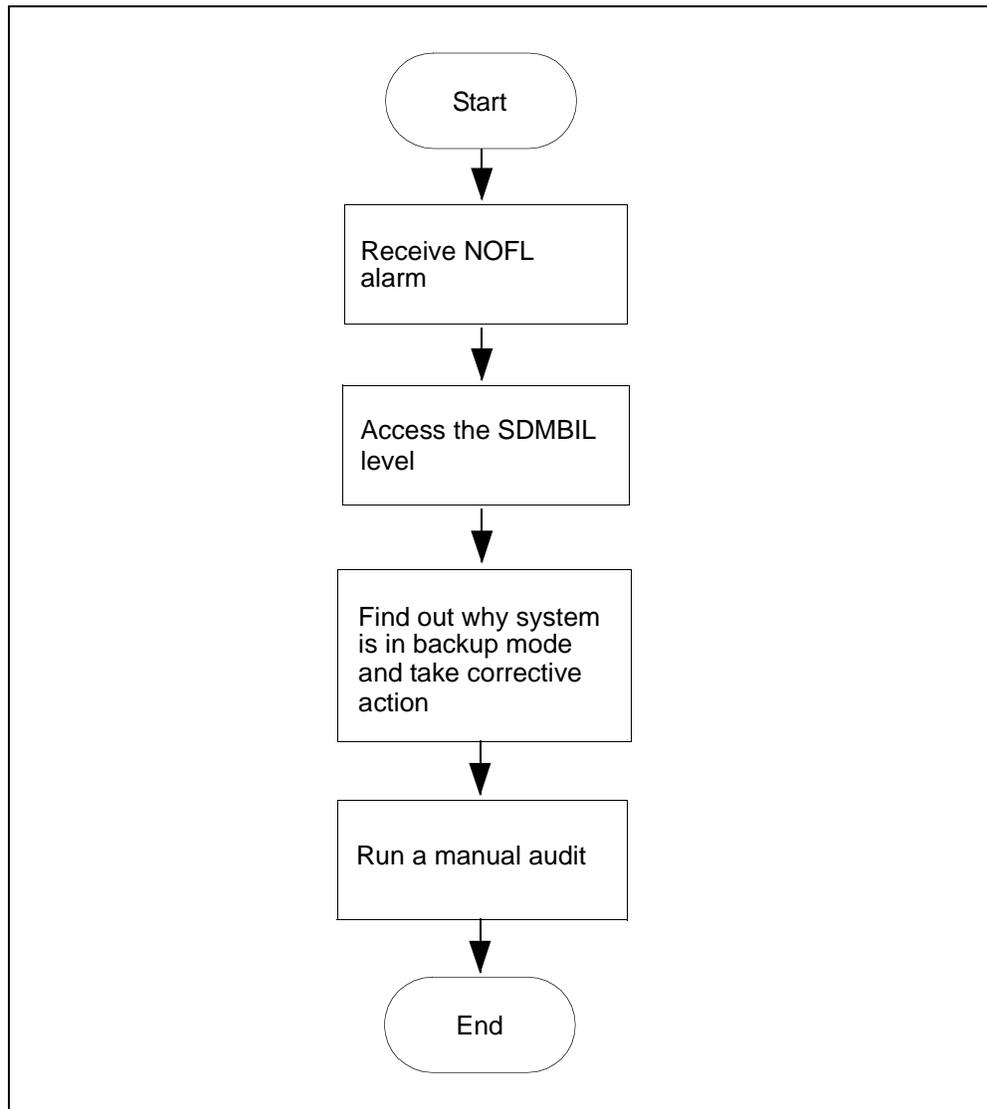
### Impact

Because no file is available for SBA data storage, data intended for storage is lost.

### Procedure

The following flowchart is a summary of the procedure. Use the instructions in the procedure to clear the alarm.

### NOFL alarm clearing flowchart



**Note:** Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or \$, displayed by the system through a GUI or on a command line.

## Clearing a NOFL alarm

### At the MAP

- 1 Post the billing stream:

```
mapci;mtc;appl;sdbil;post <stream_name>
```

where

<stream\_name> is the name of the billing stream.

- 2 Determine why the system is in backup mode.
- 3 Display all alarms that have been raised:

```
DispAL
```

- 4 Determine the status of the billing stream.

| If the billing stream is | Perform the following steps                                                                                     |
|--------------------------|-----------------------------------------------------------------------------------------------------------------|
| SysB                     | perform the procedure for the alarm or the condition, and then go to step <a href="#">5</a> .                   |
| RBsy                     | refer to <a href="#">Clearing a major SBACP alarm on page 136</a> , and then return to step <a href="#">5</a> . |
| ManB                     | Go to step <a href="#">8</a>                                                                                    |
| Bkup                     | Go to step <a href="#">8</a>                                                                                    |

- 5 Use Audit to clear the alarm.

| If the alarm  | Do                     |
|---------------|------------------------|
| cleared       | step <a href="#">6</a> |
| did not clear | step <a href="#">8</a> |

- 6 Ensure that the billing system is in recovery:

```
post <streamname>
```

- 7 In the display, look for the status of the billing stream.

| If the billing system | Do                                 |
|-----------------------|------------------------------------|
| is in recovery (Rcvy) | step <a href="#">12</a>            |
| is not in recovery    | contact your next level of support |

- 8 Perform the procedure [Adjusting disk space in response to SBA backup file system alarms on page 95](#)

9 Use Audit to clear the alarm.

| If the alarm  | Do                                 |
|---------------|------------------------------------|
| cleared       | step <a href="#">10</a>            |
| did not clear | contact your next level of support |

10 Ensure that the billing system is in recovery:

**post <streamname>**

11 In the display, look for the status of the billing stream.

| If the billing system | Do                                 |
|-----------------------|------------------------------------|
| is in recovery (Rcvy) | step <a href="#">12</a>            |
| is not in recovery    | contact your next level of support |

12 You have completed this procedure.

---

## Clearing a NOREC alarm

---

### Indication

At the MTC level of the MAP display, NOREC appears under the APPL header of the alarm banner. It indicates an alarm for the recovery system.

### Meaning

The SBA system is unable to create a recovery stream. The most likely reasons for not being able to start a recovery stream include the following:

- the system is out of buffers (also causes a NOSTOR alarm).
- the disk on the core manager is full (also causes DSKWR and LODSK alarms)

If the stream is set to:

- `on`  
the alarm is major, or
- `both`  
the alarm is minor

### Impact

No backup files are recovered by the SBA system.

If the stream is set to `both`, data is still being routed to DIRP. Therefore, you can send the billing records to the operating company collector through the previously-established network used by DIRP.

### Action

Contact your next level of support when you receive this alarm.

---

## Clearing an NOSC alarm

---

### Indication

At the MTC level of the MAP display, NOSC appears under the APPL header of the alarm banner and indicates a core manager alarm.

The core manager generates the SDMB370 log report when this alarm is raised.

### Meaning

The NOSC alarm indicates that the CDR has received an invalid structure code. Valid structure codes are 220, 360, 364, 625, 645, and 653.

**Note:** If the fixed template id 0 or if the CurrentTplID in the CDR MIB is used, structure codes 220 and 645 are invalid.

### Impact

The CDR2BAF conversion process does not create BAF records.

### Action

This alarm is cleared when a call is completed that contains a valid structure code. Contact your next level of support if this alarm fails to clear.

---

## Clearing a NOSTOR alarm

---

### Purpose

Use this procedure to clear a no storage (NOSTOR) alarm.

### Indication

NOSTOR appears under the APPL header of the alarm banner at the MTC level of the MAP display and indicates a critical alarm for the backup system.

### Meaning

The SBA buffer pool cannot allocate buffers. This means that all buffers are in use, though it does not necessarily mean that the disk is full.

The NOSTOR alarm is usually seen when the system is in backup mode and the traffic is too high for the disk to process. If the disk stream is configured as:

- both  
the alarm severity level is major
- on  
the alarm severity level is critical

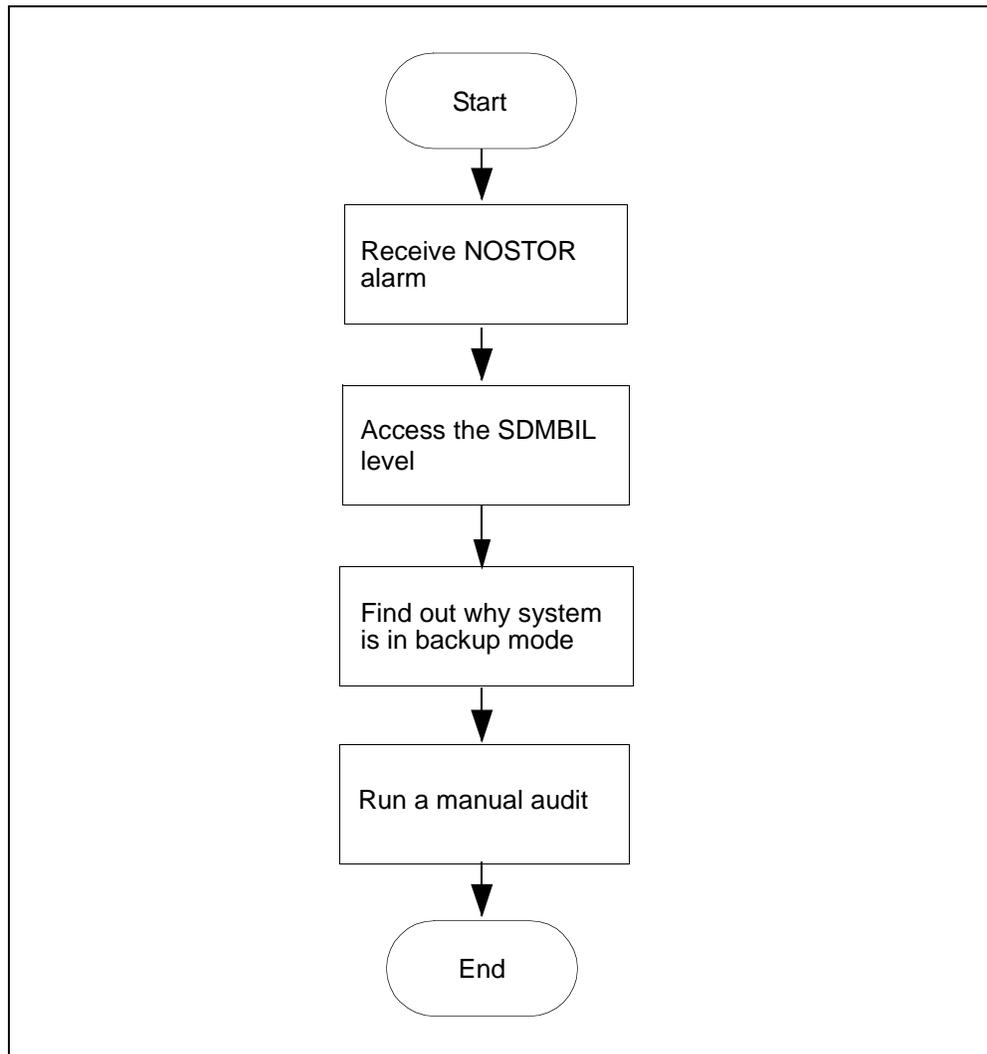
#### **ATTENTION**

The option to configure a billing stream as both is only intended to be a temporary path while you are performing maintenance and alarm clearing tasks. The option to configure a billing stream to the both mode on a permanent basis is not supported.

### Procedure

The following flowchart is a summary of the procedure. Use the instructions in the procedure to clear the alarm.

## NOSTOR alarm clearing flowchart



**Note:** Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or \$, displayed by the system through a GUI or on a command line.

### Clearing a NOSTOR alarm

#### *At the MAP*

- 1 Post the billing stream:  
`mapci;mtc;appl;sdmbil;post <stream_name>`  
*where*  
`<stream_name>` is the name of the billing stream
- 2 Determine why the system is in backup mode.

- 3 Display all alarms that have been raised:

**DispAL**

- 4 Determine the state of the billing stream.

| If the billing stream is | Perform the following steps                                                                                 |
|--------------------------|-------------------------------------------------------------------------------------------------------------|
| SysB                     | perform the procedure for the alarm or the condition, and then go to step <a href="#">5</a> .               |
| RBsy                     | refer to <a href="#">Clearing a major SBACP alarm on page 136</a> , and then go to step <a href="#">5</a> . |
| ManB                     | RTS the billing stream                                                                                      |
| Bkup                     | Go to step <a href="#">8</a>                                                                                |

- 5 Use Audit to clear the alarm.

| If the alarm  | Do                     |
|---------------|------------------------|
| cleared       | step <a href="#">6</a> |
| did not clear | step <a href="#">8</a> |

- 6 Ensure that the billing system is in recovery:

**post <streamname>**

- 7 In the display, look for the status of the billing stream.

| If the billing system | Do                                 |
|-----------------------|------------------------------------|
| is in recovery (Rcvy) | step <a href="#">12</a>            |
| is not in recovery    | contact your next level of support |

- 8 Perform the procedure [Adjusting disk space in response to SBA backup file system alarms on page 95](#)

- 9 Use Audit to clear the alarm.

| If the alarm  | Do                                 |
|---------------|------------------------------------|
| cleared       | step <a href="#">10</a>            |
| did not clear | contact your next level of support |

- 10 Ensure that the billing system is in recovery:

**post <streamname>**

**11** In the display, look for the status of the billing stream.

| <b>If the billing system</b> | <b>Do</b>                          |
|------------------------------|------------------------------------|
| is in recovery (Rcvy)        | step <a href="#">12</a>            |
| is not in recovery           | contact your next level of support |

**12** You have completed this procedure.

---

## Clearing a NOVOL alarm

---

### Purpose

Use this procedure to clear a no disk volume (NOVOL) alarm.

### Indication

NOVOL appears under the APPL header of the alarm banner at the MTC level of the MAP display and indicates a critical alarm for the backup system.

The core manager generates the SDMB820 log report when this alarm is raised.

### Meaning

On startup, the SBA backup file system is unable to find a volume in which to create a file. If the stream is configured as:

- both  
the alarm severity level is major
- on  
the alarm severity level is critical

#### **ATTENTION**

The option to configure a billing stream as both is only intended to be a temporary path while you are performing maintenance and alarm clearing tasks. The option to configure a billing stream to the both mode on a permanent basis is not supported.

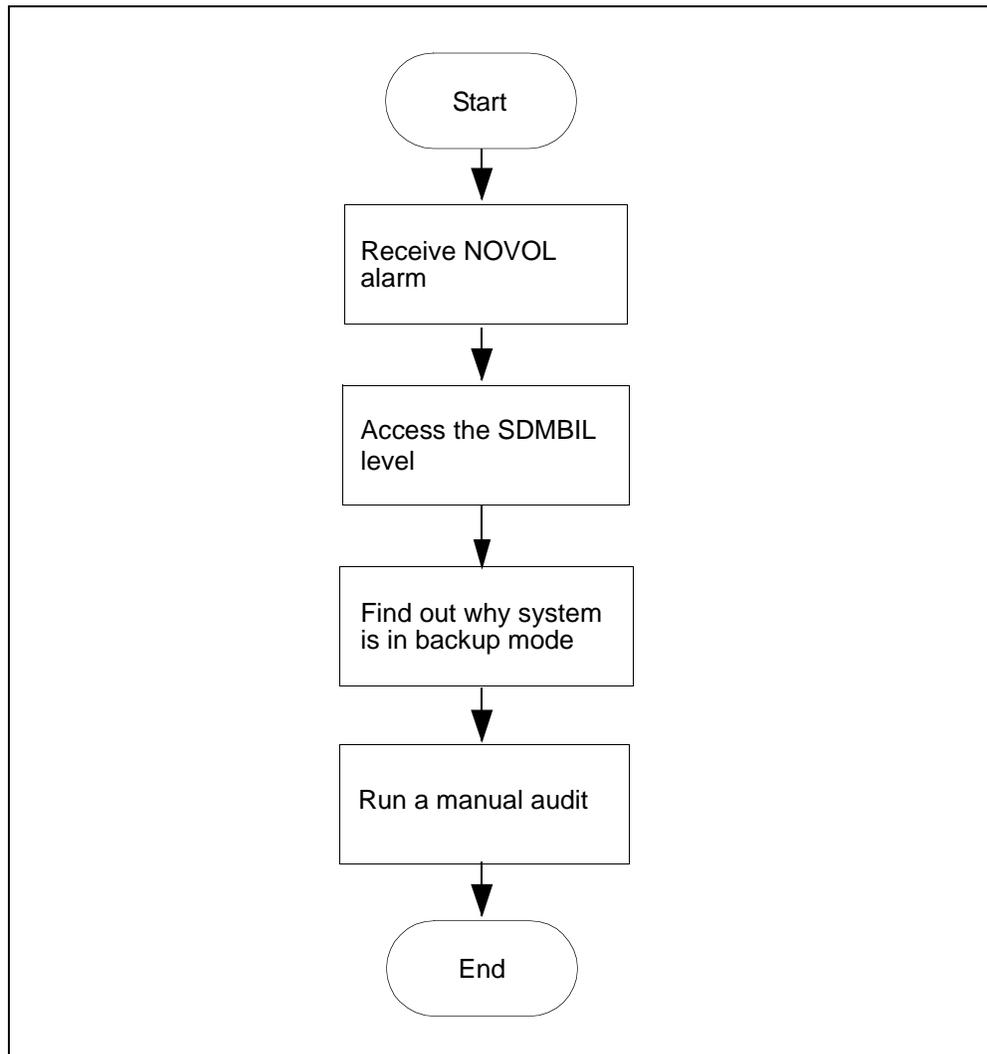
### Impact

Because there is no volume available for SBA storage, data intended for backup storage can be lost.

### Procedure

The following flowchart is a summary of the procedure. Use the instructions in the procedure to clear the alarm.

## NOVOL alarm clearing flowchart



**Note:** Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or \$, displayed by the system through a GUI or on a command line.

### Clearing a NOVOL alarm

#### *At the MAP*

- 1 Post the billing stream:  
`mapci;mtc;appl;sdbil;post <stream_name>`  
*where*  
`<stream_name>` is the name of the billing stream
- 2 Determine why the system is in backup mode.

- 3 Display all alarms that have been raised:

**DispAL**

- 4 Determine the status of the billing stream.

| If the billing stream is | Perform the following steps                                                                                 |
|--------------------------|-------------------------------------------------------------------------------------------------------------|
| SysB                     | perform the procedure for the alarm or the condition, and then go to step <a href="#">5</a> .               |
| RBsy                     | refer to <a href="#">Clearing a major SBACP alarm on page 136</a> , and then go to step <a href="#">5</a> . |
| ManB                     | Go to step <a href="#">8</a>                                                                                |
| Bkup                     | Go to step <a href="#">8</a>                                                                                |

- 5 Use Audit to clear the alarm.

| If the alarm  | Do                     |
|---------------|------------------------|
| cleared       | step <a href="#">6</a> |
| did not clear | step <a href="#">8</a> |

- 6 Ensure that the billing system is in recovery:

**post <streamname>**

- 7 In the display, look for the status of the billing stream.

| If the billing system | Do                                 |
|-----------------------|------------------------------------|
| is in recovery (Rcvy) | step <a href="#">12</a>            |
| is not in recovery    | contact your next level of support |

- 8 Perform the procedure [Adjusting disk space in response to SBA backup file system alarms on page 95](#)

- 9 Use Audit to clear the alarm.

| If the alarm  | Do                                 |
|---------------|------------------------------------|
| cleared       | step <a href="#">10</a>            |
| did not clear | contact your next level of support |

- 10 Ensure that the billing system is in recovery:

**post <streamname>**

**11** In the display, look for the status of the billing stream.

| <b>If the billing system</b> | <b>Do</b>                          |
|------------------------------|------------------------------------|
| is in recovery (Rcvy)        | step <a href="#">12</a>            |
| is not in recovery           | contact your next level of support |

**12** You have completed this procedure.

---

## Clearing an RTBCF alarm

---

### Indication

At the MTC level of the MAP display, RTBCF appears under the APPL header of the alarm banner. It indicates a critical alarm for the Real Time Billing (RTB) application.

The core manager generates the SDMB375 log report when this alarm is raised. When this alarm is cleared, the core manager generates the SDMB675 log report.

Refer to the log reports for more information about the condition causing the alarm.

### Meaning

The RTBCF alarm indicates that RTB is unable to transfer an open file after RTBMaxConsecutiveFailures.

### Impact

RTB will move to the SysB state, if RTB auto-recovery is OFF. RTB will move to the IsTb state, if RTB auto-recovery is ON. In either event, RTB stops transferring open files.

### Action

Refer to log report SDMB675 for more information about the RTBCF alarm. If required, contact your next level of support.

---

## Clearing an RTBER alarm

---

### Purpose

Use this procedure to clear an RTBER alarm.

### Indication

At the MTC level of the MAP display, RTBER appears under the APPL header of the alarm banner, and indicates a critical alarm for real time billing (RTB).

### Meaning

The RTBER alarm indicates that RTB has encountered a severe system error trying to re-establish file transfers with the data processing and management system (DPMS).

### Impact

This alarm has the following impact:

- RTB is unable to send billing files to the DPMS
- RTB moves to the SysB state
- the condition generates an SDMB375 log

### Action

#### *At the MAP*

- 1 Read the text in log SDMB375 for the cause of error.
- 2 Use the Logs reference documentation for SDMB375 to determine the actions to take to clear each type of error.
- 3 After you correct the error, return the RTB destination to service.  
The system generates SDMB675 when the error is corrected and the alarm is cleared.

---

## Clearing an RTBFM alarm

---

### Purpose

Use this procedure to clear an RTBFM alarm.

### Indication

At the MTC level of the MAP display, RTBFM appears under the APPL header of the alarm banner, indicating a critical alarm for the RTB program.

The core manager generates the SDMB375 log report when this alarm is raised. When this alarm is cleared, the core manager generates the SDMB675 log report. Refer to the log reports for more information about the condition causing the alarm.

### Meaning

The RTBFM alarm indicates that communication with the file manager is lost and that the file manager failed to close current active files.

### Impact

RTB will move to the SysB state, if RTB auto-recovery is OFF. RTB will move to the IsTb state, if RTB auto-recovery is ON.

### Action

Refer to log report SDMB675 for more information about the RTBFM alarm. If required, contact your next level of support.

**Note:** If the core manager is utilizing RTB streams, ensure that whenever you busy (BSY) and return the SBA application to service (RTS) you must also return any RTB streams to service separately.

The RTB stream does not return itself to service when the SBA application is returned to service.

Use the Query command to determine whether you have RTB streams running on your core manager.

---

## Clearing an RTBPD alarm

---

### Purpose

Use this procedure to clear an RTBPD alarm.

### Indication

At the MTC level of the MAP display, RTBPD appears under the APPL header of the alarm banner and indicates a critical alarm for the RTB program.

The core manager generates the SDMB375 log report when this alarm is raised. When this alarm is cleared, the core manager generates the SDMB675 log report.

### Meaning

The RTBPD alarm indicates that the RTB controlling process died and that RTB is halted.

### Impact

RTB moves to the SysB state.

### Action

Refer to log reports SDMB375 and SDMB675 for more information about the condition causing the alarm, and corrective actions. If required, contact your next level of support.

---

## Clearing an RTBST alarm

---

### Indication

At the MTC level of the MAP display, RTBST appears under the APPL header of the alarm banner and indicates a critical alarm for the RTB program.

The core manager generates the SDMB375 log report when this alarm is raised. When this alarm is cleared, the core manager generates the SDMB675 log report.

### Meaning

The RTBST alarm is raised if the schedule tuple is deleted or invalid for RTB.

### Impact

RTB moves to the SysB state.

### Action

Refer to the log reports for more information about the condition causing the alarm.

Refer to log report SDMB675 for more information about the RTBST alarm. You need to verify that the

- protocol is set to RFTPW, and
- file format type is set to "DIRP" in the schedule tuple associated with the alarm

If required, contact your next level of support.

## Clearing a major SBACP alarm

### Purpose

Use this procedure to clear an SBACP alarm.

### Indication

At the MTC level of the MAP display, SBACP appears under the APPL header of the alarm banner and indicates a major alarm for the SDM Billing Application (SBA).

### Meaning

The SBA is shutting down because either

- a user busied the SBA or the core manager, or
- a process is repeatedly dying and the SBA shut down

### Impact

The SBA on the core manager is out of service and billing records are being written to backup volumes on the core.

### Action

Use the instructions in the following procedure to clear the alarm.

**Note:** Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or \$, displayed by the system through a GUI or on a command line.

#### *At the core manager*

- 1 Go to the Appl level of the mtc tool by typing:

```
mtc appl
```

| If the SBA application is            | Do                                 |
|--------------------------------------|------------------------------------|
| ISTB, Offl, or SysB                  | step <a href="#">2</a>             |
| ManB                                 | step <a href="#">3</a>             |
| InSv, and the alarm is cleared       | step <a href="#">10</a>            |
| InSv, but the alarm is still present | contact your next level of support |

- 2 Busy the SBA application:

```
bsy <SBA_no>
```

where

<SBA\_no> is the number next to the SBA application.

- 3 Return the SBA application to service:

**rts <SBA\_no>**

*where*

<SBA\_no> is the number of the SBA application.

**Note:** Any streams configured for real-time billing (RTB) are also returned to service.

Log report SDMB375 is generated when a stream configured for RTB fails to return to service.

| If the SBA                                                      | Do                                 |
|-----------------------------------------------------------------|------------------------------------|
| returned to service successfully and the alarm is cleared       | step <a href="#">4</a>             |
| returned to service successfully and the alarm is still present | contact your next level of support |
| did not return to service successfully                          | contact your next level of support |

- 4 Return the RTB streams to service. Exit the maintenance interface.

**quit all**

- 5 Access the billing maintenance level:

**billmtc**

- 6 Access the schedule level:

**schedule**

- 7 Access the real-time billing level:

**rtb**

- 8 Busy the stream:

**bsy <stream\_name> DIRP <destination\_name>**

*where:*

**<stream\_name>**

is the name of the billing stream configured for RTB (for example OCC)

- 9 Return the stream to service:

```
rts <stream name> DIRP <destination_name>
```

where:

**<stream name>**

is the name of the billing stream configured for RTB (for example OCC)

| <b>If the billing stream configured for RTB</b> | <b>Do</b>                          |
|-------------------------------------------------|------------------------------------|
| returns to service successfully                 | you have completed this procedure  |
| does not return to service successfully         | contact your next level of support |

- 10 You have completed this procedure.

## Clearing a minor SBACP alarm

---

### Indication

At the MTC level of the MAP display, SBACP appears under the APPL header of the alarm banner, and indicates a minor alarm for the SBA program.

### Meaning

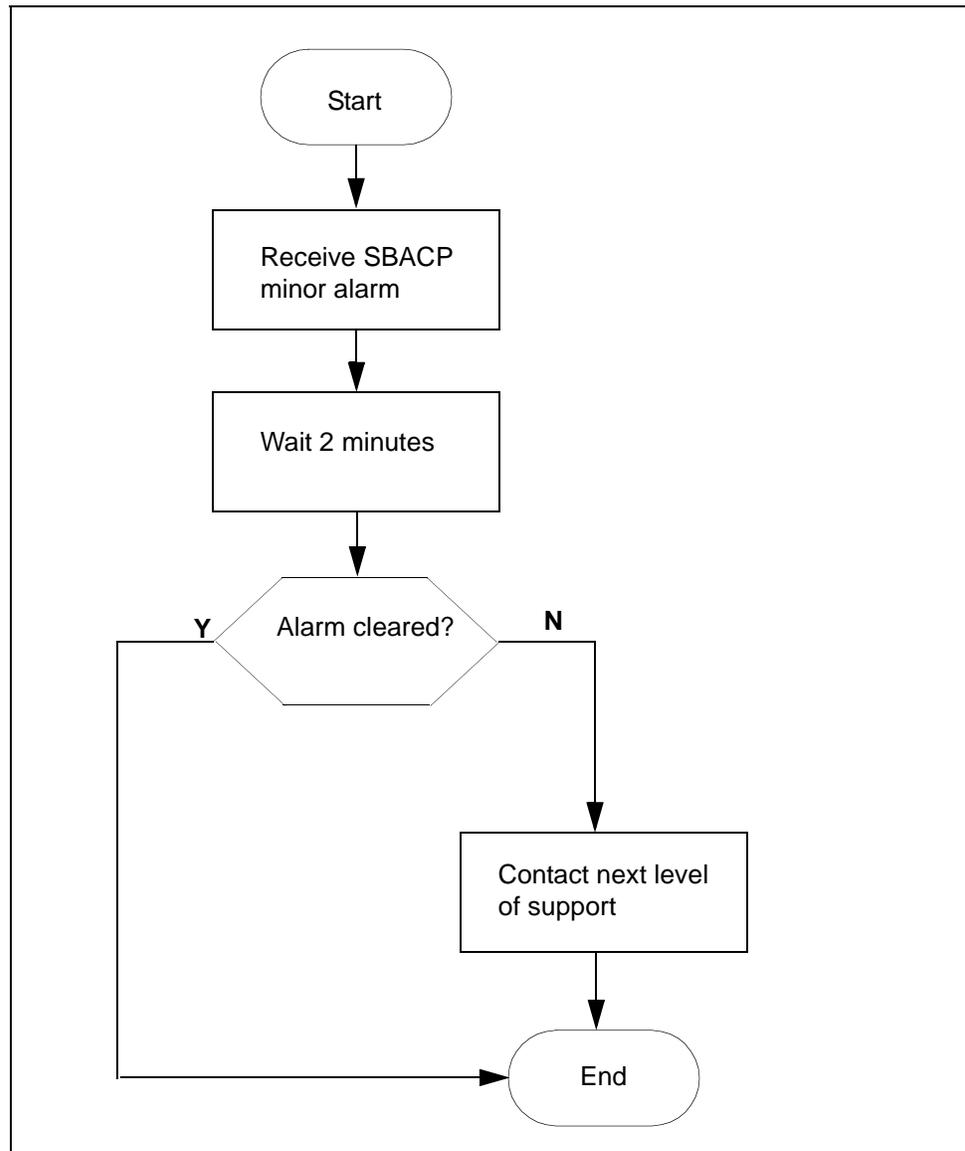
The SBA program is shutting down because one of the processes has failed three times in one minute.

### Impact

The SBA program ends, but restarts within two minutes.

### Action

The following flowchart is a summary of the procedure. Use the instructions in the following procedure to clear the alarm.

**SBACP (minor) alarm clearing flowchart****Clearing a minor SBACP alarm*****At the MAP***

- 1 Wait 2 minutes for the SBA to restart.
- 2 Contact your next level of support if the
  - alarm does not clear, or
  - SBA application fails three times within one minute
- 3 You have completed the procedure.

---

## Clearing an SBAIF alarm

---

### Purpose

Use this procedure to clear a SuperNode Billing Manager file transfer (SBAIF) alarm.

### Indication

At the MTC level of the MAP display, SBAIF appears under the APPL header of the alarm banner and indicates a major alarm.

The system also generates an SDMB390 log.

### Meaning

SuperNode Billing Application (SBA) cannot perform a scheduled transfer of billing files from the core manager to a downstream destination.

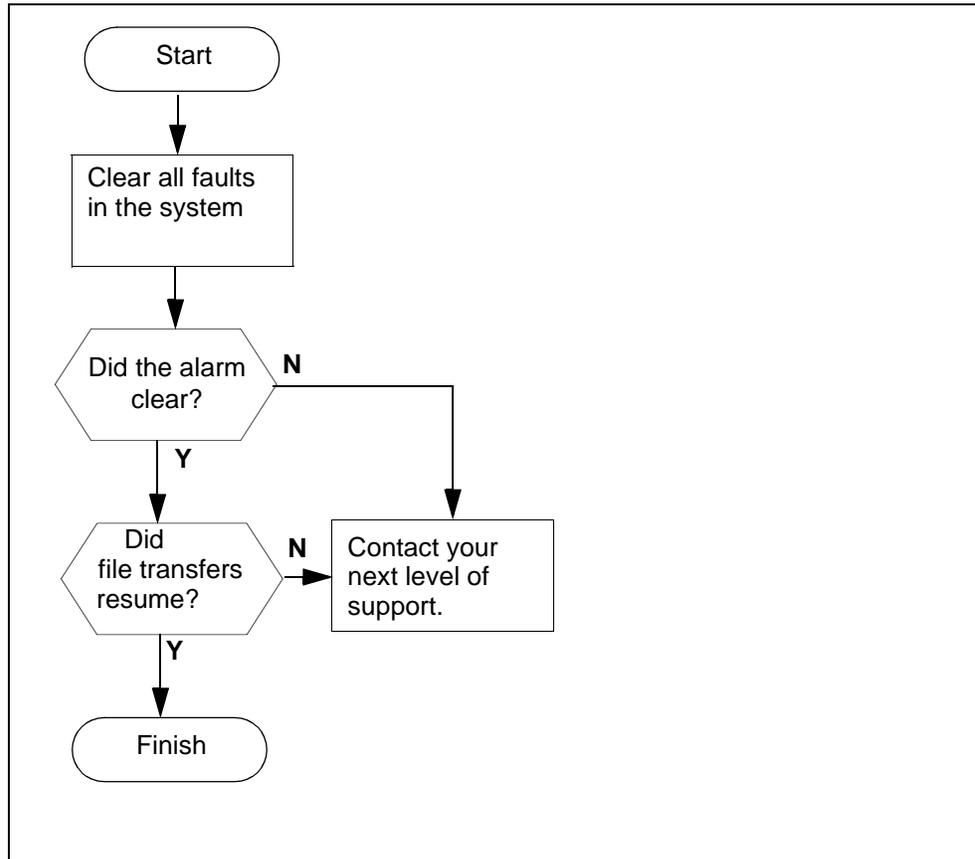
### Impact

If the alarm does not clear, SBA is not able to transfer files to the downstream destination:

- SBA uses local storage on the core manager to store billing files. Alarms are generated as SBA uses available capacity.
- if local storage becomes full, the Core is unable to send billing records to the core manager. The Core sends the billing records to backup storage. Alarms are generated as the Core uses available capacity.

### Action

The following flowchart is a summary of the procedure. Use the instructions in the procedure to clear the alarm.

**SBAIF alarm clearing flowchart****Clearing an SBAIF alarm*****At a workstation or console***

- 1 Clear all faults in the system using the appropriate procedures in this document.

The SBAIF alarm clears when the fault is corrected.

| If the SBAIF alarm | Do                                  |
|--------------------|-------------------------------------|
| clears             | step <a href="#">2</a>              |
| does not clear     | Contact your next level of support. |

- 2 Access the core manager.

- 3 Monitor the billing-related logs and look for log SDMB690, which indicates that the SBAIF alarm has cleared.

| If log SDMB690 | Do                                  |
|----------------|-------------------------------------|
| is present     | step <a href="#">4</a>              |
| is not present | contact your next level of support. |

- 4 Make sure SBA successfully performs a scheduled transfer of billing files. Monitor billing-related logs and look for log SDMB691, which indicates the file transfer schedule is now working for the stream.

**Note:** The length of time for SBA to resume transferring billing files depends on the following configured parameters:

- the number of active scheduled tuples
- the time interval to transfer files

| If                                                                                                | Do                                 |
|---------------------------------------------------------------------------------------------------|------------------------------------|
| log SDMB691 indicates the file transfer schedule is now working for the stream.                   | step <a href="#">5</a>             |
| log SDMB691 or any other log indicates a new problem with the scheduled transfer of billing files | contact your next level of support |

- 5 You have completed this procedure.

## Verifying the file transfer protocol

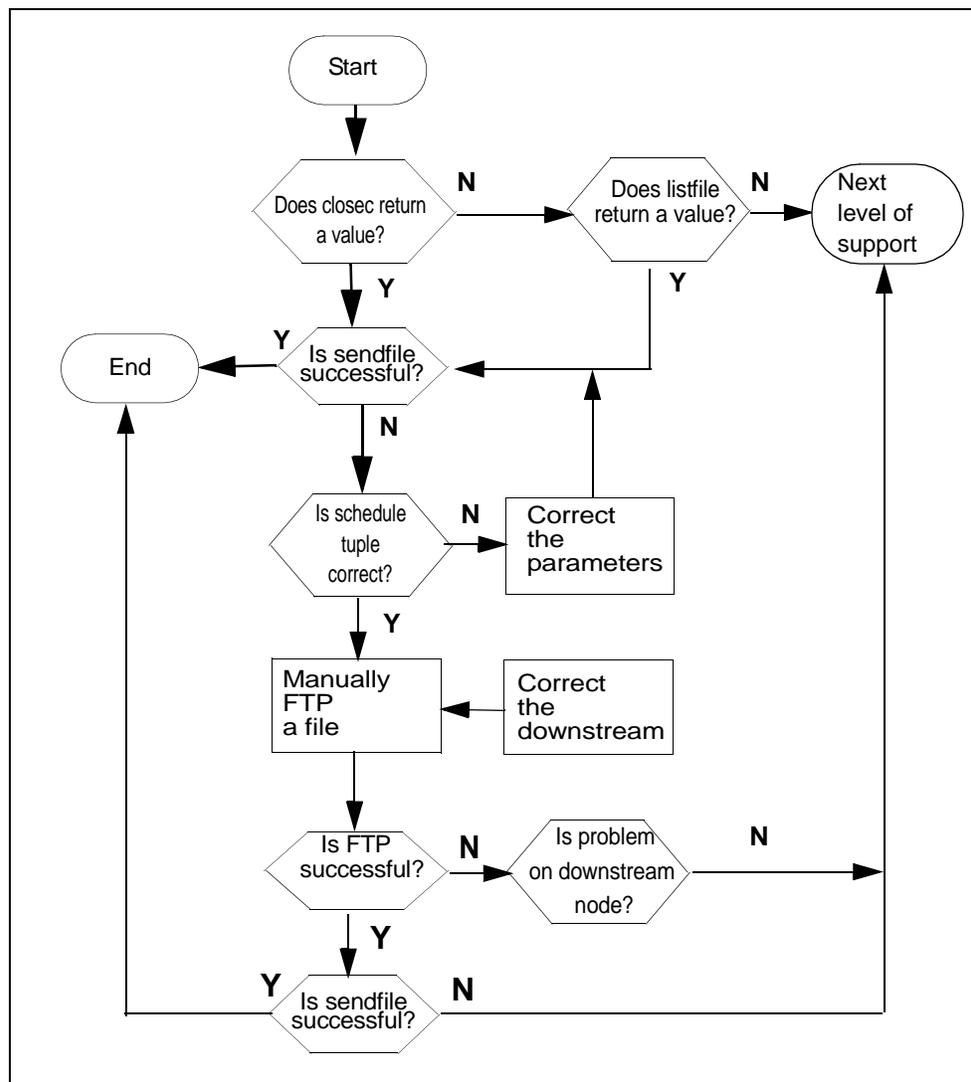
### Purpose

You can use this procedure on the core manager to verify that the file transfer protocol (FTP) is configured correctly to transfer files.

### Action

The following flowchart summarizes the steps outlined in the procedure.

**FTP verification flowchart**



**Note:** Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or \$, displayed by the system through a GUI or on a command line.

## Verify the FTP

### At the core manager

- 1 Access the bill maintenance level:

**billmtc**

- 2 Access the file system:

**filesys**

- 3 Close active billing files:

**closec <stream\_name>**

*where*

**<stream\_name>** is the name of the stream.

**Note:** You must close any active billing files prior to the FTP process.

- 4 Determine the results of the closec command.

| If the “closec” command    | Do                     |
|----------------------------|------------------------|
| returns a filename         | step <a href="#">7</a> |
| does not return a filename | step <a href="#">5</a> |

- 5 List the primary file (closedNotSent directory):

**listfile <stream\_name>**

*where*

**<stream\_name>** is the name of the stream

- 6 If the listfile command does not return a filename, contact your next level of support because this can indicate a problem with billing generation.

- 7 Send the primary file (closedNotSent directory):

**sendfile <stream\_name>**

*where*

**<stream\_name>** is the name of the stream.

**Note:** The sendfile command sends the billing file to the operating company billing collector.

8 Go to the previous level:

**quit**

9 Determine the results of the sendfile command.

| If the “sendfile” command is | Do                                |
|------------------------------|-----------------------------------|
| successful                   | you have completed this procedure |
| not successful               | step <a href="#">10</a>           |

**Note:** Observe the SDMB logs on the CM in logutil to determine why the `sendfile` command is not successful prior to continuing with step [10](#).

10 Access the schedule level:

**schedule**

11 List the parameters of the schedule tuple:

**list**

| If the parameters are                   | Do                      |
|-----------------------------------------|-------------------------|
| correct, but you are receiving an alarm | step <a href="#">21</a> |
| incorrect                               | step <a href="#">12</a> |

12 Reset the schedule tuple parameters:

**change**

13 Enter the stream name (name of billing file).

14 Enter the file format.

15 Enter the destination name.

**Note:** The destination name can be up to 15 alphanumeric characters.

16 Observe the schedule tuple displayed.

17 Enter the corrected parameters.

**Note:** You can change parameters one at a time or you can choose to change the entire schedule tuple.

18 Enter the new values of the parameters you have chosen to change.

- 19 Save the changed parameters:

**save**

| If you have                                    | Do                                                                                                                                                                                                                                                                                                                       |
|------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| corrected the parameters in the schedule tuple | step <a href="#">7</a>                                                                                                                                                                                                                                                                                                   |
| determined that the parameters are correct     | <ul style="list-style-type: none"> <li>step <a href="#">20</a> (verify login and write permissions are correct for FTP process without testing a billing file),<br/>OR</li> <li>step <a href="#">23</a> (verify login and write permissions are correct for FTP process while testing an actual billing file)</li> </ul> |

- 20 Exit the maintenance interface:

**quit all**

- 21 Login as root user.

- 22 Attempt to FTP any billing file to the destination used by the “sendfile” command. This action verifies that FTP is functioning properly for the node and directory.

**Note:** You can use any billing file for step [22](#) because you are only verifying login and write ability on the downstream node.

- 23 Exit back to the command prompt:

**quit all**

- 24 Login as root user.

- 25 Copy a billing file from the closedNotSent directory to a temporary directory:

```
cp /<logical_vol>/closedNotSent/<file> /tmp
```

where

**<logical\_vol>** is the logical volume for the stream that is in use

**<file>** is the name of the billing file in the closedNotSent directory

**Note:** You can obtain the logical volume from the `confstrm` level of the `billmtc` by requesting a list on the stream.

- 26 Access the /tmp directory:  
**cd /tmp**
- 27 FTP to the downstream node:  
**ftp <address> <port>**  
*where*  
**<address>** is the Primary\_Destination IP address of the destination node  
**<port>** is the Primary\_Port of the destination node
- 28 Log onto the node when prompted by the FTP (Remote\_Login and Remote\_Password defined in the schedule tuple):  
**Note:** A successful login is confirmed by a “230 User <user\_name> logged in” message returned by the FTP.  
If the login attempt is unsuccessful, obtain a valid login ID and password and update the schedule tuple with the valid values.
- 29 Change the directory to the one the schedule tuple is using:  
**ftp> cd <remote\_directory>**  
*where*  
**<remote\_directory>** is the Remote\_Storage\_Directory defined in the schedule tuple.  
**Note:** A successful login is confirmed by a “250 CWD command successful” message returned by the FTP.
- 30 If the “cd” command is unsuccessful, obtain a valid directory from the downstream node and update the schedule tuple with the valid values.
- 31 Set the file transfer mode to binary:  
**ftp> binary**  
**Note:** A successful command is confirmed by a “200 Type set to I” message returned by the FTP.
- 32 Execute the “structure” command and verify the returned message:  
**ftp> stru f**  
**Note:** The response from a UNIX machine for a successful command would be: “We only support file structure, sorry.”  
The response from an AS400 machine for a successful command would be: “250 Data structure is File”.

- 33** Attempt to write a file to the destination node directory used for billing:

```
ftp> put <file> <file.tmp>
```

where

**<file>** is the name of a billing file that is copied to the /tmp directory in step [25](#).

**<file.tmp>** is the name of the billing file with the .tmp extension appended.

**Note:** The responses from a UNIX machine for a valid command would be “200 PORT command successful” and “226 Transfer complete”.

- 34** Rename the <file.tmp> file:

```
ftp> rename <file.tmp> <file>
```

where

**<file.tmp>** is the name of the billing file with .tmp extension appended that you created in step [33](#).

**<file>** is the name of billing file to which the .tmp extension was appended in step [33](#).

**Note:** The responses from a UNIX machine for a valid command would be “350 File exists, ready for destination name” and “250 RNTD command successful”.

- 35** Exit from the FTP session:

```
ftp> quit
```

| If the file transfer is                               | Do                      |
|-------------------------------------------------------|-------------------------|
| successful                                            | step <a href="#">38</a> |
| unsuccessful because of a permission error            | step <a href="#">36</a> |
| unsuccessful for a reason other than permission error | step <a href="#">38</a> |

- 36** Correct the directory permissions to allow write access.

- 37** Repeat steps [21](#) through [35](#).

- 38** Send the primary files in the closedNotSent directory:

```
sendfile <billing_stream> dest <dest_name>
```

where

**<billing\_stream>** is the name of the billing stream

**<dest\_name>** is the name you choose to name the destination (for example, fraud detection).

**Note:** The `sendfile` command with the `dest` option sends the billing file to the specified destination only.

| If the “sendfile” command is | Do                                 |
|------------------------------|------------------------------------|
| successful                   | you have completed this procedure  |
| unsuccessful                 | contact your next level of support |

## Verifying the FTP Schedule

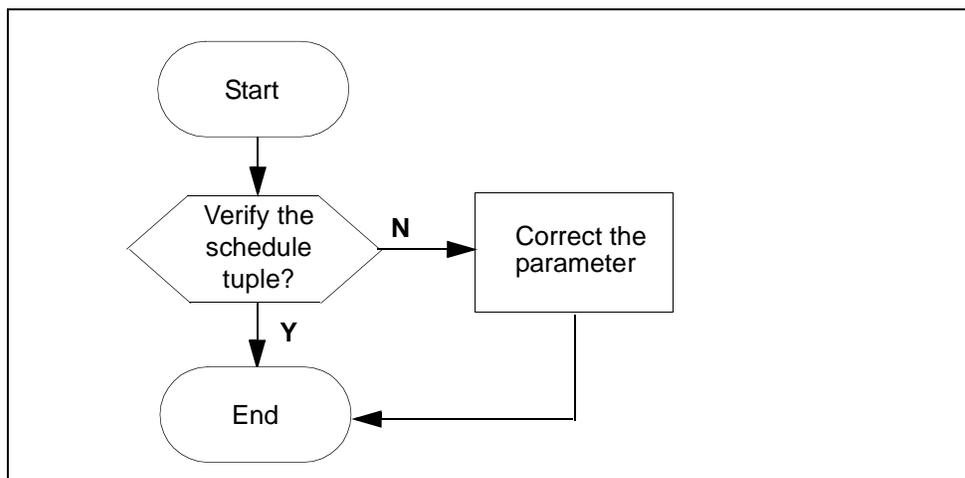
### Purpose

You can use this procedure to verify that the schedule is configured correctly and can transfer files using FTP.

### Action

The following flowchart summarizes the steps in the procedure.

#### Verifying the FTP schedule flowchart



**Note:** Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or \$, displayed by the system through a GUI or on a command line.

#### Verifying the FTP schedule

##### *At any workstation or console*

- 1 Log in to the core manager.
- 2 Access the bill maintenance level:  
**billmtc**
- 3 Verify the schedule tuple:  
**schedule**

- 4 List the parameters of the schedule tuple:

**list**

| If the parameters are | Do                                 |
|-----------------------|------------------------------------|
| correct               | contact your next level of support |
| incorrect             | step <a href="#">5</a>             |

- 5 Reset the schedule tuple parameters:

**change**

- 6 Enter the stream name (billing file name).  
 7 Enter the file format.  
 8 Enter the destination name.

**Note:** The destination name can be up to 15 alphanumeric characters.

- 9 Observe the schedule tuple displayed.

- 10 Enter the parameters that you need to correct.

**Note:** You can change parameters one at a time or you can choose to change the entire schedule tuple.

- 11 Enter the new values of the parameters you have chosen to change.

- 12 Save the changed parameters:

**save**

| If the parameters are                    | Do                                 |
|------------------------------------------|------------------------------------|
| correct, but still receiving an alarm    | contact your next level of support |
| correct and no longer receiving an alarm | step <a href="#">13</a>            |

- 13 Wait for the next scheduled transfer to execute after the scheduled transfer interval for the alarm not to appear.

- 14 You have completed the procedure.

---

## Replacing one or more failed disk drives on an SSPFS-based server

---

### Application

Use this procedure to replace one or more failed disk drives on a Succession Server Platform Foundation Software (SSPFS)-based server (a Netra t1400 or a Netra 240 server). Also use this procedure if a disk drive was pulled out by mistake. Simply re-inserting the disk is not sufficient to recover.

Disk failures will appear as IO errors or SCSI errors from the Solaris kernel. These messages will appear in the system log and on the console terminal. To indicate a disk failure, log SPFS310 is generated, and an alarm light is illuminated on the front panel. After the disk is replaced, the alarm light will go off within a few minutes.

Systems installed with SSPFS use disk mirroring. With mirrored hot-swap disks, a single failed disk can be replaced without interrupting the applications running on the server. Thus, a single disk can be replaced while the system is in-service. Follow one of the links below for a view of the disks on a Netra t1400 and Netra 240:

- [Netra t1400 on page 154](#)
- [Netra 240 on page 155](#)

The steps to replace a failed drive are to identify the failed drive, replace it physically, and replace it logically.

Follow one of the links below according to your office configuration to replace the failed disk drives:

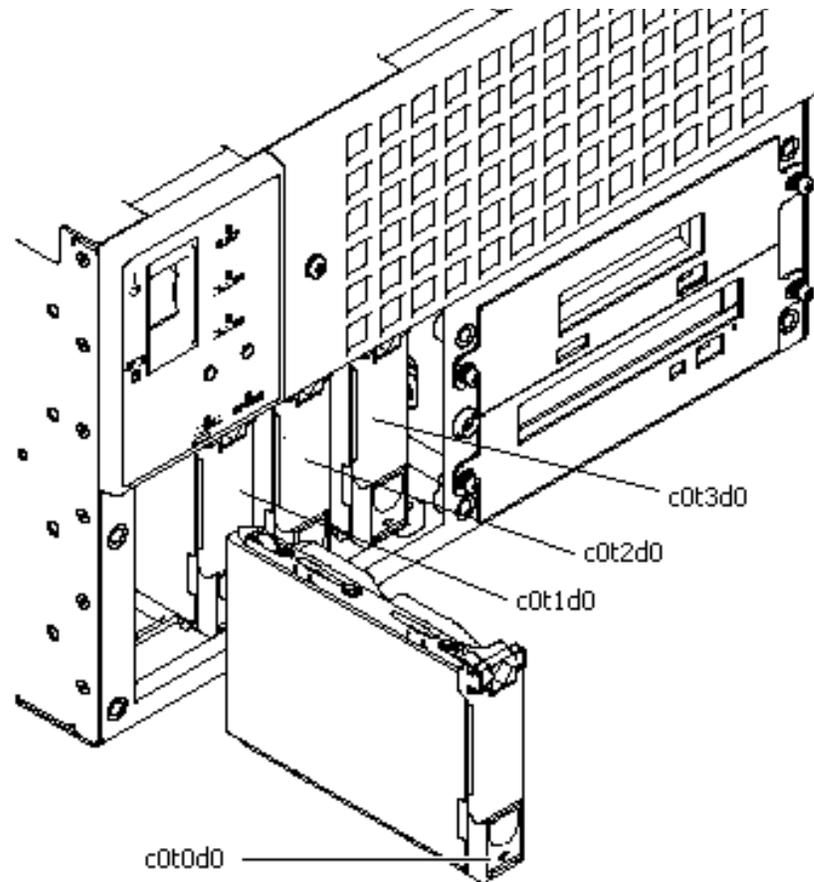
- [Replacing failed disks on a Netra t1400 on page 156](#)
- [Replacing failed disks on a Netra 240 simplex on page 159](#)
- [Replacing failed disks on a Netra 240 cluster \(two-server\) on page 161](#)

## Netra t1400

Each Netra t1400 is equipped with four hot-swap drives: “c0t0d0”, “c0t1d0”, “c0t2d0”, and “c0t3d0”. Each physical drive is divided into slices, which are named based on the physical disk and a slice number. For example, “c0t0d0s0” is the first slice of the physical disk “c0t0d0”.

The following figure identifies the disk drives of the Netra t1400.

### Netra t1400 disk drives

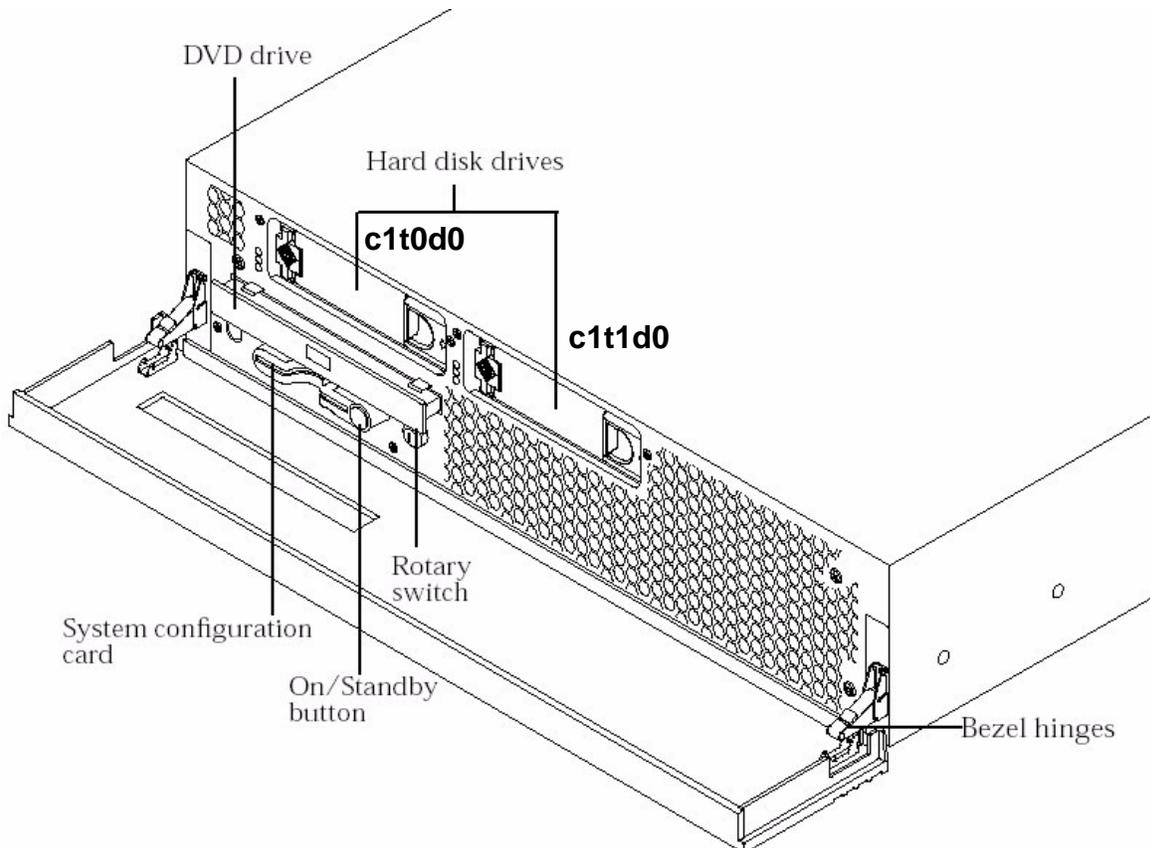


## Netra 240

Each Netra 240 is equipped with two hot-swap drives: “c1t0d0”, and “c1t1d0”.

The following figure identifies the disk drives of the Netra 240.

### Netra 240 disk drives



## Prerequisites

You have a replacement disk.

## Action

Perform the following steps to complete this procedure.

### Replacing failed disks on a Netra t1400

#### At the server

- 1 Locate the failed disk(s) using figure [Netra t1400 disk drives on page 154](#).
- 2 Physically replace the disk using the documentation for the Netra t1400. When complete, proceed with step [3](#) in this procedure to logically replace the disk.

**Note:** If more than one disk needs to be replaced, physically replace one disk and return to this procedure to logically replace the disk (step [3](#)), before you proceed to physically replace the next failed disk.

#### At your workstation

- 3 Logically replace the disk you just physically replaced.

| If you physically replaced | Do                     |
|----------------------------|------------------------|
| c0t0d0                     | step <a href="#">a</a> |
| c0t1d0                     | step <a href="#">b</a> |
| c0t2d0                     | step <a href="#">c</a> |
| c0t3d0                     | step <a href="#">d</a> |

- a Logically replace disk “c0t0d0” by entering the following sequence of commands:

```
# metadb -d c0t0d0s7
# prtvtoc -h /dev/rdisk/c0t1d0s2 | fmthard -s
- /dev/rdisk/c0t0d0s2
# metadb -a c0t0d0s7
# metareplace -e d2 c0t0d0s1
# metareplace -e d5 c0t0d0s0
# metareplace -e d8 c0t0d0s3
# metareplace -e d11 c0t0d0s4
# metareplace -e d100 c0t0d0s5
```

Proceed to step [4](#)

- b Logically replace disk “c0t1d0” by entering the following sequence of commands.

```
# metadb -d c0t1d0s7
# prtvtoc -h /dev/rdisk/c0t0d0s2 | fmthard -s
- /dev/rdisk/c0t1d0s2
# metadb -a c0t1d0s7
# metareplace -e d2 c0t1d0s1
# metareplace -e d5 c0t1d0s0
# metareplace -e d8 c0t1d0s3
# metareplace -e d11 c0t1d0s4
# metareplace -e d100 c0t1d0s5
```

Proceed to step [4](#)

- c Logically replace disk “c0t2d0” by entering the following sequence of commands.

```
# metadb -d c0t2d0s7
# prtvtoc -h /dev/rdisk/c0t3d0s2 | fmthard -s
- /dev/rdisk/c0t2d0s2
# metadb -a cot2d0s7
# metareplace -e d100 c0t2d0s0
```

Proceed to step [4](#)

- d Logically replace disk “c0t3d0” by entering the following sequence of commands.

```
# metadb -d c0t3d0s7
# prtvtoc -h /dev/rdisk/c0t2d0s2 | fmthard -s
- /dev/rdisk/c0t3d0s2
# metadb -a c0t3d0s7
# metareplace -e d100 c0t3d0s0
```

Proceed to step [4](#)

- 4 Use the following table to determine your next step.

| If you                                         | Do                     |
|------------------------------------------------|------------------------|
| have another disk to physically replace        | step <a href="#">1</a> |
| do not have another disk to physically replace | step <a href="#">5</a> |

- 5 Use the following table to determine your next step.

| If you replaced                                                                         | Do                                |
|-----------------------------------------------------------------------------------------|-----------------------------------|
| 1 disk                                                                                  | you have completed this procedure |
| 2 non-mirrored disks (i.e. c0t0d0 and c0t2d0 or c0t3d0, or c0t1d0 and c0t2d0 or c0t3d0) | you have completed this procedure |
| 2 mirrored disks (i.e. c0t0d0 and c0t1d0, or c0t2d0 and c0t3d0)                         | step <a href="#">6</a>            |
| 3 disks                                                                                 | step <a href="#">6</a>            |
| 4 disks                                                                                 | step <a href="#">6</a>            |

- 6 Restore the file systems and oracle data. If required, refer to procedure “Performing a full system restore on a Sun server - SN06.2 or greater” in the ATM/IP Security and Administration document, NN10402-600.

**Note:** As long as one disk from each pair is good, the data in the system is intact. When both disks in a pair fail, the data needs to be restored.

You have completed this procedure.

## Replacing failed disks on a Netra 240 simplex

### At the server

- 1 Locate the failed disk(s) using figure [Netra 240 disk drives on page 155](#).
- 2 Physically replace the disk using the documentation for the Netra 240. When complete, proceed with step [3](#) in this procedure to logically replace the disk.

**Note:** If both disks need to be replaced, physically replace one disk and return to this procedure to logically replace the disk (step [3](#)), before you proceed to physically replace the other failed disk.

### At your workstation

- 3 Logically replace the disk you just physically replaced.

| If you physically replaced | Do                     |
|----------------------------|------------------------|
| c1t0d0                     | step <a href="#">a</a> |
| c1t1d0                     | step <a href="#">b</a> |

- a Logically replace disk “c1t0d0” by entering the following sequence of commands:

```
# metadb -d c1t0d0s7
# prtvtoc -h /dev/rdisk/c1t1d0s2 | fmthard -s
- /dev/rdisk/c1t0d0s2
# metadb -a c1t0d0s7
# metareplace -e d2 c1t0d0s1
# metareplace -e d5 c1t0d0s0
# metareplace -e d8 c1t0d0s3
# metareplace -e d11 c1t0d0s4
# metareplace -e d100 c1t0d0s5
```

Proceed to step [4](#)

- b Logically replace disk “c1t1d0” by entering the following sequence of commands:

```
# metadb -d c1t1d0s7
# prtvtoc -h /dev/rdisk/c1t1d0s2 | fmthard -s
- /dev/rdisk/c1t1d0s2
# metadb -a c1t1d0s7
# metareplace -e d2 c1t1d0s1
# metareplace -e d5 c1t1d0s0
# metareplace -e d8 c1t1d0s3
# metareplace -e d11 c1t1d0s4
# metareplace -e d100 c1t1d0s5
```

Proceed to step [4](#)

- 4 Use the following table to determine your next step.

| If you                              | Do                     |
|-------------------------------------|------------------------|
| have another disk to replace        | step <a href="#">1</a> |
| do not have another disk to replace | step <a href="#">5</a> |

- 5 Use the following table to determine your next step.

| If you replaced | Do                                |
|-----------------|-----------------------------------|
| 1 disk          | you have completed this procedure |
| both disks      | step <a href="#">6</a>            |

- 6 Restore the file systems and oracle data. If required, refer to procedure “Performing a full system restore on a Sun server - SN06.2 or greater” in the ATM/IP Security and Administration document, NN10402-600.

**Note:** As long as one disk is good, the data in the system is intact. When both disks fail, the data needs to be restored.

You have completed this procedure.

## Replacing failed disks on a Netra 240 cluster (two-server)

### *At the server*

- 1 Locate the failed disk(s) using figure [Netra 240 disk drives on page 155](#).
- 2 Use the following guidelines to determine the steps you need to do, and do only those steps in the order they appear:
  - **to replace one disk on one unit**
    - physically replace the disk (step [3](#))
    - logically replace this disk (step [4](#))
  - **to replace one disk on each unit**
    - physically replace the disk on the Active unit first (step [3](#))
    - logically replace this disk (step [4](#))
    - physically replace the disk on the other unit (step [3](#))
    - logically replace this disk (step [4](#))
  - **to replace both disks on a unit**
    - physically replace one disk on the unit (step [3](#))
    - logically replace this disk (step [4](#))
    - physically replace the other disk on this unit (step [3](#))
    - logically replace this disk (step [4](#))
    - clone the image from the Active unit onto this unit (step [6](#))
  - **to replace three disks**
    - physically replace the disk on the Active unit first (step [3](#))
    - logically replace this disk (step [4](#))
    - physically replace one disk on the other unit (step [3](#))
    - logically replace this disk (step [4](#))
    - physically replace the other disk on this same unit (step [3](#))
    - logically replace this disk (step [4](#))
    - clone the image from the Active unit onto this unit (step [6](#))

- **to replace four disks**
    - physically replace one disk on the unit with the most recent backup (step [3](#))
    - logically replace this disk (step [4](#))
    - physically replace the other disk on this same unit (step [3](#))
    - logically replace this disk (step [4](#))
    - restore the file systems and oracle data on this unit (step [5](#))
    - physically replace one disk on the other unit (step [3](#))
    - logically replace this disk (step [4](#))
    - physically replace the other disk on this same unit (step [3](#))
    - logically replace this disk (step [4](#))
    - clone the image from the Active unit onto this unit (step [6](#))
- 3** Physically replace the disk using the documentation for the Netra 240. When complete, proceed with step [4](#) in this procedure to logically replace the disk.

***At your workstation***

- 4** Logically replace the disk you just physically replaced.

| If you physically replaced | Do                     |
|----------------------------|------------------------|
| c1t0d0                     | step <a href="#">a</a> |
| c1t1d0                     | step <a href="#">b</a> |

- a Logically replace disk “c1t0d0” by entering the following sequence of commands:

```
# metadb -d c1t0d0s7
# prtvtoc -h /dev/rdisk/c1t1d0s2 | fmthard -s
- /dev/rdisk/c1t0d0s2
# metadb -a c1t0d0s7
# metareplace -e d2 c1t0d0s1
# metareplace -e d5 c1t0d0s0
# metareplace -e d8 c1t0d0s3
# metareplace -e d11 c1t0d0s4
# metareplace -e d100 c1t0d0s5
```

- b Logically replace disk “c1t1d0” by entering the following sequence of commands:

```
# metadb -d c1t1d0s7
# prtvtoc -h /dev/rdisk/c1t1d0s2 | fmthard -s
- /dev/rdisk/c1t1d0s2
# metadb -a c1t1d0s7
# metareplace -e d2 c1t1d0s1
# metareplace -e d5 c1t1d0s0
# metareplace -e d8 c1t1d0s3
# metareplace -e d11 c1t1d0s4
# metareplace -e d100 c1t1d0s5
```

- 5 Restore the file systems and oracle data. If required, refer to procedure “Performing a full system restore on a Sun server - SN06.2 or greater” in the ATM/IP Security and Administration document, NN10402-600.

**Note:** As long as one disk is good, the data in the system is intact. When both disks fail, the data needs to be restored.

- 6 Clone the data from the Active unit. If required, refer to procedure “Cloning the image of one node in a cluster to the other node” in the ATM/IP Security and Administration document, NN10402-600.

You have completed this procedure.

---

## Shutting down an SSPFS-based server

---

### Application

Use this procedure to shut down a Succession Server Platform Foundation Software (SSPFS)-based server, which may be hosting one or more of the following components:

- CS 2000 Management Tools
- Integrated Element Management System (EMS)
- Audio Provisioning Server (APS)
- Media Gateway (MG) 9000 Manager
- CS 2000 SAM21 Manager
- Network Patch Manager
- Core Billing Manager (CBM)

**ATTENTION**

The SSPFS-based server may be hosting more than one of the above components, therefore, ensure it is acceptable to shut down the server.

Use one of the following procedures according to your office configuration:

- [One-server configuration on page 165](#)
- [Two-server \(cluster\) configuration on page 166](#)

### Prerequisites

You must have root user privileges.

## Action

Use one of the following procedures according to your office configuration:

- [One-server configuration on page 165](#)
- [Two-server \(cluster\) configuration on page 166](#)

### One-server configuration

#### *At your workstation*

- 1 Log in to the server by typing  
> **telnet <IP address>**  
and pressing the Enter key.  
where  
**IP address**  
is the IP address of the SSPFS-based server you want to power down
- 2 When prompted, enter your user ID and password.
- 3 Change to the root user by typing  
\$ **su - root**  
and pressing the Enter key.
- 4 When prompted, enter the root password.
- 5 Shut down the server by typing  
# **init 0**  
and pressing the Enter key.  
The server shuts down gracefully, and the telnet connection is closed.
- 6 If required, turn off the power to the server at the circuit breaker panel of the frame.
- 7 You have completed this procedure.  
To bring the server back up, turn on the power to the server at the circuit breaker panel of the frame. The server recovers on its own once power is restored.

## Two-server (cluster) configuration

### At your workstation

- 1 Log in to the Inactive server by typing

```
> telnet <IP address>
```

and pressing the Enter key.

where

#### IP address

is the physical IP address of the Inactive SSPFS-based server in the cluster you want to power down (unit 0 or unit 1)

- 2 When prompted, enter your user ID and password.

- 3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

- 4 When prompted, enter the root password.

**Note:** Ensure you are on the Inactive server by typing `ubmstat`. If `ClusterIndicatorACT` is displayed in the response, which indicates you are on the Active server, log out of that server and log in to the other server through telnet using the physical IP address of the other unit. The response must display `ClusterIndicatorSTBY`, which indicates you are on the Inactive server.

- 5 Shut down the Inactive server by typing

```
# init 0
```

and pressing the Enter key.

The server shuts down gracefully, and the telnet connection is closed.

- 6 If required, turn off the power to the Inactive server at the circuit breaker panel of the frame. You have completed a partial power down (one server).

If you want to perform a full power down (both servers), proceed to step [7](#), otherwise, you have completed this procedure.

7

**ATTENTION**

Only perform the remaining steps if you want to perform a full power down, which involves powering down both servers in the cluster.

Telnet to the Active server by typing

```
> telnet <IP address>
```

and pressing the Enter key.

where

**IP address**

is the physical IP address of the Active SSPFS-based server in the cluster you want to power down

**8** When prompted, enter your user ID and password.

**9** Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

**10** When prompted, enter the root password.

**11** Shut down the Active server by typing

```
# init 0
```

and pressing the Enter key.

The server shuts down gracefully, and the telnet connection is closed.

**12** If required, turn off the power to the servers at the circuit breaker panel of the frame. You have completed a full power down (two servers).

**13** You have completed this procedure.

To bring the servers back up, turn on the power to the servers at the circuit breaker panel of the frame. The servers recover on their own once power is restored.

---

## Preparing a CD-RW or DVD-RW for use

---

### Application

Use this procedure to verify the CD-RW or DVD-RW is ready for use when using it for the first time, or when you want to erase the contents of a used CD-RW or DVD-RW to use it again.

### Prerequisites

None

### Action

Perform the following steps to complete this procedure.

#### *At the server*

- 1 Insert the CD or DVD into the drive.

**Note:** Only rewriteable media can be erased. Verify that the CD or DVD you are attempting to erase is either a CD-RW or DVD-RW before inserting it into the drive.

#### *At your workstation*

- 2 Log in to the server by typing  
> **telnet <server>**  
and pressing the Enter key.

where

**server**

is the IP address or hostname of the SSPFS-based server

- 3 When prompted, enter your user ID and password.
- 4 Use the following table to determine your next step.

| If the CD or DVD is | Do                     |
|---------------------|------------------------|
| new                 | step <a href="#">5</a> |
| used                | step <a href="#">6</a> |

- 5 Verify the CD or DVD is ready for use by typing
- ```
$ cdrw -l
```
- and pressing the Enter key

If the system response	Do
provides the CD device	step <a href="#">10</a>
indicates “No CD writers found or no media in the drive”	step <a href="#">6</a>

- 6 Erase the contents of the CD or DVD by typing
- ```
$ cdrw -b all
```
- and pressing the Enter key

**Note:** Erasing a DVD-RW can take over two hours. You can also use the “fast” and “session” arguments. For more details, refer to the man pages by typing `man cdrw`.

- 7 Verify the CD or DVD is ready for use by typing
- ```
$ cdrw -l
```
- and pressing the Enter key

If the system response	Do
provides the CD device	step <a href="#">10</a>
indicates “No CD writers found or no media in the drive” or “Media in the device is not erasable”	step <a href="#">8</a>

- 8 Eject the CD from the drive as follows:
- a Ensure you are at the root directory level by typing
- ```
$ cd /
```
- and pressing the Enter key.

**b** Eject the CD by typing

```
# eject cdrom
```

and pressing the Enter key.

**Note:** If the DVD drive tray will not open after you have determined that the DVD drive is not busy and is not being read from or written to, enter the following commands:

```
# /etc/init.d/volmgt stop
```

```
# /etc/init.d/volmgt start
```

Then, press the eject button located on the front of the DVD drive.

**c** Remove the CD or DVD from the drive.

**9** Obtain another CD or DVD and repeat the process starting with step [4](#).

**10** Proceed to use the CD or DVD.

You have completed this procedure.

## Increasing the size of a file system on an SSPFS-based server

### Application

Use one of the following procedures to increase the size of a file system on a Succession Server Platform Foundation Software (SSPFS)-based server:

- [Simplex configuration \(one server\) on page 172](#)
- [High-availability configuration \(two servers\) on page 177](#)

It is recommended you perform this procedure during off-peak hours.

The Succession Server Platform Foundation Software (SSPFS) creates file systems to best fit the needs of applications. However, it may be necessary to increase the size of a file system.

Not all file systems can be increased. The table below lists the file systems that cannot be increased, and lists examples of those that can be increased.

**Note:** Not all the file systems that can be increased are listed.

### SSPFS file systems

| Cannot be increased | Can be increased (examples) |
|---------------------|-----------------------------|
| / (root)            | /data                       |
| /var                | /opt/nortel                 |
| /opt                | /data/oradata               |
| /tmp                | /audio_files                |
|                     | /PROV_data                  |
|                     | /user_audio_files           |
|                     | /data/qca                   |
|                     | /data/mg9kem/logs           |

While file systems are being increased, writes to the file system are blocked, and the system activity increases. The greater the size increase of a file system, the greater the impact on performance.

## Prerequisites

It is recommended that you back up your file systems and oracle data (if applicable) prior to performing this procedure. Refer to procedures [Performing a backup of oracle data on an SSPFS-based server on page 207](#) and [Performing a backup of file systems on an SSPFS-based server on page 184](#) if required.

## Action

Perform the following steps to complete this procedure.

### Simplex configuration (one server)

#### *At your workstation*

- 1 Log in to the server by typing  

```
> telnet <server>
```

and pressing the Enter key.  
where  
**server**  
is the IP address or host name of the server
- 2 When prompted, enter your user ID and password.
- 3 Change to the root user by typing  

```
$ su - root
```

and pressing the Enter key.
- 4 When prompted, enter the root password.

**5** Determine the amount of disk utilization by the file systems as follows:

**a** Access the command line interface by typing

```
# cli
```

and pressing the Enter key.

*Example response*

```
Command Line Interface
```

```
1 - View
```

```
2 - Configuration
```

```
3 - Other
```

```
X - exit
```

```
select -
```

**b** Enter the number next to the “View” option in the menu.

*Example response*

```
View
```

```
1 - sspfs_soft (Display Software  
Installation Level Of SSPFS)
```

```
2 - chk_sspfs (Check SSPFS Processes)
```

```
3 - sw_conf (The software configuration of  
the znc0s0jx)
```

```
4 - cpu_util (Overall CPU utilization)
```

```
5 - cpu_util_proc (CPU utilization by  
process)
```

```
6 - port_util (I/O port utilization)
```

```
7 - disk_util (Filesystem utilization)
```

```
X - exit
```

```
select -
```

- c Enter the number next to the “disk\_util” option in the menu.

*Example response*

```

=== Executing "disk_util"
Filesystem      kbytes   used   avail capacity  Mounted on
/dev/md/dsk/d2  4129290 1892027 2195971   47%      /
/proc           0         0         0         0%      /proc
fd              0         0         0         0%      /dev/fd
mnttab          0         0         0         0%      /etc/mnttab
/dev/md/dsk/d8  2053605  155600 1836397    8%      /var
swap            3505488    40 3505448    1%      /var/run
swap            524288     448 523840    1%      /tmp
/dev/md/dsk/d11 5161437 1428691 3681132   28%     /opt
/dev/md/dsk/d23 2031999   34313 1936727    2%     /PROU_data
/dev/md/dsk/d24 2031999  169042 1801998    9%     /audio_files
/dev/md/dsk/d20 3080022  294615 2723807   10%     /data
/dev/md/dsk/d25  949455  440344  452144   50%     /user_audio_files
/dev/md/dsk/d21 3080022  275962 2742460   10%     /opt/nortel
/dev/md/dsk/d22 12386331 10337214 1925254   85%     /data/oradata
/dev/md/dsk/d26  122847    1041  109522    1%     /data/qca
=== "disk_util" completed successfully

```

The “capacity” column indicates the percentage of disk utilization by the file system, which is specified in the “Mounted on” column.

- 6 Note the file system you want to increase, as well as its current size (under column “Kbytes”).
- 7 Exit each menu level of the command line interface to eventually exit the command line interface, by typing

```
select - x
```

and pressing the Enter key.

8

#### ATTENTION

Before you proceed with this procedure, ensure the file system you want to increase is full or nearly full and that its content is valid application data. Remove any unneeded files or files generated in error that are taking up disk space.

Determine the size by which to increase the file system, by subtracting the desired size for the file system based on your specific needs, from its current size (noted in [6](#)).

For example, to determine the size by which to increase the “qca” file system, subtract its current size, 122847k from the desired size, for example, 256000k. You would increase the size of the “qca” file system by 133153k, or 133MB.

- 9 Determine the amount of free disk space that can be allocated to file systems as follows:

- a Determine the amount of free disk space on your system by typing

```
# echo ` /opt/nortel/sspfs/fs/meta.pl fs ` 2048
/ 5000 - p | dc
```

and pressing the Enter key.

**Note:** Use the back quote on the same key as the Tilda (~) for `/opt/nortel/sspfs/fs/meta.pl fs`.

The resulting number is the amount of free disk space in megabytes (MB) that can be allocated to existing file systems.

| If the value is    | Do                                     |
|--------------------|----------------------------------------|
| less than zero (0) | contact Nortel Networks for assistance |
| more than zero (0) | step <a href="#">b</a>                 |

- b Use the following table to determine your next step.

| If                                                                                                                                                                                                                            | Do                                     |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------|
| the value you determined in step <a href="#">8</a> (size by which to increase the file system) is greater than the value you obtained in step <a href="#">9a</a> (amount of free disk space you can allocate to file systems) | contact Nortel Networks for assistance |
| the value you determined in step <a href="#">8</a> (size by which to increase the file system) is less than the value you obtained in step <a href="#">9a</a> (amount of free disk space you can allocate to file systems)    | step <a href="#">10</a>                |

## 10

**ATTENTION**

Once you increase the size of a file system, you cannot decrease it. Therefore, it is strongly recommended that you grow a file system in small increments.

Increase the size of the file system by typing

```
# filesystem grow -m <mount_point> -s <size>m
```

Where

**mount\_point**

is the name of the file system you want to increase (noted in step [6](#))

**size**

is the size in megabytes (m) by which you want to increase the file system (determined in step [8](#))

**Example**

```
# filesystem grow -m /data -s 512m
```

**Note:** The example above increases the “/data” file system by 512 megabytes (MB).

You have completed this procedure.

## High-availability configuration (two servers)

### ATTENTION

During this procedure, the cluster will be running without a standby node. The duration is estimated at approximately one hour.

### At your workstation

- 1 For all users except those using Core and Billing Manager (CBM), start a login session using telnet. For CBM, start a login session connecting to the inactive node using ssh.

| If using          | Do                     |
|-------------------|------------------------|
| telnet (unsecure) | step <a href="#">2</a> |
| ssh (secure)      | step <a href="#">6</a> |

- 2 Log in to the Inactive node by typing
 

```
> telnet <server>
```

 and pressing the Enter key.  
 where
 

```
server
```

 is the physical IP address of the Inactive node in the cluster  
**Note:** If you use the cluster IP address, you will log in to the Active node. Therefore, ensure you use the physical IP address of the Inactive node to log in.
- 3 When prompted, enter your user ID and password.
- 4 Change to the root user by typing
 

```
$ su - root
```

 and pressing the Enter key.
- 5 When prompted, enter the root password.  
**Note:** Ensure you are on the Inactive server by typing `ubmstat`. If `ClusterIndicatorACT` is displayed in the response, which indicates you are on the Active server, log out of that server and log in to the other server through telnet using the physical IP address of the other unit. The response must display `ClusterIndicatorSTBY`, which indicates you are on the Inactive server.
- 6 Log in using ssh (secure) as follows:

- a** Log in to the server by typing
- ```
> ssh -l root <server>
```
- and pressing the Enter key.

where

**server**

is the physical IP address of the inactive server

**Note:** If this is the first time you are logging in using ssh, the system will request that you confirm to continue connecting. Enter *yes* at the prompt.

- b** When prompted, enter the root password.

**At the Inactive node**

- 7** Verify the cluster indicator to ensure you are logged in to the Inactive node, by typing

```
# ubmstat
```

and pressing the Enter key.

If the system response is	Do
ClusterIndicatorSTBY	step <a href="#">8</a>
ClusterIndicatorACT	step <a href="#">2</a>

- 8** Verify the status of file systems on this server by typing

```
# udfstat
```

and pressing the Enter key.

If the file systems are	Do
STANDBY normal UP clean	step <a href="#">9</a>
not STANDBY normal UP clean	contact your next level of support

- 9** Determine the amount of disk utilization by the file systems as follows:

- a** Access the command line interface by typing

```
# cli
```

and pressing the Enter key.

*Example response*

Command Line Interface

- 1 - View
- 2 - Configuration
- 3 - Other
  
- X - exit

select -

- b** Enter the number next to the "View" option in the menu.

*Example response*

View

- 1 - sspfs\_soft (Display Software Installation Level Of SSPFS)
- 2 - chk\_sspfs (Check SSPFS Processes)
- 3 - sw\_conf (The software configuration of the znc0s0jx)
- 4 - cpu\_util (Overall CPU utilization)
- 5 - cpu\_util\_proc (CPU utilization by process)
- 6 - port\_util (I/O port utilization)
- 7 - disk\_util (Filesystem utilization)
  
- X - exit

select -

- c** Enter the number next to the "disk\_util" option in the menu.

*Example response*

```

=== Executing "disk_util"
Filesystem      kbytes  used  avail capacity  Mounted on
/dev/md/dsk/d2  4129290 1892027 2195971  47%      /
/proc           0         0         0      0%      /proc
fd              0         0         0      0%      /dev/fd
mnttab          0         0         0      0%      /etc/mnttab
/dev/md/dsk/d8  2053605 155600 1836397  8%      /var
swap            3505488  40 3505448  1%      /var/run
swap            524288  448 523840  1%      /tmp
/dev/md/dsk/d11 5161437 1428691 3681132  28%     /opt
/dev/md/dsk/d23 2031999  34313 1936727  2%      /PROU_data
/dev/md/dsk/d24 2031999 169042 1801998  9%      /audio_files
/dev/md/dsk/d20 3080022 294615 2723807 10%     /data
/dev/md/dsk/d25  949455 440344  452144  50%     /user_audio_files
/dev/md/dsk/d21 3080022 275962 2742460 10%     /opt/nortel
/dev/md/dsk/d22 12386331 10337214 1925254 85%     /data/oradata
/dev/md/dsk/d26  122847  1041  109522  1%      /data/qca

=== "disk_util" completed successfully

```

The *capacity* column indicates the percentage of disk utilization by the file system, which is specified in the *Mounted on* column.

- 10 Note the file system you want to increase, as well as its current size (under column *Kbytes*).
- 11 Exit each menu level of the command line interface to eventually exit the command line interface, by typing

```
select - x
```

and pressing the Enter key.

12

#### ATTENTION

Before you proceed with this procedure, ensure the file system you want to increase is full or nearly full and that its content is valid application data. Remove any unneeded files or files generated in error that are taking up disk space.

Determine the size by which to increase the file system, by subtracting the desired size for the file system based on your specific needs, from its current size (noted in 10).

For example, to determine the size by which to increase the “qca” file system, subtract its current size, 122847k from the desired size, for example, 256000k. You would increase the size of the “qca” file system by 133153k, or 133MB.

- 13 Determine the amount of free disk space that can be allocated to file systems as follows:
  - a Determine the amount of free disk space on your system by typing

```
# echo `/opt/nortel/sspfs/fs/meta.pl fs` 2048  
/ 5000 - p | dc
```

and pressing the Enter key.

**Note:** Use the back quote on the same key as the Tilda (~) for `/opt/nortel/sspfs/fs/meta.pl fs`.

The resulting number is the amount of free disk space in megabytes (MB) that can be allocated to existing file systems.

If the value is	Do
less than zero (0)	contact Nortel Networks for assistance
more than zero (0)	step <a href="#">b</a>

- b** Use the following table to determine your next step.

If	Do
the value you determined in step <a href="#">12</a> (size by which to increase the file system) is greater than the value you obtained in step <a href="#">13a</a> (amount of free disk space you can allocate to file systems)	contact Nortel Networks for assistance
the value you determined in step <a href="#">12</a> (size by which to increase the file system) is less than the value you obtained in step <a href="#">13a</a> (amount of free disk space you can allocate to file systems)	step <a href="#">14</a>

14

#### ATTENTION

Once you increase the size of a file system, you cannot decrease it. Therefore, it is strongly recommended that you grow a file system in small increments.

Increase the size of the desired file system by typing

```
# GrowClusteredFileSystem.ksh <mount_point>
<size>m
```

Where

#### **mount\_point**

is the name of the file system you want to increase (noted in step [10](#))

**size**

is the size in megabytes (m) by which you want to increase the file system (determined in step [12](#))

**Example**

```
# GrowClusteredFileSystem.ksh /data/qca 10m
```

**Note:** The example above increases the “/data/qca” file system by 10 megabytes (MB).

- 15** Reboot the Inactive node by typing

```
# init 6
```

and pressing the Enter key.

- 16** Wait for the Inactive node to reboot, then log in again using its physical IP address.

- 17** Verify the status of file systems on the Inactive node by typing

```
# udstat
```

and pressing the Enter key.

If the file systems are	Do
STANBY normal UP clean	step <a href="#">18</a>
not STANBY normal UP clean	contact your next level of support

- 18** Log in to the Active node by typing

```
> telnet <server>
```

and pressing the Enter key.

where

**server**

is the physical IP address of the active node in the cluster

- 19** When prompted, enter your user ID and password.

- 20** Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

- 21** When prompted, enter the root password.

**Note:** Ensure you are on the Active server by typing `ubmstat`. If `ClusterIndicatorSTBY` is displayed in the response, which indicates you are on the Inactive server, log out of that server and log in to the other server through telnet using the physical IP address of the other unit. The response must display

*ClusterIndicatorACT*, which indicates you are on the Active server.

***At the Active node***

**22** Stop the cluster by typing

# **StopCluster**

and press the Enter key.

This action causes a cluster failover and makes the active node inactive, and the inactive node active.

***At the newly Active node***

**23** Clone the other node using procedure [Cloning the image of one node in a cluster to the other node on page 1](#) if required.

You have completed this procedure.

---

## Performing a backup of file systems on an SSPFS-based server

---

### Application

Use this procedure to perform a backup of the file systems on a Succession Server Platform Foundation Software (SSPFS)-based server (Sun Netra t1400 or Sun Netra 240) running the (I)SN06.2 or greater release of the SSPFS.

The server can be hosting one or more of the following components:

- CS 2000 Management Tools
- Integrated Element Management System (EMS)
- Audio Provisioning Server (APS)
- Media Gateway (MG) 9000 Manager
- CS 2000 SAM21 Manager
- Network Patch Manager
- Core Billing Manager (CBM)

### Prerequisites

This procedure has the following prerequisites:

- you must be running SSPFS (I)SN06.2 or greater
- you must perform a data backup prior to performing this procedure (refer to procedure [Performing a backup of oracle data on an SSPFS-based server on page 207](#), if required)

**Note:** The data backup is not required prior to this procedure for the Core Billing Manager (CBM) product family.

- for a Sun Netra t1400, you need a blank 4mm Digital Data Storage (DDS-3) tape of 125m and 12 GB to store the data
- for Sun Netra 240, you need one or more blank CD-R, CD-RW, DVD-R or DVD-RW to store the data

**Note 1:** The backup utility limits the storage to 2 GB on a DVD-R and DVD-RW.

**Note 2:** If you are using a new CD-RW or DVD-RW, or want to use a used CD-RW or DVD-RW and need to erase the contents, refer to procedure “Preparing a CD-RW or DVD-RW for use” in the ATM/IP Security and Administration document, NN10402-600, if required.

## Action

### ATTENTION

In a two-server configuration, execute this procedure on the Active server.

#### *At the server*

- 1 Insert the blank tape, CD or DVD into the drive. In a two-server configuration, insert the blank CD or DVD into the Active server.

#### *At your workstation*

- 2 Log in to the server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

#### **server**

is the IP address or host name of the SSPFS-based server on which you are performing the backup

Enter the physical IP address of the Active server in a two-server configuration.

- 3 When prompted, enter your user ID and password.

- 4 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

- 5 When prompted, enter the root password.

If you are using	Do
a tape	step <a href="#">6</a>
a CD or DVD	step <a href="#">7</a>

- 6 Rewind the tape by typing

```
# mt -f /dev/rmt/0 rewind
```

and pressing the Enter key.

- 7 Backup the file systems by typing
- ```
# /opt/nortel/sspfs/bks/bkfullsys
```
- and pressing the Enter key.

*Example response:*

```
Backup Completed Successfully
```

**Note:** If you are using CD or DVD, the system will prompt you to insert another blank CD or DVD if more than one is needed.

| If you are using | Do                     |
|------------------|------------------------|
| a tape           | step <a href="#">8</a> |
| a CD or DVD      | step <a href="#">9</a> |

- 8 Verify the backup to tape was successful as follows:
- List the content of the tape by typing

```
# gtar -tvMf /dev/rmt/0
```

and pressing the Enter key.
  - Eject and remove the tape from the drive, label it, write-protect it, and store it in a safe place.  
You have completed this procedure.
- 9 Verify the backup to CD or DVD was successful as follows:
- Reinsert the backup CD or DVD into the drive.
  - List the content of the CD or DVD by typing

```
# gtar -tvMf /cdrom/*bkfullsys*/*.tar
```

and pressing the Enter key.

**Note:** When a DVD backup spans more than one disk, all the DVDs with the exception of the last one produce a file error during the verification process. This error message does not interfere with the backup process but can reappear several times as the backup spans multiple disks.

- 10** Eject the CD from the drive as follows:
  - a** Ensure you are at the root directory level by typing  
# **cd /**  
and pressing the Enter key.
  - b** Eject the CD by typing  
# **eject cdrom**  
and pressing the Enter key.

**Note:** If the DVD drive tray will not open after you have determined that the DVD drive is not busy and is not being read from or written to, enter the following commands:  
# **/etc/init.d/volmgt stop**  
# **/etc/init.d/volmgt start**  
Then, press the eject button located on the front of the DVD drive.
  - c** Remove the CD or DVD from the drive, label it, and store it in a safe place.

You have completed this procedure.

---

## Verifying disk utilization on an SSPFS-based server

---

### Application

Use this procedure to verify disk utilization by the file systems on a Succession Server Platform Foundation Software (SSPFS)-based server.

### Prerequisites

You must have root user privileges.

### Action

Perform the following steps to complete this procedure.

#### *At your workstation*

- 1 Log in to the server by typing  
> **telnet <server>**  
and pressing the Enter key.  
where  
**server**  
is the IP address or host name of the SSPFS-based server
- 2 When prompted, enter your user ID and password.
- 3 Change to the root user by typing  
\$ **su - root**  
and pressing the Enter key.
- 4 When prompted, enter the root password.
- 5 Access the command line interface by typing  
# **cli**  
and pressing the Enter key.

#### *Example response*

```
Command Line Interface
 1 - View
 2 - Configuration
 3 - Other

X - exit

select -
```

- 6 Display the current disk capacity utilization as follows:
- a Enter the number next to the "View" option in the menu.

*Example response*

```
View
 1 - sspfs_soft (Display Software
      Installation Level Of SSPFS)
 2 - chk_sspfs (Check SSPFS Processes)
 3 - sw_conf (The software configuration of
      the znc0s0jx)
 4 - cpu_util (Overall CPU utilization)
 5 - cpu_util_proc (CPU utilization by
      process)
 6 - port_util (I/O port utilization)
 7 - disk_util (Filesystem utilization)

X - exit

select -
```

- b Enter the number next to the "disk\_util" option in the menu.

*Example response*

```
=== Executing "disk_util"
Filesystem      kbytes  used  avail  capacity  Mounted on
/dev/md/dsk/d2  4129290 1892027 2195971    47%      /
/proc           0         0         0         0%      /proc
fd              0         0         0         0%      /dev/fd
mnttab          0         0         0         0%      /etc/mnttab
/dev/md/dsk/d8  2053605 155600 1836397     8%      /var
swap            3505488    40 3505448     1%      /var/run
swap            524288     448 523840     1%      /tmp
/dev/md/dsk/d11 5161437 1428691 3681132    28%     /opt
/dev/md/dsk/d23 2031999   34313 1936727     2%     /PROU_data
/dev/md/dsk/d24 2031999 169042 1801998     9%     /audio_files
/dev/md/dsk/d20 3080022 294615 2723807    10%     /data
/dev/md/dsk/d25  949455 440344  452144    50%     /user_audio_files
/dev/md/dsk/d21 3080022 275962 2742460    10%     /opt/nortel
/dev/md/dsk/d22 12386331 10337214 1925254    85%     /data/oradata
/dev/md/dsk/d26  122847   1041  109522     1%     /data/qca

=== "disk_util" completed successfully
```

You have completed this procedure.

## Replacing a DVD drive on an SSPFS-based server

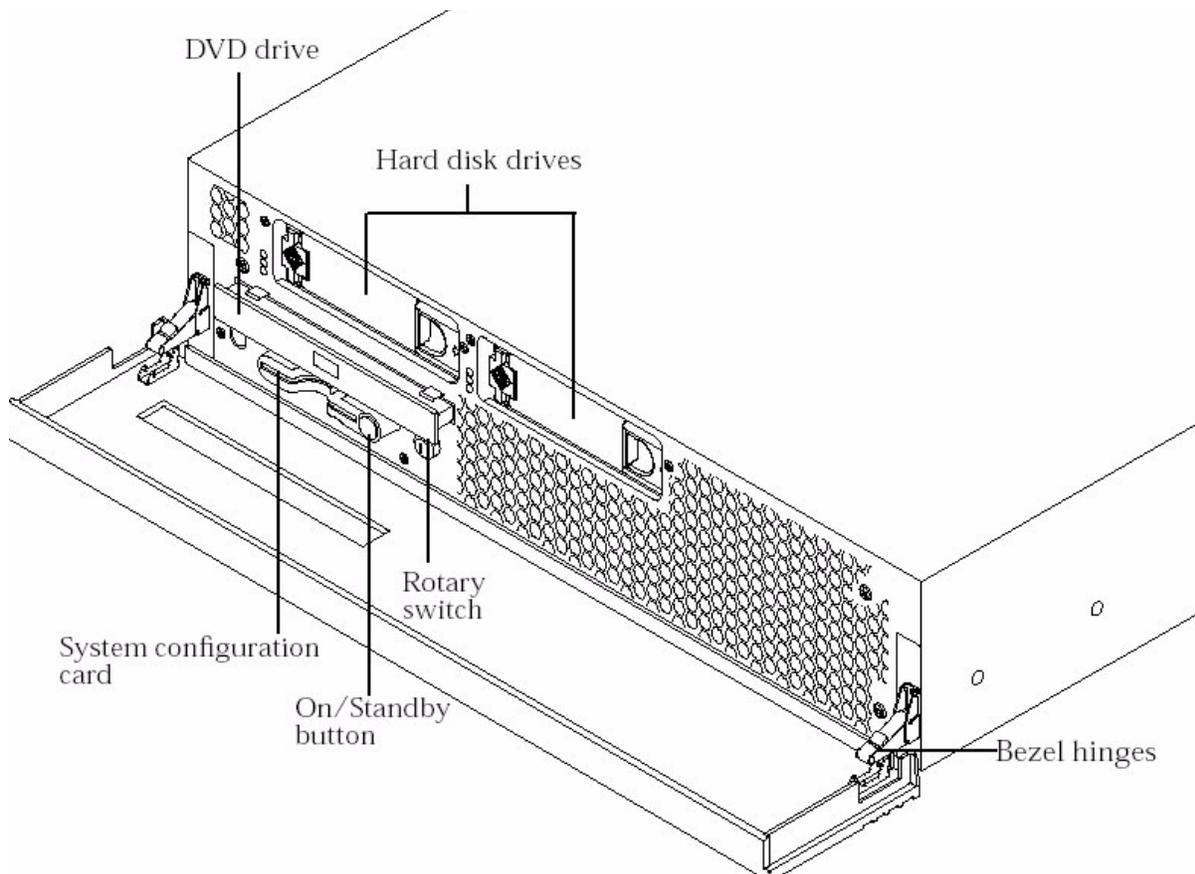
### Application

Use this procedure to replace a DVD drive on a Netra 240 server. This procedure applies to simplex and high-availability (HA) systems. An HA system refers to a Sun Netra 240 server pair.

#### ATTENTION

The DVD drive is not hot-swappable. The server must be powered down. Therefore, ensure the server can be powered down before you proceed with the procedure.

The following figure shows the location of the DVD drive on the Netra 240.



Use one of the methods below according to your office configuration:

- [Simplex configuration \(one server\)](#)
- [High-availability configuration \(two servers\)](#)

## Prerequisites

None.

## Action

### Simplex configuration (one server)

#### *At your workstation*

- 1 Power down the server. Refer to procedure [Shutting down an SSPFS-based server on page 164](#) if required.
- 2 Physically replace the DVD drive using the Sun documentation for the Netra 240.
- 3 Once the new DVD drive is in place, restore power to the server by turning on the power at the circuit breaker panel of the frame. The server recovers on its own once power is restored.
- 4 You have completed this procedure.

### High-availability configuration (two servers)

#### *At your workstation*

- 1 Use the following table to determine your first step.

| <b>If you are replacing the DVD drive on the</b> | <b>Do</b>              |
|--------------------------------------------------|------------------------|
| active server                                    | step <a href="#">2</a> |
| inactive server                                  | step <a href="#">3</a> |

- 2 Initiate a manual failover. Refer to procedure [Initiating a manual failover on a Sun Netra 240 server pair on page 117](#) if required.
- 3 Once the active server acquires the status of standby (inactive), power down the server. Refer to procedure [Shutting down an SSPFS-based server on page 164](#) if required.
- 4 Physically replace the DVD drive using the Sun documentation for the Netra 240.
- 5 Once the new DVD drive is in place, restore power to the server by turning on the power at the circuit breaker panel of the frame. The server recovers on its own once power is restored.

**6** You have completed this procedure.

---

## Initiating a manual failover on a Sun Netra 240 server pair

---

### Application

Use this procedure to initiate a manual failover on a Sun Netra 240 server pair. Initiating a manual failover can be required in the following situations:

- general maintenance
- software update without a data schema or configuration change

The failover causes the standby (inactive) server to take over and start providing OAM&P services as the new active server.

**ATTENTION**

During an automatic or manual failover, the high-availability (HA) cluster takes approximately 5 minutes to failover and bring up the standby node to Active state.

### Prerequisites

You must perform this procedure on the active node.

### Action

Perform the following steps to complete this procedure.

**ATTENTION**

Perform the steps that follow on the Active server.

#### ***At the active node console***

- 1 Log in to the active node through the console (port A) using the root user ID and password.

**Note:** Ensure you are on the Active server by typing `ubmstat`. If `ClusterIndicatorSTBY` is displayed in the response, which indicates you are on the Inactive server, log out of that server and log in to the other server in the pair. The response must display `ClusterIndicatorACT`, which indicates you are on the Active server.

- 2 Initiate the manual failover by typing

# **swact**

and pressing the Enter key.

*Example response*

```
Are you sure you want to initiate a cluster  
failover? [Y/N]
```

- 3 If it is acceptable to initiate a manual failover, indicate you want the failover to occur by typing

**y**

and pressing the Enter key.

You have completed this procedure.

---

## Viewing customer logs on an SSPFS-based server

---

### Application

Use this procedure to view customer logs for the following components:

- Succession Element and Sub-element Manager (SESM)
- Gateway Controller (GWC)
- Media Gateway 9000 (MG 9000)
- Succession Server Platform Foundation Software (SSPFS)

Customer logs reside in directory `/var/log` on the server. For details on customer logs, refer to the Succession Fault Management Log Reference document, NN10275-909.

### Prerequisites

None

### Action

Perform the following steps to complete this procedure.

#### *At your workstation*

- 1 Telnet to the server by typing  

```
> telnet <IP address>
```

and pressing the Enter key.  
where  
**IP address**  
is the IP address of the SSPFS-based server
- 2 When prompted, enter your user ID and password.
- 3 Access the directory where the customer log files reside by typing  

```
$ cd /var/log
```

and pressing the Enter key.
- 4 List the directory content by typing  

```
$ ls
```

and pressing the Enter key.

The customer log files are appended with numbers, for example "customerlog.0". The files with the lower numbers are the newer files.

- 5 Use the following table to determine your next step.

| If you want to                        | Do                             |
|---------------------------------------|--------------------------------|
| view the entire content of a log file | substep <a href="#">a</a> only |
| view specific content of a log file   | substep <a href="#">b</a> only |

- a View the entire content of a log file by typing

```
$ cat <log_filename> |more
```

and pressing the Enter key.

*where*

**log\_filename**

is the name of the customer log file you want to view.

**Example**

```
$ cat customerlog.0 |more
```

- b View specific content of the log file by typing

```
# cat <log_filename> |grep <search_string>
```

and pressing the Enter key.

*where*

**search\_string**

is the text you want to search for.

**Example**

```
$ cat customerlog.0 |grep SPFS350
```

- 6 To print the contents of this file, contact your site system administrator for assistance with using UNIX print commands and with locating a printer connected to your network.
- 7 You have completed this procedure.