



Core and Billing Manager 800 Fault Management

What's new in Core and Billing Manager 800 Fault Management in SN09

Features changes

There are no feature changes in this release.

Other changes

The following changes have been made in the documentation:

- Removed log SDMB330.
- Modified log SDM316.
- Modified procedure Clearing an RTBCD alarm.
- Removed log SDM333.

Fault Management Strategy

The Core and Billing Manager 800 (CBM 800) 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 800 applications have failed
- the CBM 800 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 800 and its connections.

Fault conditions on the CBM 800 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 800 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 800, 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 800. 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 800, collects the logs generated by the CBM 800 and by the core in order to provide a single fault feed to the operational support systems (OSS).

A list of the CBM 800 logs can be found in [CBM 800 logs on page 10](#).

Fault clearing procedures

The basic strategy for clearing CBM 800 faults is outlined in [Strategy for clearing a CBM 800 fault condition on page 25](#).

Tools and utilities

It is important to note that CBM 800 application maintenance is separated from the maintenance of the platform on which the CBM 800 resides. Thus, CBM 800 application maintenance function is performed through the CBM maintenance interface (CBMMTC) and through the command line. Maintenance for the Carrier VoIP SPFS platform and for the Sun Netra240 hardware platform is performed through a suite of SPFS 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   CLI: RTP2
  ISTb  -     -     -     ISTb  -   Host: wcary2qx
  M                                           Active

CBMMtc
0 Quit
2 Mtc
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 - cluster-related status, not applicable to the CBM 800
- 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

Alarm Indicator	Description
C	critical
?	indeterminate

SPFS / Sun Netra240 services

The SPFS common OAM platform provides the system monitoring and maintenance procedures for the platform on which the CBM 800 runs. The platform provides the basic resources necessary for the CBM 800 and its applications. The SPFS platform is maintained using SPFS-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 SPFS 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 800 maintenance procedures

This document contains the procedures used for maintaining the CBM 800 and for responding to fault conditions that arise on the CBM 800. 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 800 application", "SuperNode Billing Application (SBA)", and "SPFS / Sun Netra 240 services".

CBM 800 application fault clearing procedures

The following table contains the fault clearing procedures for CBM 800 applications.

CBM 800 application
Strategy for clearing a CBM 800 fault condition
Clearing a CBM application alarm
Clearing a GDD logical volume size threshold violation
Collecting DEBUG information using the CBMGATHER command
Displaying or storing log records using logreceiver
Retrieving and viewing log records
Troubleshooting Log Delivery problems on a CBM
Verifying the file transfer protocol
Verifying the FTP Schedule

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 64](#).

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

SuperNode Billing Application (SBA)

[Clearing a NOREC alarm](#)

[Clearing an NOSC alarm](#)

[Clearing a NOSTOR alarm](#)

[Clearing a NOVOL alarm](#)

[Clearing an RTBCD 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](#)

SPFS / Sun Netra 240 services fault clearing procedures

The following table shows selected SPFS 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.

SPFS / Sun Netra 240 services

[Replacing a failed power supply](#)

[Replacing failed Ethernet interfaces](#)

[Replacing a failed CBM 800 unit](#)

[Accessing TCP and TCP-IN log devices from a remote location](#)

[Replacing one or more failed disk drives on an SPFS-based server](#)

[Replacing a failed SPFS-based server](#)

[Shutting down an SPFS-based server](#)

[Preparing a DVD-RW for use](#)

[Increasing the size of a file system on an SPFS-based server](#)

[Performing a backup of file systems on an SPFS-based server](#)

[Performing a full system restore on an SPFS-based server](#)

[Verifying disk utilization on an SPFS-based server](#)

[Replacing a DVD drive on an SPFS-based server](#)

CBM 800 logs

The following is a list of the CBM 800 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
SDM300	The connection from the core manager to the Core or the operating company LAN server(s) is down.	Contact your system administrator or Nortel for assistance.
SDM301	A logical volume is not mirrored.	Check hardware faults as mirroring may be lost due to a hard disk failure on the core manager. Note: If a disk has just been replaced and brought back in-service, the system can take more than 15 minutes to restore mirroring.
SDM302	The use of a system resource has exceeded its threshold.	Isolate and clear the problem.
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.

Log	Trigger	Action
SDM304	The Log Delivery application cannot deliver logs to the specified UNIX file.	<p>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:</p> <ul style="list-style-type: none">• “Configuring a core manager for log delivery” in the Configuration Management document• “Deleting a device using logroute” in the Configuration Management document <p>If required, contact your next level of support for assistance.</p>
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.	<p>Upgrade the CM software to a version that is compatible with the SDM software.</p> <p>Note: The software on the core manager must not be at a lower release level than the software on the Core.</p>
SDM308	System image backup (S-tape) is required or has failed.	<p>If a manual system image backup (S-tape) is required, refer to procedure “Creating system image backup tapes (S-tapes) manually” in the Security and Administration document. Ensure the backup tape is inserted. If required, contact your system administrator or Nortel for assistance.</p>

Log	Trigger	Action
SDM309	A hardware device is faulty or has been manually taken out of service.	Use the “querysdm” command from the MAP display. If required, replace the faulty module using the corresponding procedure in this document. Check the cabling to the module. If you cannot determine the reason for the fault, contact your next level of support.
SDM314	A message associated with a specific link is received on a different link. This indicates that the links are not properly connected.	Check for wrongly connected links and correct.
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.
SDM317	The system has detected a Distributed Computing Environment (DCE) problem.	Contact your next level of support to help determine the cause of the failure.
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.
SDM332	Indicates that the system audit completed with failures.	Execute the ‘sysaudit-report’ command to display the results of the system audit.
SDM334	OC3 Card receive/transmit fault	Use the logs command from the hw level of the cbmmtc display to check for an OC3 card fault on the CBM. Check the cabling to the OC3 port listed in the log.

Log	Trigger	Action
SDM335	Bad incoming CRCs on link	Use the logs command from the hw level of the cbmmtc display to check for an OC3 link fault on the CBM. Use the "trns1" command from the MAP display to check the link status. Perform link tests from the MS card level.
SDM336	No heartbeat response received	Use the logs command from the hw level of the cbmmtc display to check for OC3 link faults on the CBM. Check the cabling to the OC3 port listed in all logs. Use the "trns1" command from the MAP display to check the link status. Perform link tests from the MS card level.
SDM338	Audit finds that omdata file system usage exceeds 60% or 80%.	No action required
SDM500	Indicates the initial startup of the core manager. This log is included in the SDM Log Delivery log stream, but does not appear on the RMI.	No action required
SDM501	Indicates a core manager state change to in service (InSv). This log is included in the SDM Log Delivery log stream, but does not appear on the RMI.	No action required
SDM502	Indicates a core manager state change to manual busy (ManB). This log is included in the SDM Log Delivery log stream, but does not appear on the RMI.	No action required
SDM503	Indicates a core manager state change to system busy (SysB). This log is included in the SDM Log Delivery log stream, but does not appear on the RMI.	Refer to the procedure "Clearing a critical APPL alarm" in NN10082-911, <i>CS 2000 Core Manager Fault Management</i> .

Log	Trigger	Action
SDM504	Indicates a core manager state change to in-service trouble (ISTb). This log is included in the SDM Log Delivery log stream, but does not appear on the RMI.	Refer to the procedure "Clearing a minor or major APPL SDM alarm" in NN10082-911, <i>CS 2000 Core Manager Fault Management</i> .
SDM505	Indicates a core manager state change to offline (OffL) state. This log is included in the SDM Log Delivery log stream, but does not appear on the RMI.	No action required
SDM550	Indicates a core manager node status change. One or more of the following can cause the status change: <ul style="list-style-type: none"> • core manager node state • hardware device • software component • application 	Refer to the corresponding procedure in this document if required. Note: Log SDM550 is generated on the CM.
SDM600	The connection from the core manager to the Core or the operating company LAN server(s) has been reestablished. This log is generated only after a connectivity failure has been corrected, and not at system startup.	No action required
SDM601	Mirroring has been reestablished after a logical volume mirroring failure.	No action required
SDM602	A system software resource has returned below its alarm threshold.	No action required
SDM603	A fault on a core manager application or process has cleared.	No action required.

Log	Trigger	Action
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.	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.) 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.
SDM605	Indicates that logs for a specific application have been lost.	No action required.
SDM608	A system image backup (S-tape) has been completed.	No action required.
SDM609	A hardware device has been returned to the in-service state.	No action required.
SDM614	A crossed link alarm has been cleared.	No action required.
SDM615	The SDM Exception Reporting Application generates a warning report at 8:00 a.m. local time when the system generates thresholded logs within the preceding 24 h.	Use LOGUTIL to disable thresholding for logs indicated in the report.
SDM616	A log delivery connection attempt was rejected.	No action required.
SDM617	A Distributed Computing Environment (DCE) problem is cleared.	No action required.
SDM618	The system generates this log report when the /var logical volume reaches 95% full on the disk.	No action required.

Log	Trigger	Action
SDM619	The OM Access Server has detected a corrupt OM Group during an OM Schema download.	No action required.
SDM620	Reports SDM system performance data such as CPU usage, number of processes, swap space occupancy, and logical volume capacities.	No action required.
SDM621	A split mode upgrade has finished.	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.
SDM630	Indicates the start time and completion time of the REX test.	No action required.
SDM632	Indicates that the system audit failure reported through log SDM332 has been cleared.	No action required.
SDM633	Indicates an OC3 link condition change.	No action required.
SDM634	Indicates that a OC3 Card fault has cleared	No action required.
SDM635	Indicates that a bad incoming CRCs problem has cleared	No action required.
SDM636	Indicates that a heartbeat alarm has cleared	No action required.
SDM650	SDM link maintenance requests the logging of a failed link maintenance action. An example of a link maintenance action is the system testing of a link.	No action required Note: Log SDM650 is generated on the CM.

Log	Trigger	Action
SDM700	Log report SDM700 reports a Warm, Cold, or Reload restart or a norestartswact on the core	No action required.
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.

SDM Billing Application (SBA) logs

Log	Trigger	Action
SDMB321	A billing backup-related problem occurred, which affects one file.	Ensure that the backup volume is not busy or full.
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

Log	Trigger	Action
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"> • Records cannot be written to file (by stream). When this occurs, alarm DSKWR is raised. • The Record Client/File Manager is unable to write to the disk. • The disk use is above the critical threshold specified in the MIB in parameter. When this occurs, alarm LODSK is raised. • The disk use is above the major threshold specified in the MIB in parameter. When this occurs, alarm LODSK is raised. • The disk use is above the minor threshold specified in the MIB in parameter. When this occurs, alarm LODSK is raised. • Reached limit for disk space or for the number of files that can reside on the system for a particular stream. • The SBA cannot close or open a file. • Flush file failed 	<ul style="list-style-type: none"> • Check the disk space on the core manager. You may need to FTP files or may need to clean up the disk. • Check the disk space on the core manager. You may need to FTP files or may need to clean up the disk. • Check to see if files are being sent FTP. If not, set the system up to FTP files or back up files. • Check to see if files are being sent FTP. If not, set the system up to FTP files or back up files. • Check to see if files are being sent FTP. If not, set the system up to FTP files or back up files. • Check to see if files are being sent FTP. If not, set the system up to FTP files or back up files. • 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. • Contact your next level of support.
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

Log	Trigger	Action
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>Note: 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"> • insufficient storage space in system • exceeded storage allocation on downstream DPMS • unable to fork child process • unable to open pseudo terminal master • unable to setsid in child process • unable to open pseudo terminal slave in child process • unable to set stdout of child process to pseudo terminal slave • unable to set stderr of child process to pseudo terminal slave • unable to set stdin of child process to pseudo terminal slave • local error in processing • DPMS FTP service not available • DPMS FTP connection closed • requested file action not taken: <command>. File unavailable <p>Verify FTP if the log indicates any one of the following errors:</p> <ul style="list-style-type: none"> • not logged in while executing command: <command> • unable to exec FTP process
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

Log	Trigger	Action
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

Log	Trigger	Action
SDMB655	<ul style="list-style-type: none"> • The state of a billing file has changed. • Disk utilization for a particular stream has dropped below a threshold. • A billing file could not be moved to closedSent. 	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

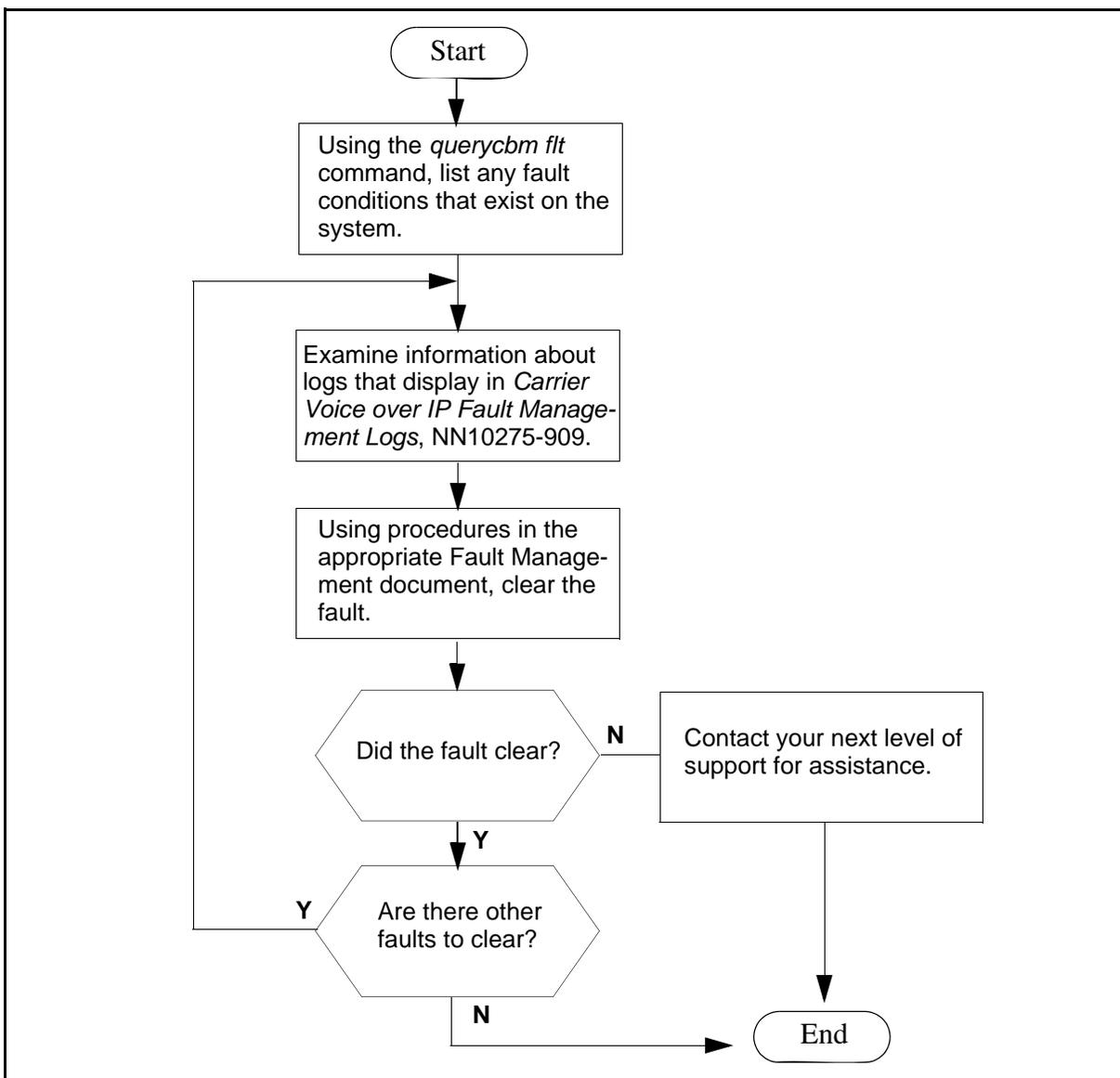
Log	Trigger	Action
SDMB691	Identifies events related to the scheduled transfer of billing files.	For the version of this alarm that displays the message, "Unable to initialize file transfer schedule for stream <stream>", make sure the system is free of faults. When the system is free of faults, the SBA 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 800 fault condition

The following procedure shows the basic steps to be performed to clear a CBM 800 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 800 fault are outlined in the following flowchart.

Basic task flow for clearing faults on the CBM 800



Procedure

Strategy for clearing a CBM 800 fault condition

At your CBM 800

- 1 Log into the CBM 800 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>
Connection to the Core	SDM314	Major Crossed Link: link 0 (domain 0 port 0) crossed to Core with link 1 (domain 0 port 1)
	SDM334	OC3 Card Fault: transmit fault on link 0 (domain 0 port 0)
	SDM335	Minor Link Fault: Bad Incoming CRCs on link 0 (domain 0 port 0)
Network Time Protocol	SDM327	NTP alarm. Synchronization started, can take up to 30 minutes.
Billing related	SDMBxx	Specific to the SBA
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 SPFS / Sun Netra 240 services fault clearing procedures on page 9
Communication problem with the Core (SDM314, SDM 334, SDM335)	Refer to Clearing a major or minor or critical APPL;SDM alarm on page 35
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, contact your next level of support for assistance.
Application problem (SDM 303)	Refer to Clearing a CBM application alarm on page 28
SBA related (SDMBxx)	Refer to SBA alarm troubleshooting on page 64

- 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 6
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 3
no fault conditions exist	step 7

- 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 Clearing a GDD logical volume size threshold violation on page 33
do <i>not</i> receive a GDD threshold alarm	step 4

- 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	step 6
ISTb	step 7
SysB	step 9
Fail	step 10

- 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	step 13

If	Do
the application does not return to service	step 5

- 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	step 13
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	step 13
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 step 13

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

querycbm flt

If	Do
more faults are reported	step 2
all faults are cleared	step 14

- 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 SPFS procedure Increasing the size of a file system on an SPFS-based server on page 203
Decrease the number of days to retain logs	step 2

- 2 Log in to the CBM 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 or minor or critical APPL;SDM alarm

Application

Use this procedure to clear an APPL;SDM minor, major, or critical MAP alarm that has been triggered by the core manager.

Indication

At the MAPCI;MTC level of the MAP display, SDM appears under the APPL header of the alarm banner and indicates a CBM alarm.

Meaning

A CBM alarm indicates

- the core manager is sending an alarm status to the CM because it has at least one alarmed component, or
- the CM has designated the core manager as system busy because it is unable to communicate with the core manager

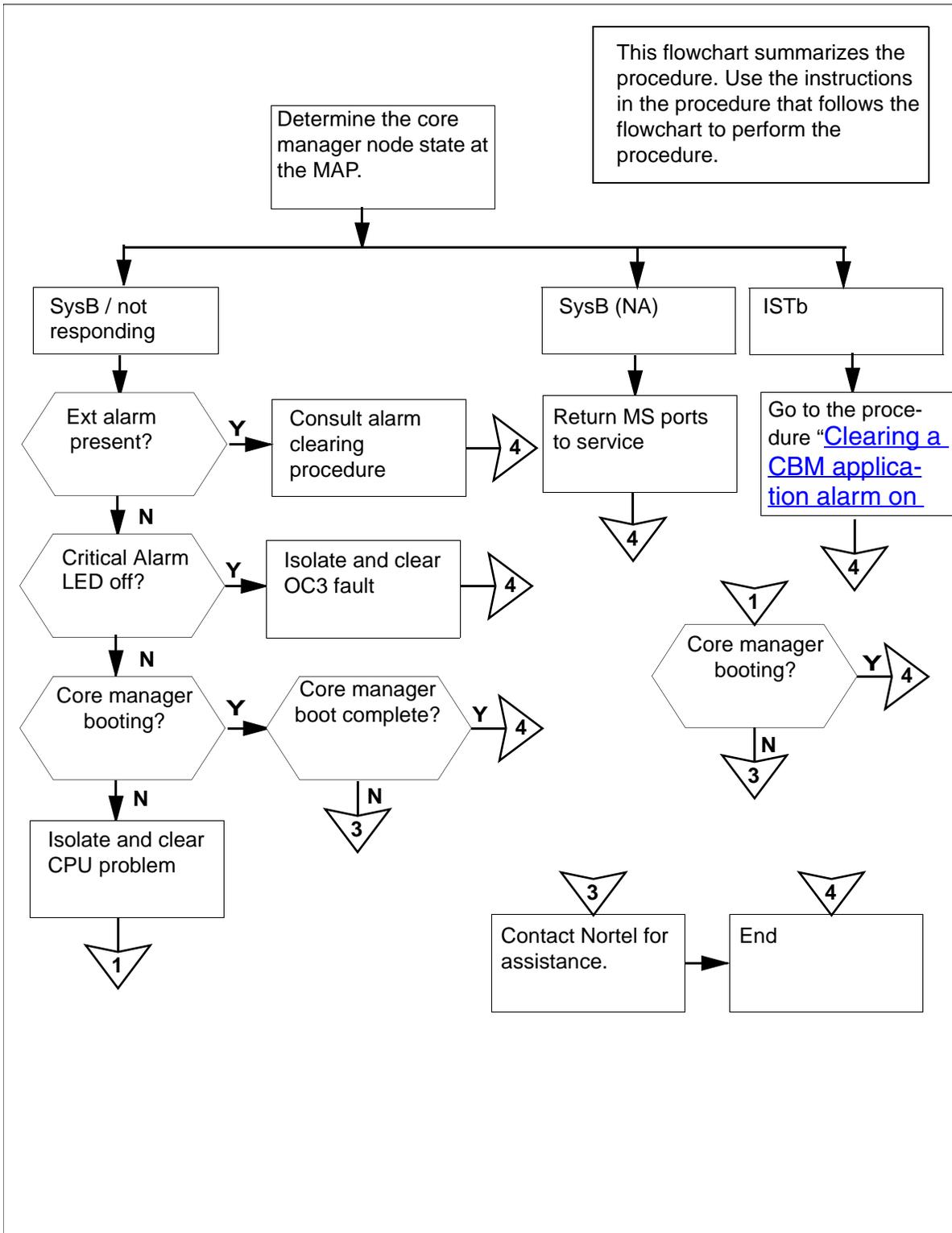
Impact

If the CM is unable to communicate with the core manager, the local state and operating condition of the core manager are unknown to the CM. The core manager maintenance interface must be used to obtain information about the core manager.

Action

The following flowchart is only a summary of the procedure. Use the instructions in the step-action procedure that follows the flowchart to clear the alarm.

Summary of clearing an APPL;SDM alarm



Clearing an APPL;SDM alarm

At the MAP display

- 1 Access the SDM level of the MAP display:

```
> mapci;mtc;appl;sdm
```

Example response:

```
SDM SysB(NA) Links_OOS: 2 of 2
```

- 2 Determine the state of the core manager.

If the state is	Do
SysB/ (NA)	step 6
SysB/ is not responding	step 5
ISTb	the Clearing a CBM application alarm on page 28
ManB	step 3

- 3 If applicable, determine from office records or other personnel why the CBM was set to manual busy state. When permissible, return to CBM to service:

```
> rts
```

Example response:

```
SDM RTS initiated.
```

```
SDM RTS completed.
```

- 4 Determine the CBM state.

If the CBM	Do
remains ManB	contact your next level of support
returns to service	you have completed this procedure
does not return to service	step 2

- 5 Determine from the response if any links are out of service, as indicated by **Links_OOS:** (see example response for step [1](#)).

If all links	Do
not out of service	contact your next level of support

If all links	Do
out of service	step 13

- 6** Determine the MS hardware that provides the OC3 links to the core manager:
- > **trns1**
- Note:** The CM has designated the core manager as system busy (SysB) because all message switch (MS) ports that provide the OC3 links to the core manager are unavailable. The core manager may still be operational, but it is unable to communicate with the computing module (CM).
- Example response*
- ```
SDM 0 PORT 0 (MS 0:15:0) OK ,C MsgCnd:Closed
SDM 0 PORT 1 (MS 1:15:0) ManB MsgCnd:Closed
```
- 7** Record the MS port card number that is associated with the core manager OC3 links.
- Note:** In the example response shown in step [6](#), the port card number is 15.
- 8** Access the MS level of the MAP display:
- > **ms**
- 9** Access the shelf level:
- > **shelf 0**
- 10** Access the MS port card level that is associated with the core manager OC3 links:
- > **card <cardno>**
- where*
- <cardno>**  
is the MS card number noted in step [7](#).
- 11** Note the status of the MS port card and its ports. Use the generic MS alarm clearing procedures provided with your DMS switching system to return the ports to service.
- 12** You have completed this procedure.
- 13** Access the EXT level of the MAP display:
- > **ext**
- 14** List all major EXT alarms:
- > **list maj**

**Note:** If no major alarms are present, the MAP does not display any results on the screen.

- 15 Determine if the core manager has triggered an FSP frame fail alarm for the equipment aisle containing the core manager.

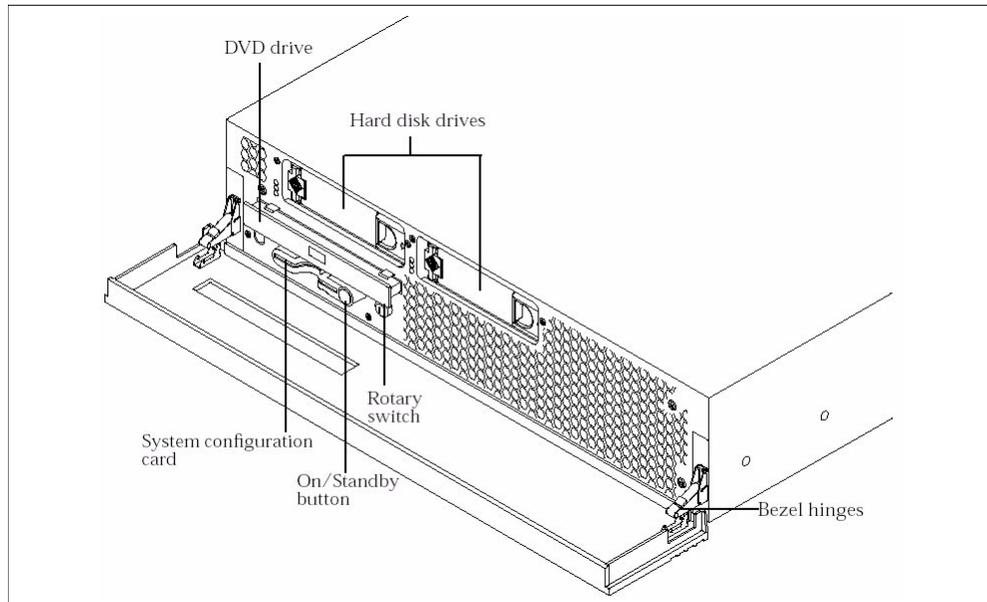
| If FSP alarm is | Do                      |
|-----------------|-------------------------|
| present         | step <a href="#">16</a> |
| not present     | step <a href="#">18</a> |

**Note:** An EXT FSP major alarm triggered by the core manager indicates that one or both -48V dc power inputs to the core manager have failed, or that the core manager has shut down because of thermal failure (overheating).

- 16 Clear the EXT FSP alarm using the procedure Clearing an EXT FSP major alarm in the Fault Management document.
- 17 You have completed this procedure.

**At the front of the core manager**

- 18 At the front of the core manager, determine if an Alarm LED is on.



**Note:** If the System in Service light is off, but power is available to the system and it has not shut down because of

thermal failure (overheating), one or more of the following conditions is present or has occurred:

- system software has crashed
- the system is booting, or the attempt to boot has failed
- the system has been manually shut down

| If the in-service light is | Do                      |
|----------------------------|-------------------------|
| on                         | step <a href="#">31</a> |
| off                        | step <a href="#">19</a> |

- 19** Determine from office records or other personnel if the core manager was manually shut down.

| If the system was      | Do                      |
|------------------------|-------------------------|
| manually shut down     | step <a href="#">22</a> |
| not manually shut down | step <a href="#">20</a> |

- 20** Ensure that the local console is connected to the CBM console port using the designated cable. Ensure that the console is operational and correctly configured for VT100 operation.

***At the local VT100 console***

- 21** Determine if the system is booting.

| If the system is                    | Do                      |
|-------------------------------------|-------------------------|
| booting                             | step <a href="#">23</a> |
| not booting, or the boot has failed | step <a href="#">22</a> |

***At the front of the MSP***

- 22** Cycle power to the core manager by turning the top two modular supervisory panel (MSP) breakers off and on.

The MSP breakers supply power to the core manager.

**At the local VT100 console**

- 23** Monitor the boot process. The boot process takes at least 5 minutes.

| <b>If the boot process</b>                               | <b>Do</b>               |
|----------------------------------------------------------|-------------------------|
| does not start                                           | step <a href="#">24</a> |
| starts, but does not complete (returns to the OK prompt) | step <a href="#">26</a> |
| completes normally, and the login prompt is displayed    | step <a href="#">31</a> |

**At the front of the MSP**

- 24** Cycle power to the core manager by turning the top two modular supervisory panel (MSP) breakers off and on.

The MSP breakers supply power to the core manager.

**At the local VT100 console**

- 25** Monitor the boot process. The boot process takes at least 5 minutes

| <b>If the boot process</b>                               | <b>Do</b>                           |
|----------------------------------------------------------|-------------------------------------|
| does not start                                           | Contact your next level of support. |
| starts, but does not complete (returns to the OK prompt) | step <a href="#">26</a>             |
| completes normally, and the login prompt is displayed    | step <a href="#">31</a>             |

**At the front of the MSP**

- 26** Cycle power to the core manager by turning the top two modular supervisory panel (MSP) breakers off and on.

The MSP breakers supply power to the core manager.

**At the local VT100 console**

- 27** Monitor the boot process at the local VT100 console.

| <b>If the boot process</b> | <b>Do</b>               |
|----------------------------|-------------------------|
| does not start             | step <a href="#">28</a> |

| If the boot process                                   | Do                      |
|-------------------------------------------------------|-------------------------|
| completes normally, and the login prompt is displayed | step <a href="#">31</a> |

- 28 Perform a system software reinstall using the procedure [Performing a full system restore on an SPFS-based server on page 226](#). Ensure that you reboot the system as indicated in that procedure.

- 29 Monitor the boot process.

| If the boot process                                      | Do                                 |
|----------------------------------------------------------|------------------------------------|
| starts, but does not complete (returns to the OK prompt) | contact your next level of support |
| completes normally, and the login prompt is displayed    | step <a href="#">30</a>            |

- 30 Complete the remainder of the procedure [Performing a full system restore on an SPFS-based server on page 226](#).

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

- 31 Log in to the core manager as the root, or a maint class user.

- 32 Access the maintenance interface:

```
cbmmtc
```

- 33 Access the maintenance (Mtc) level:

```
> mtc
```

- 34 Access the core level:

```
> core
```

*Example response:*

```
Communication Path State Core Address CBM
Address
1 VIA OC3 . 10.80.1.2 10.80.1.3
link 0: Open
link 1: Open
```

- 35 Continue according to state of the links.

| If                          | Do                      |
|-----------------------------|-------------------------|
| all links are open          | step <a href="#">44</a> |
| any of the links are closed | step <a href="#">36</a> |

- 36** Note the number of each closed link.

***At the back of the core manager***

- 37** Physically inspect the fiber link connections to the core manager OC3 cards.

| If the fibre links                            | Do                      |
|-----------------------------------------------|-------------------------|
| require reconnecting or replacement           | step <a href="#">38</a> |
| appear undamaged, and are correctly connected | step <a href="#">40</a> |

- 38**



**CAUTION**

**Transmit and receive cables**

Do not mix the transmit and receive cables for each domain. Ensure that you reconnect the cables to the correct slots. Link 0 transmit and link 0 receive connect to MS0. Link 1 transmit and link 1 receive connect to MS1.

Reconnect or replace the fiber cables on the OC3 card.

***At the local VT100 console***

- 39** Monitor the link status at the core level.

| If                          | Do                                |
|-----------------------------|-----------------------------------|
| any of the links are closed | step <a href="#">40</a>           |
| all links are open          | you have completed this procedure |

**Note:** Allow 5 minutes for the core manager link status to update if one or more fibers were reconnected or replaced.

***At the MAP display***

- 40** At the MAP display, determine the MS hardware that provides the OC3 links to the core manager:

**> trns1**

*Example response:*

```
SDM 0 PORT 0 (MS 0:15:0) SysB MsgCnd:Closed
SDM 0 PORT 1 (MS 1:15:0) OK MsgCnd:Open
```

- 41** Record the MS port card number associated with the system-busy links identified in step [39](#).

**Note:** In the example response shown in step [40](#), the port card number is 15.

***At the local VT100 console***

- 42** Access the hardware (Hw) menu level of the CBM maintenance interface:

**>hw**

- 43** Check for Alarm Logs for the OC3 links:

**>logs**

```

CBM MATE NET APPL SYS HW CLLI: CTAT1
ISTb - . . . ISTb Host: TAK0_svr
M M Active
Hw C
0 Quit R
2 O
3 S
4 Logs S
5 _
6 I
7
8
9
10
11
12 The Log Information retrieved for HW are
13 ** SDM314 Major Crossed Link: link 0 (domain
0 port 0) crossed
14 QueryCBM with link 1 (domain 0 port 1)
15 Crossed Link
16
cbm800=TAK0_svr;NODE=TAK0_svr;CLASS=HW;HWTYPE=
CROSS_LINK_0
17 Help Thu Jun 24 09:19:26 2004
18 Refresh
maint

```

- 44** Check that the system displays a dot for the status of the HW.

| If                                    | Do                                 |
|---------------------------------------|------------------------------------|
| HW is in service (indicated by a dot) | you have completed this procedure  |
| HW is in alarm                        | contact your next level of support |

---

## Clearing OC3 link faults

---

### Application

Use this procedure to clear an OC3 Links Fault alarm that has been triggered by the core manager.

### Indication

At the MTC level of the MAP display, SDM \*C\* appears under the APPL header of the alarm banner and indicates a CBM critical alarm.

### Meaning

A CBM critical alarm indicates that the core manager is sending system busy status to the CM because it is out of service, or the CM has designated the core manager as system busy because it is unable to communicate with the core manager.

### Impact

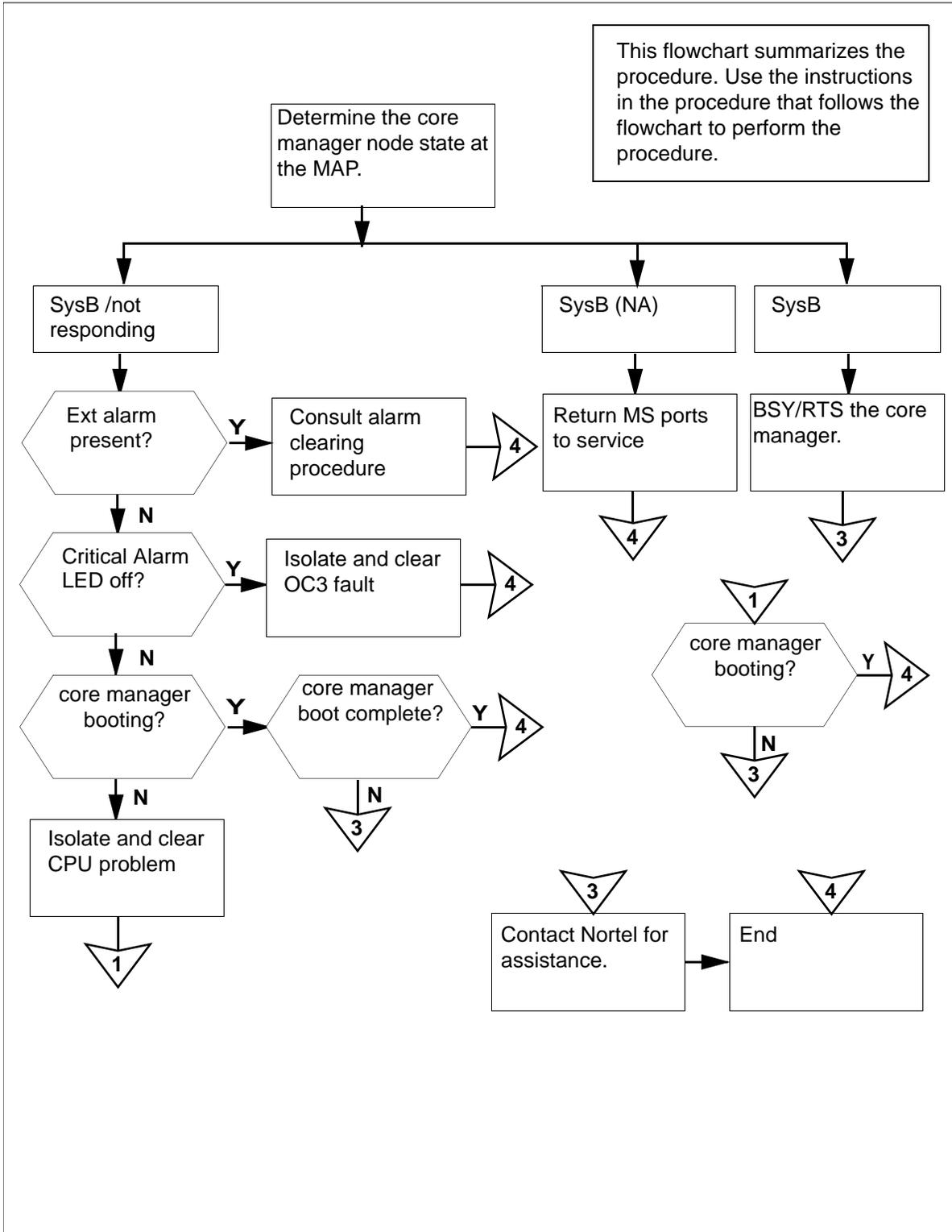
If the CM is unable to communicate with the core manager, the local state and operating condition of the core manager are unknown to the CM. MAP commands requesting state changes to the core manager are not sent to the core manager, and MAP requests for information from the core manager cannot be completed.

The core manager maintenance interface can be used to obtain information about the core manager, when the CM-core manager link is not functioning. When communications are restored, the core manager local state aligns itself to the CM view of its state.

### Action

The following flowchart is only a summary of the procedure. Use the instructions in the step-action procedure that follows the flowchart to clear the alarm.

### Summary of clearing OC3 link faults



## Clearing critical APPL alarm

### *At the local VT100 console*

- 1 Access the hardware (Hw) menu level of the CBM maintenance interface:

```
>hw
```

- 2 Check for Alarm Logs for the OC3 links:

```
>logs
```

```
CBM MATE NET APPL SYS HW CLLI: CTAT1
ISTb - . . . ISTb Host: TAK0_svr
M M Active
Hw C
0 Quit R
2 O
3 S
4 Logs S
5
6 I
7
8
9
10
11
12 The Log Information retrieved for HW are
13 ** SDM314 Major Crossed Link: link 0
 (domain 0 port 0) crossed
14 QueryCBM with link 1 (domain 0 port 1)
15
16
cbm800=TAK0_svr;NODE=TAK0_svr;CLASS=HW;HWTYPE=
CROSS_LINK_0
17 Help Thu Jun 24 09:19:26 2004
18 Refresh
root
```

```
CBM MATE NET APPL SYS HW CLLI: CTAT1
ISTb - . ISTb . . Host: TAK0_svr
 Active
```

Hw

0 Quit

2

3

4 Logs

5

6

7

8

9

10

11

12 The Log Information retrieved for HW are

13 \*\* SDM334 Major OC3 Card Fault: receive  
fault on link 0 (domain 0

14 QueryCBM port 0)

15

16

cbm800=TAK0\_svr;NODE=TAK0\_svr;CLASS=HW;HWTYPE=  
OC3\_FAULT\_0

17 Help Wed Jun 23 11:07:29 2004

18 Refresh

root

```
CBM MATE NET APPL SYS HW CLLI: CTAT1
ISTb - . ISTb . . Host: TAK0_svr
 Active
```

Hw

0 Quit

2

3

4 Logs

5

6

7

```
8
9
10
11
12 The Log Information retrieved for HW are
13 ** SDM334 Major OC3 Card Fault: receive
14 fault on link 0 (domain 0
15 QueryCBM port 0)
16
17 cbm800=TAK0_svr;NODE=TAK0_svr;CLASS=HW;HWTYPE=
18 OC3_FAULT_0
19 Help Wed Jun 23 11:07:29 2004
20 Refresh
21 root
```

- 3** Check that the system displays a dot for the status of the HW alarm.

| If                                          | Do                                 |
|---------------------------------------------|------------------------------------|
| HW alarm is in service (indicated by a dot) | you have completed this procedure  |
| HW is in alarm                              | contact your next level of support |

## 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.

### 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 *Core and Billing Manager 800 Accounting NTP* (NN10357811).
- 2 Access the SDMBIL level:  

```
> mapci;mtc;appl;sdmbil;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;sdmbil;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 *Core and Billing Manager 800 Accounting NTP* (NN10357811).

- 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 SPFS-based server on page 196](#).
- 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;sdmbil;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.

---

## Replacing a failed CBM 800 unit

---

### Purpose

Use the following procedures to replace a failed CBM 800 unit.

### Prerequisites

The following precautions must be observed in order to successfully perform this procedure.



#### **WARNING**

##### **Static electricity damage**

Wear an electrostatic discharge (ESD) grounding wrist strap connected to the COAM or MISC cabinet when handling CBM 800 hardware. This protects the hardware against damage caused by static electricity.

### Procedure

**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.

#### **Replacing failed CBM 800**

##### ***At your workstation***

- 1 Log into the core.

##### ***At the core***

- 2 List the billing streams configured on the core:  

```
table sdbill;lis all
```
- 3 Look at the streams listed while you were performing step 2. Write down all of the names of the billing streams that are not status OFF.
- 4 Perform this step and step 5 for each billing stream that you noted in step 3. These two steps will direct all billing records to the backup volumes on the core; otherwise the core will continually attempt to communicate with the CBM 800. Access the SDBIL level and post the billing stream:

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

where

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

- 5 Busy the billing stream:

**bsy**

| If                                                                              | Do                     |
|---------------------------------------------------------------------------------|------------------------|
| you have busied all of the billing streams listed in step <a href="#">2</a>     | step <a href="#">6</a> |
| you have not busied all of the billing streams listed in step <a href="#">2</a> | step <a href="#">4</a> |

***At the shelf***

- 6 Perform [Replacing a failed SPFS-based server on page 60](#)

***At your workstation***

- 7 Perform [Performing a full system restore on an SPFS-based server on page 226](#)

***At the MAP***

- 8 List the billing streams configured on the core:

```
table sdmbill;lis all
```

- 9 Look at the streams listed while you were performing step [8](#). Write down all of the names of the billing streams that are not status OFF.

- 10 Perform this step and step [11](#) for each billing stream that you noted in step [9](#). These two steps will direct all billing records to the newly-active CBM 800 from the core. Access the SDMBIL level and post the billing stream:

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

where

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

**11** Return the billing stream to service:**rts**

| If                                                                                           | Do                      |
|----------------------------------------------------------------------------------------------|-------------------------|
| you have returned to service all of the billing streams listed in step <a href="#">8</a>     | step <a href="#">12</a> |
| you have not returned to service all of the billing streams listed in step <a href="#">8</a> | step <a href="#">10</a> |

**Note:** Steps [10](#) and [11](#) may take some time to complete due to the SuperNode Billing Application (SBA) going into recovery.

**At the core****12** Verify the status of streams that are not status OFF to determine whether these streams are in service. Access the SDBIL level and post each billing stream that is not status OFF:

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

where

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

| If                                                        | Do                                  |
|-----------------------------------------------------------|-------------------------------------|
| any stream is RBsy/backup (not in recovery or in service) | Contact your next level of support. |
| any stream is InSv or RCVY                                | step <a href="#">13</a>             |

***At your workstation***

- 13** Verify that billing is collecting records:

```
query <stream_name>
```

where

```
<stream_name>
```

is the name of a billing stream that you have returned to service in step [11](#)

Note the number of records, wait approximately 10 seconds, and repeat the query command.

| <b>If the number of records</b>                                                | <b>Do</b>                          |
|--------------------------------------------------------------------------------|------------------------------------|
| increased from the first query command (meaning billing is working)            | step <a href="#">14</a>            |
| did not increase from the first query command (meaning billing is not working) | contact your next level of support |

- 14** You have completed this procedure.

---

## Replacing a failed SPFS-based server

---

### Application

Use the following procedure when an SPFS-based server has failed and you need to replace it. This procedure provides the instructions for a one-server configuration or a two server configuration.

The server can be hosting one or more of the following components:

- CS 2000 Management Tools
- Integrated Element Management System (IEMS)
- Audio Provisioning Server (APS)
- Media Gateway 9000 Manager
- CS 2000 SAM21 Manager
- Network Patch Manager (NPM)
- Core Billing Manager (CBM)

### Prerequisites

You have a replacement server.

|                                                     |
|-----------------------------------------------------|
| <p style="text-align: center;"><b>ATTENTION</b></p> |
|-----------------------------------------------------|

|                                                                                                                      |
|----------------------------------------------------------------------------------------------------------------------|
| <p>Ensure that no provisioning activities are in progress, or are scheduled to take place during this procedure.</p> |
|----------------------------------------------------------------------------------------------------------------------|

### Action

Perform the steps under one of the headings that follow to complete this procedure.

- [Replacing an SPFS-based server \(one-server configuration\) on page 61](#)
- [Replacing one server in an HA configuration on page 61](#)
- [Replacing both servers in an HA configuration on page 61](#)

## Replacing an SPFS-based server (one-server configuration)

### *At the COAM frame*

- 1 Disconnect and remove the failed server.
- 2 Connect and power up the replacement server.
- 3 Restore the file systems and oracle data from backup media. If required, refer to procedure [Performing a full system restore on an SPFS-based server on page 226](#).

**Note:** Restoring the oracle data does not apply to the CBM as it does not use an oracle database.

You have completed this procedure.

## Replacing one server in an HA configuration

### *At the COAM frame*

- 1 Disconnect and remove the failed server.
- 2 Connect and power up the replacement server.
- 3 Clone the image of the active server onto the server you just replaced.

You have completed this procedure.

## Replacing both servers in an HA configuration

### *At the COAM frame*

- 1 Disconnect and remove one failed server.
- 2 Connect and power up the replacement server.
- 3 Restore the file systems and oracle data from backup media on the server you just replaced. If required, refer to procedure [Performing a full system restore on an SPFS-based server on page 226](#).

**Note:** Restoring the oracle data does not apply to the CBM as it does not use an oracle database.

- 4 Disconnect and remove the other failed server.
- 5 Connect and power up the replacement server.
- 6 Clone the image of the active server onto the server you just replaced.

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 62](#).

### 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<br><br><a href="#">Displaying or storing log records using logreceiver on page 82</a> |
| TCP-IN     | Accessing a TCP-IN device from a remote location | “Configuring a core manager for log delivery” in the Configuration Management document<br><br>“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 62](#).
- 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 62](#).
- 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 176](#)
- [Verifying the FTP Schedule on page 183](#)

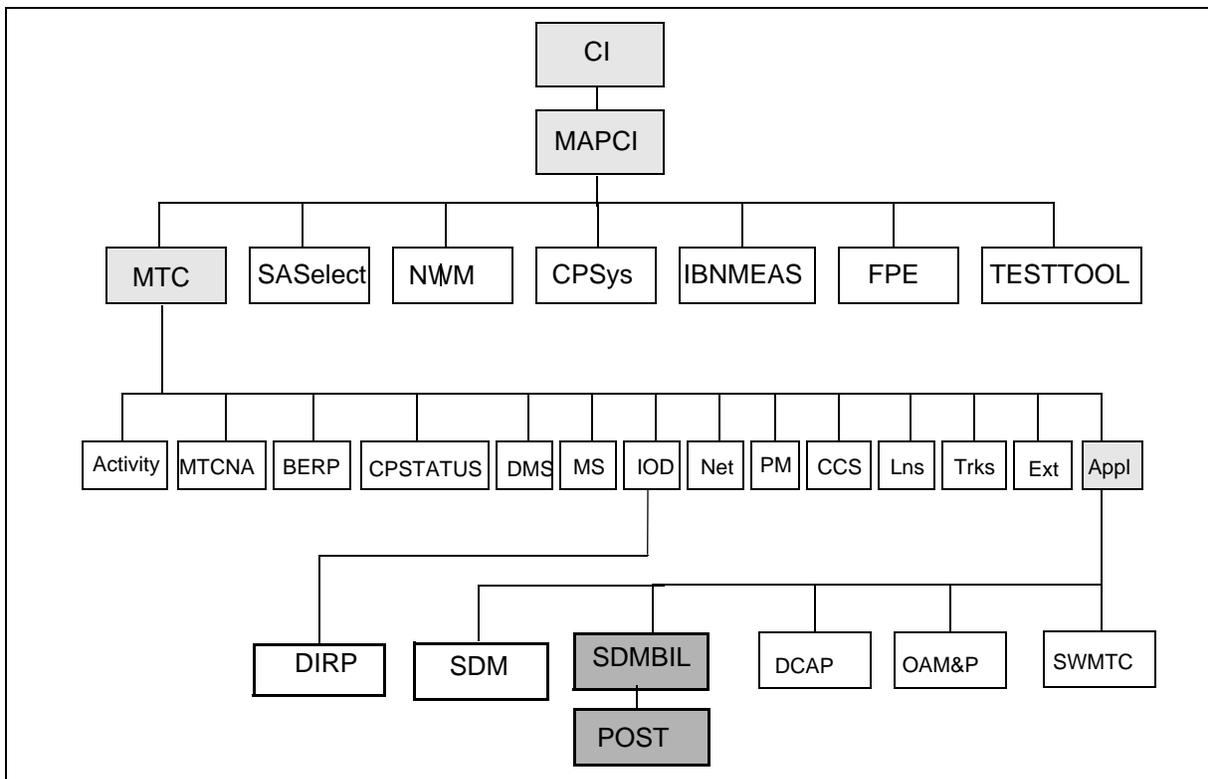
Use the following procedures to clear alarms based on communication problems between the core and the core manager:

- [Clearing a DSKWR alarm on a CBM on page 127](#)
- [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 167](#)
- [Clearing a minor SBACP alarm on page 171](#)

## 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;sdmbil;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 176](#) helps you determine that the FTP process is configured correctly and is able to transfer files
- [Verifying the FTP Schedule on page 183](#) 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 98](#)
- [Clearing a BAK70 alarm on page 102](#)
- [Clearing a BAK90 alarm on page 106](#)
- [Clearing a BAKUP alarm on page 110](#)
- [Clearing a NOBAK alarm on page 139](#)
- [Clearing a NOREC alarm on page 151](#)
- [Clearing a NOSTOR alarm on page 153](#)
- [Clearing a NOVOL alarm on page 157](#)

---

## 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

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

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 Nortel Networks support to discover the root cause of the problem and to prevent similar problems in the future.

### Collecting DEBUG information in split mode

Use the following procedure to collect DEBUG information. Collect the same output/files of the DEBUG information for both the active and inactive domains (domains 0 and 1, respectively) if accessible.

***At the core manager command line (UNIX prompt) of the active domain (domain 0)***

- 1 Run the utility to collect the output:

```
cbmgather
```

| If the <code>cbmgather</code> command | Do                     |
|---------------------------------------|------------------------|
| executes                              | <a href="#">step 3</a> |
| is not available                      | <a href="#">step 2</a> |

- 2 Run the FX utility to collect the output:

```
FXgather
```

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

```
cd /var/adm
```

```
tar cvf varadm_sysold.tar *.day* *.log
```

```
compress varadm_sysold.tar
```

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

**At the core manager command line (UNIX prompt) of the inactive domain (domain 1)**

- 4 Run the utility to collect the output:

```
cbmgather
```

| If the cbmgather command | Do                     |
|--------------------------|------------------------|
| executes                 | <a href="#">step 6</a> |
| not available            | <a href="#">step 5</a> |

- 5 Run the FX utility to collect the output:

```
FXgather
```

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

```
cd /var/adm
```

```
tar cvf varadm_sysnew.tar *.day* *.log
```

```
compress varadm_sysnew.tar
```

*Example response:*

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

| If you used the   | Do                                                      |
|-------------------|---------------------------------------------------------|
| cbmgather command | <a href="#">step 7</a> through <a href="#">step 9</a>   |
| FXgather command  | <a href="#">step 10</a> through <a href="#">step 12</a> |

**From the active domain (domain 0)**

- 7 Move the DEBUG files from the inactive domain (domain 1) to the active domain (domain 0):

```
smft -g <source file> <destination file>
```

where

**<source file>**

is each of the following files:

- /var/adm/cbmgather\_<machine\_name>\_<sys\_old\_or\_new>\_<date\_and\_time>.tar.Z

**Example**

```
/var/adm/cbmgather_wcary2p2_sysnew_20020523223351.tar.Z
```

- /var/adm/varadm\_sysnew.tar.Z

**<destination\_file>**

the name of the moved file archive

*Example command sequence:*

```
smft -g /var/adm/cbmgather_wcary2p2_sysnew
_20020523223351.tar.Z
/var/adm/cbmgather_wcary2p2_sysnew
_20020523223351.tar.Z
```

```
smft -g /var/adm/varadm_sysnew.tar.Z
/var/adm/varadm_sysnew.tar.Z
```

- 8** Move the following output/files of all previous commands out of the system to a secure location using FTP (in BINary mode):

- /var/adm/cbmgather\_<machine\_name>\_sysold  
\_<date\_and\_time>.tar.Z.

**Example**

```
/var/adm/cbmgather_wcary2p2_sysold
_20020523223351.tar.Z
```

- /var/adm/cbmgather\_<machine\_name>\_sysnew  
\_<date\_and\_time>.tar.Z

**Example**

```
/var/adm/cbmgather_wcary2p2_sysnew_200205232233
51.tar.Z
```

- /var/adm/varadm\_sysold.tar.Z
- /var/adm/varadm\_sysnew.tar.Z

- 9** Remove the gathered output/files from the system from the system:

```
rm /var/adm/varadm_sysold.tar.Z
```

```
rm /var/adm/varadm_sysnew.tar.Z
```

**From the active domain (domain 0)**

- 10 Move the DEBUG files from the inactive domain (domain 1) to the active domain (domain 0):

```
smft -g <source file> <destination file>
```

where

**<source file>**

is each of the following files:

- /var/adm/ras/gather.<date\_and\_time>/gather.out

**Example**

```
/var/adm/ras/gather.020528090819/garther.out
```

- /var/adm/ras/gather.<date\_and\_time>/gather.cpio.z

**Example**

```
/var/adm/ras/gather.020528090819/gather.cpio.Z
```

- /var/adm/varadm\_sysnew.tar.Z

**<destination\_file>**

the name of the moved file archive

Example command sequence

```
smft -g
/var/adm/ras/gather.020528090819/gather.out
/var/adm/gather_sysnew.out

smft -g
/var/adm/ras/gather.020528090819/gather.cpio.Z
/var/adm/gather_sysnew.cpio.Z

smft -g /var/adm/varadm_sysnew.tar.Z
/var/adm/varadm_sysnew.tar.Z
```

- 11 Move the following output/files of all previous commands out of the system to a secure location using FTP (in BINary mode):

- /var/adm/ras/gather.<date\_and\_time>/gather.out

**Example**

```
/var/adm/ras/gather.020528090819/garther.out
```

- /var/adm/ras/gather.<date\_and\_time>/gather.cpio.Z

**Example**

```
/var/adm/ras/gather.020528090819/gather.cpio.Z
```

- /var/adm/gather\_sysnew.out
- /var/adm/gather\_sysnew.cpio.Z

- /var/adm/varadm\_sysold.tar.Z
  - /var/adm/varadm\_sysnew.tar.Z
- 12** Remove the following gathered output/files from the system:
- ```
# rm/var/adm/gather_sysnew.out
# rm/var/adm/gather_sysnew.cpio.Z
# rm/var/adm/varadm_sysold.tar.Z
# rm/var/adm/varadm_sysnew.tar.Z
```
- 13** 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	step 3
return the SBA to service	step 5

- 3

	<p>CAUTION</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	step 5
busied successfully but you do not want to return the SBA to service at this time	step 13
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	step 6
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	step 7
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	step 13
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.

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"> an AFT session network connection has been disrupted during file transfer the retry count has been exceeded on a file the message transfer protocol (MTP) timer has expired
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.

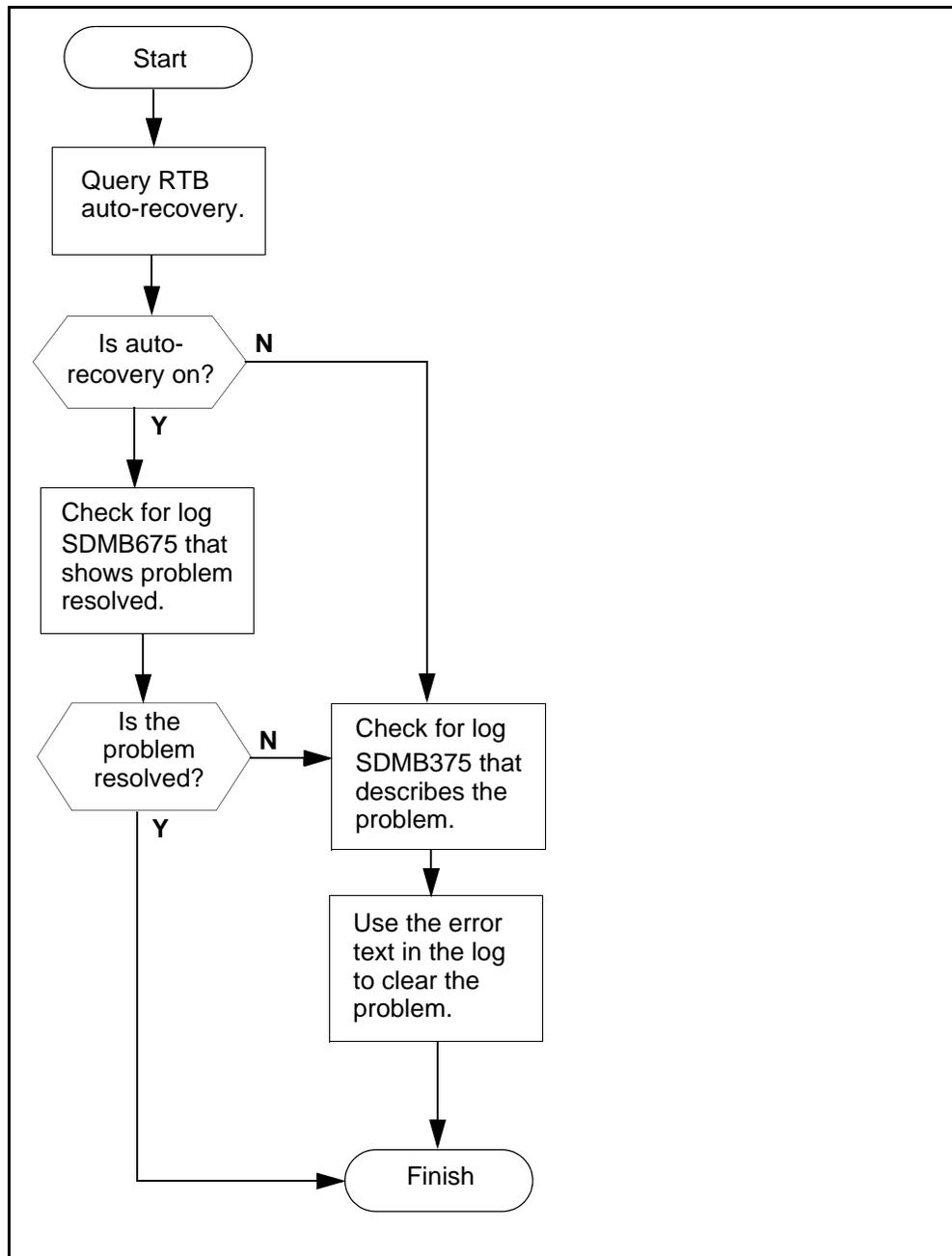
Restarting an AFT session

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.

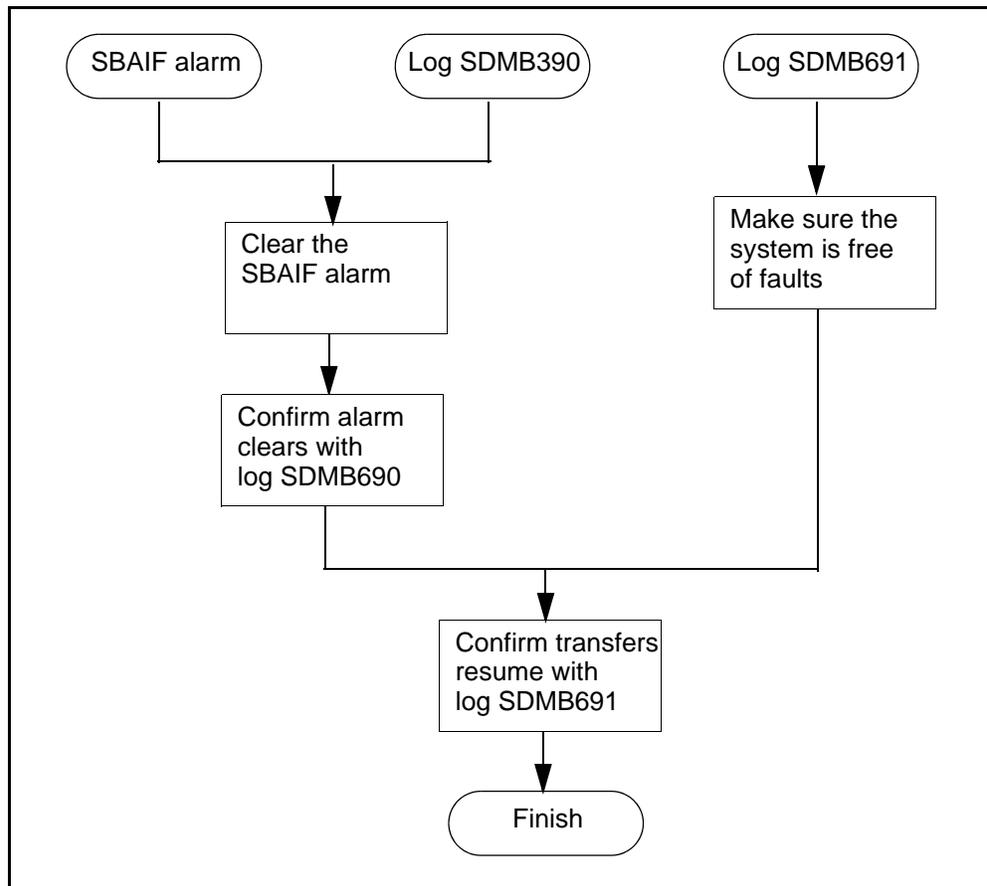
Troubleshooting RTB problems

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

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	step 4
ManB	step 5
InSv	step 6

- 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	step 6
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)”	step 7
a fault report indicates “Core log device is not Configured”	step 20
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	step 11
all files start with LOGS.recorddata	step 17

- 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. to for the ISTb state to change to InSv.

If the Log Delivery application	Do
remains ISTb	step 15
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	step 19

- 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.

```
# fileysys 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

3Mb x 2 x 50 days = 300 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	step 24

- 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.

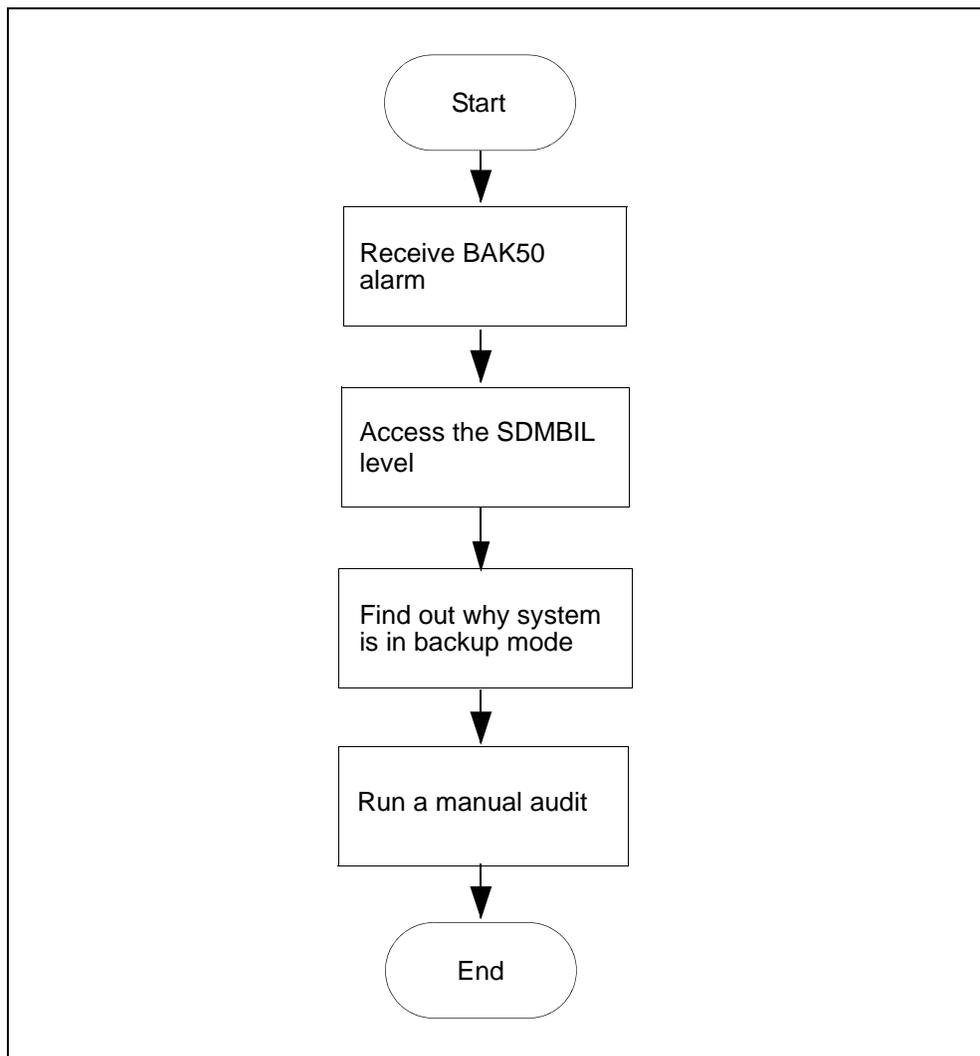
Impact

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



Clearing a BAK50 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 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 5 .
RBsy	refer to Clearing a major SBACP alarm on page 167 , and then return to step 5 .
ManB	Go to step 8
Bkup	Go to step 8

5 Use Audit to clear the alarm.

If the alarm	Do
cleared	step 6
did not clear	step 8

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 12
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 114](#)

9 Use Audit to clear the alarm.

If the alarm	Do
cleared	step 10
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 12

If the billing system	Do
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.

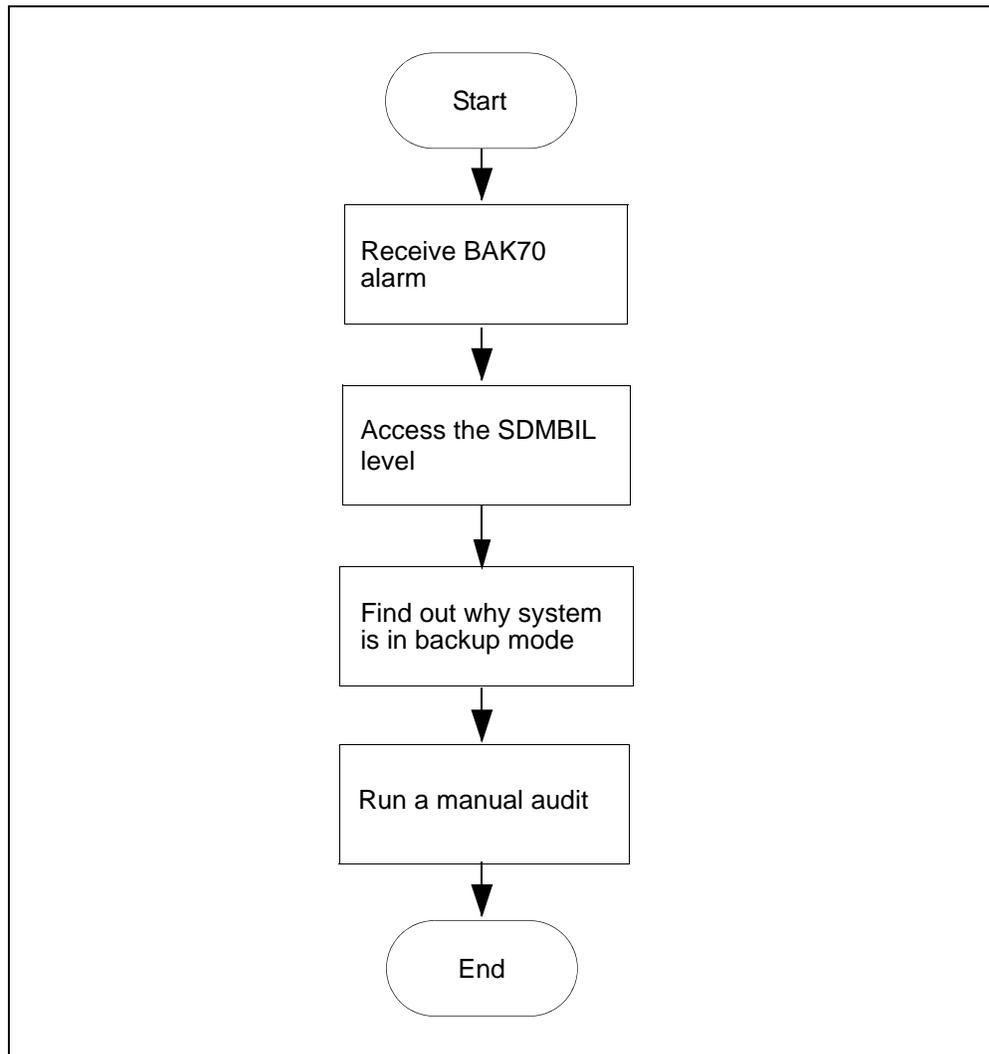
The core manager generates the SDMB820 log report when this alarm is raised.

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**Clearing a BAK70 alarm*****At the MAP***

- 1 Post the billing stream:

```
> mapci;mtc;appl;sdmbil;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 5 .
RBsy	refer to Clearing a major SBACP alarm on page 167 , and then return to step 5 .
ManB	Go to step 8
Bkup	Go to step 8

5 Use Audit to clear the alarm.

If the alarm	Do
cleared	step 6
did not clear	step 8

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 12
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 114](#)

9 Use Audit to clear the alarm.

If the alarm	Do
cleared	step 10
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 12

If the billing system	Do
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.

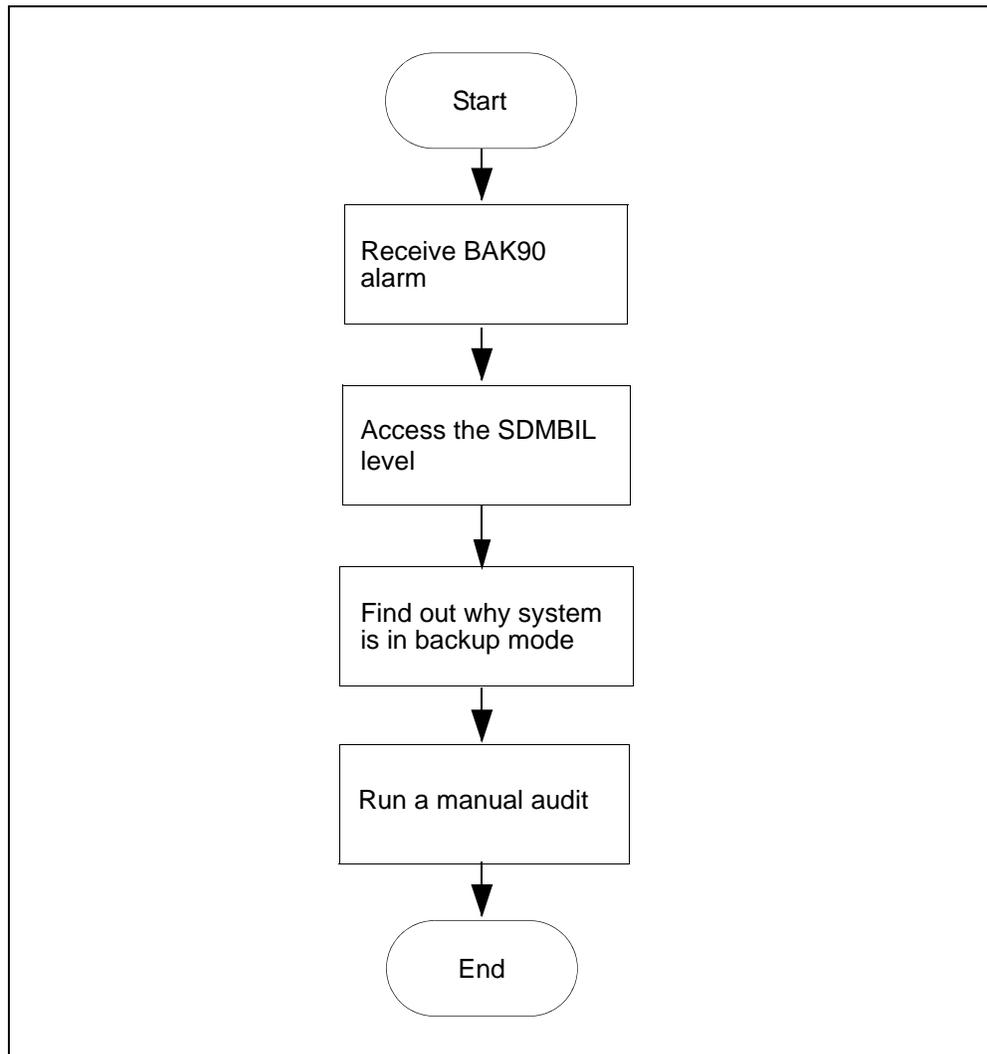
The core manager generates the SDMB820 log report when this alarm is raised.

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**Clearing a BAK90 alarm*****At the MAP***

- 1 Post the billing stream:

```
> mapci;mtc;appl;sdmbil;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 5 .
RBsy	refer to Clearing a major SBACP alarm on page 167 , and then return to step 5 .
ManB	Go to step 8
Bkup	Go to step 8

5 Use Audit to clear the alarm.

If the alarm	Do
cleared	step 6
did not clear	step 8

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 12
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 114](#)

9 Use Audit to clear the alarm.

If the alarm	Do
cleared	step 10
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 12

If the billing system	Do
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.

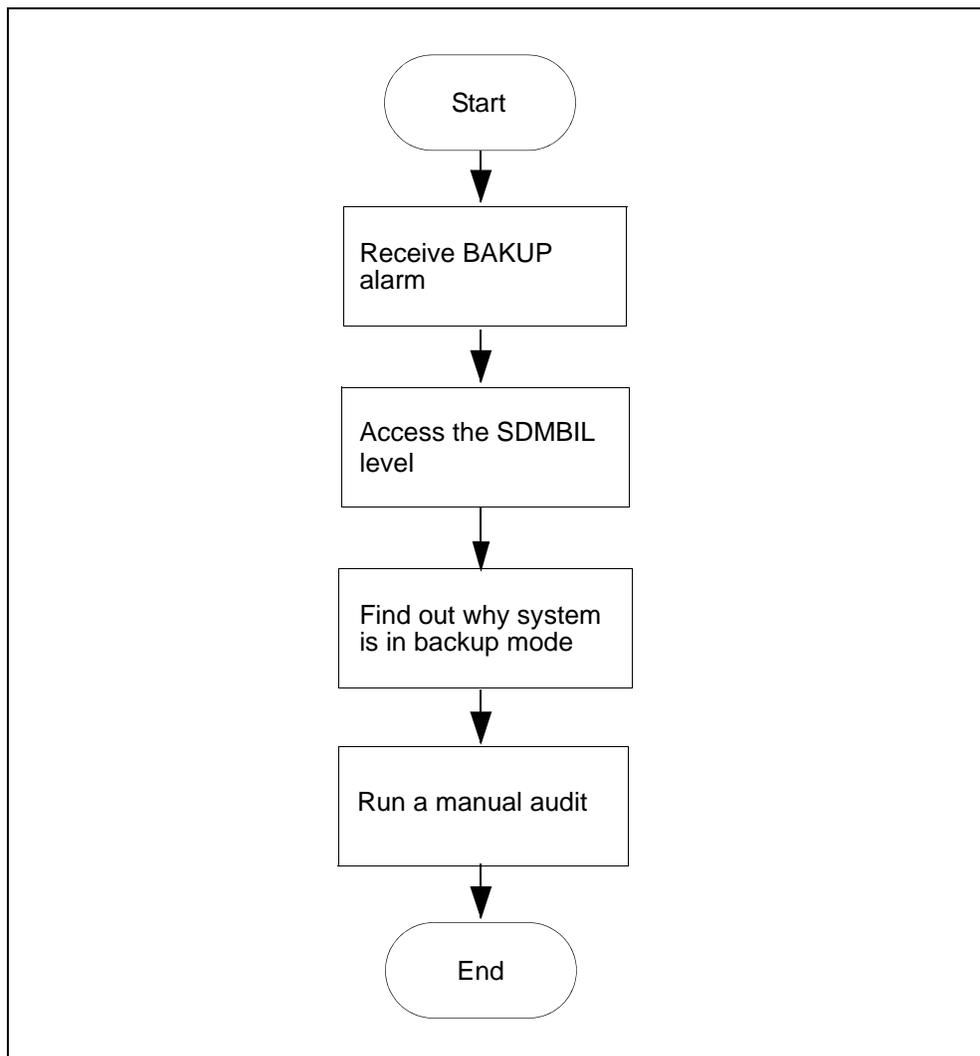
The core manager generates the SDMB820 log report when this alarm is raised.

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_{xx} alarms provide storage notification (_{xx} 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**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 5 .
RBsy	refer to Clearing a major SBACP alarm on page 167 , and then return to step 5 .
ManB	Go to step 8
Bkup	Go to step 8

5 Use Audit to clear the alarm.

If the alarm	Do
cleared	step 6
did not clear	step 8

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 12
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 114](#)

9 Use Audit to clear the alarm.

If the alarm	Do
cleared	step 10
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 12

If the billing system	Do
is not in recovery	contact your next level of support

12 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 3
IOP disks	step 5
SLM disks	step 5
3PC disks	step 5

- 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 7
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 an EXT FSP major alarm

Purpose

Use this procedure to clear an EXT FSP major MAP alarm that has been triggered by the CBM.

Application

The EXT FSP alarm is used to report fault conditions on frame supervisory panels (FSPs) and modular supervisory panels (MSPs) in various types of cabinets or frames in a DMS switching environment.

This procedure assumes that you have isolated the CBM as the cause of the EXT FSP alarm. To clear an FSP alarm generated by equipment other than the CBM, use the EXT FSP alarm clearing procedure in the generic alarm clearing documentation for your DMS switch.

Indication

At the MTC level of the MAP display, FSP appears under the Ext header of the alarm banner and indicates an external FSP major alarm.

Meaning

ATTENTION

If all three LEDs are red, the alarm card or the fuse can be faulty. Contact Nortel Networks for assistance in determining the cause. Do not attempt to replace the alarm card (NTRX41AA), or the 3/4 amp fuse.

An EXT FSP alarm triggered by the CBM means that one of the following faults has occurred:

- Input power (-48 dc) to the CBM has failed.
- The CBM has reached its maximum allowable operating temperature threshold.
- The CBM power supply has failed.

Input power failure

The status of the input power is shown by the Input Power LED on the NTRX41AA alarm card in the modular supervisory panel (MSP) at the top of the CBM cabinet. See the figure [MSP LEDs at the top of the CBM cabinet on page 118](#).

This LED is normally on (green), but if it is off, there is no input power to the CBM.

Maximum temperature threshold reached

The status of the operating temperature is shown by the Thermal Fail LED on the NTRX41AA alarm card in the modular supervisory panel (MSP) at the top of the CBM cabinet. See the figure [MSP LEDs at the top of the CBM cabinet on page 118](#).

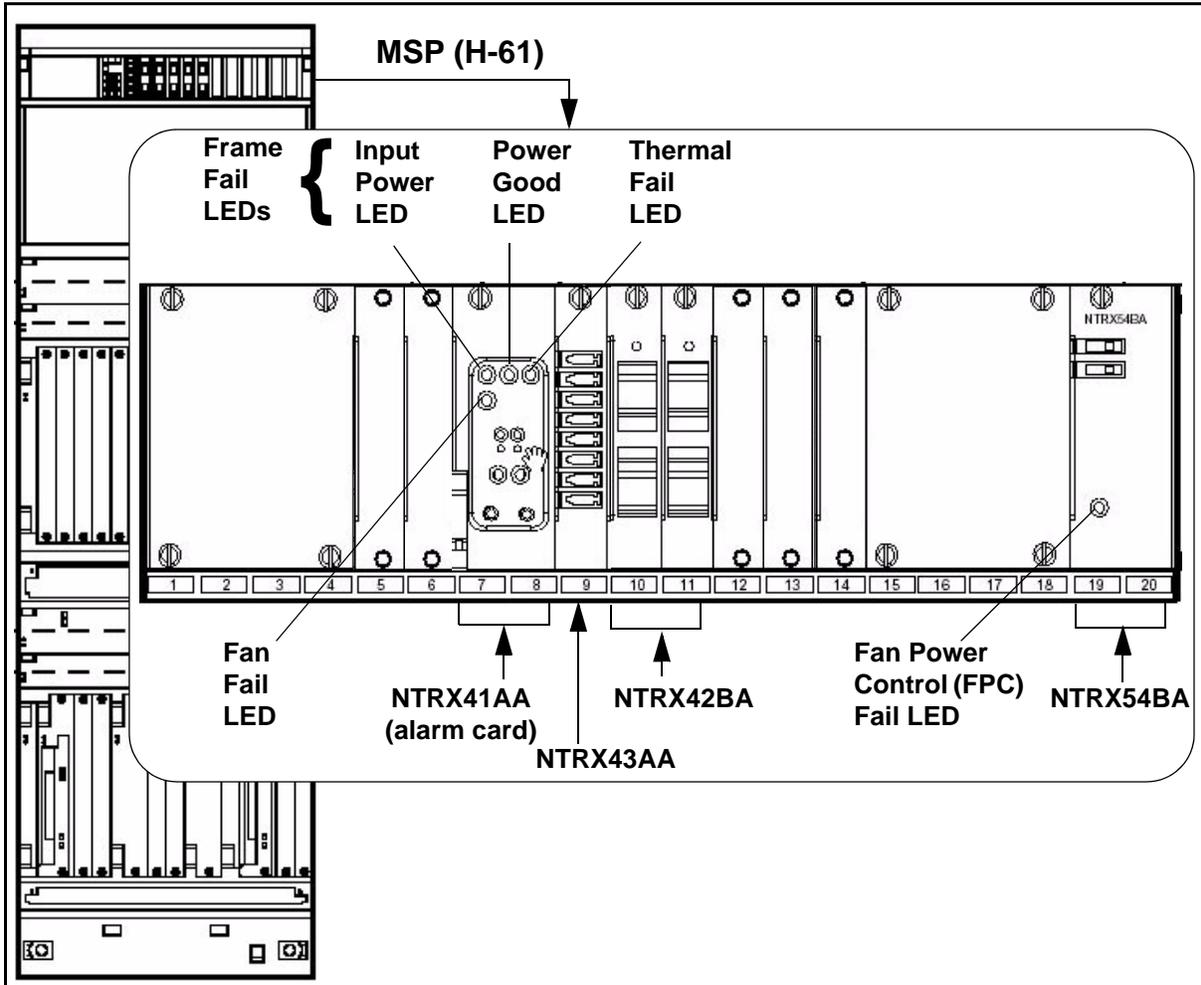
This LED is normally off, but if it is on (yellow), the thermal threshold has been reached and the CBM automatically shuts down.

Power supply failure

The status of the output power is shown by the Power Good LED on the NTRX41AA alarm card in the modular supervisory panel (MSP) at the top of the CBM cabinet. See the figure [MSP LEDs at the top of the CBM cabinet on page 118](#).

This LED is normally on (green), but if it is off, there is no output power from the CBM power supply.

MSP LEDs at the top of the CBM cabinet



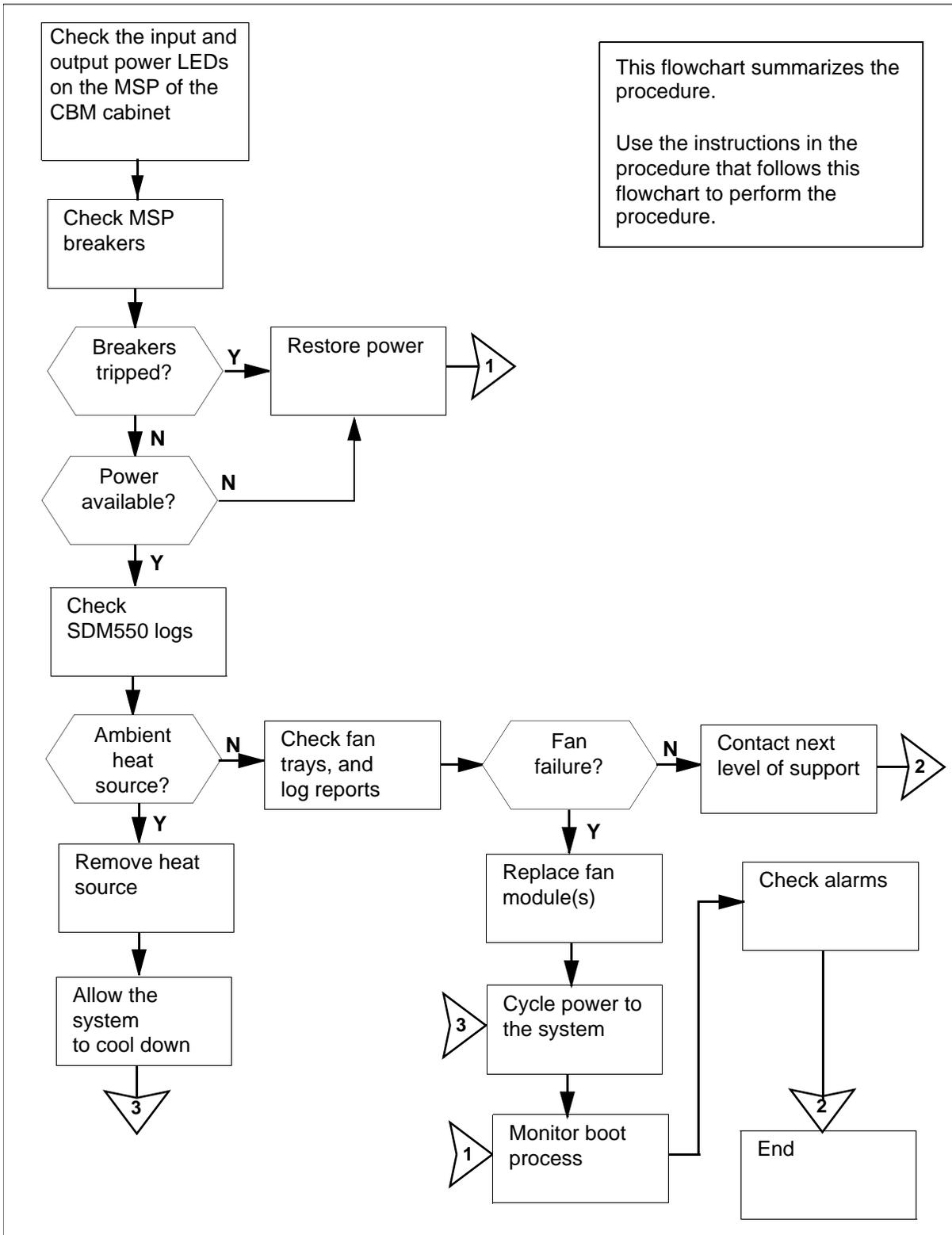
Impact

The CBM is out of service and no applications can run.

Action

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

Summary of clearing an Ext FSP major alarm



Clearing an Ext FSP major alarm

At the MSP

- 1 Check the Input Power LED on the MSP at the top of the CBM cabinet.

If the Input Power LED is	Do
on (green)	step 3
off	step 2

- 2 The -48 V dc supply to the CBM is faulty. Have qualified power maintenance personnel restore input power to the CBM. Contact Nortel Networks for assistance if required.

When power is restored, continue this procedure at step [23](#).

- 3 Check the power supply output (Power Good) LED on the MSP at the top of the CBM cabinet.

If the Input Power LED is on, and the Power Good LED is	Do
on (green)	contact your next level of support
off	step 4

- 4 Check the modular supervisory panel (MSP) breakers that supply -48V dc power to the CBM.

If the breakers have	Do
tripped	step 5
not tripped	step 6

Note: The MSP frame fail LED is lit when a breaker has tripped.

- 5 The breakers have tripped due to an over-current condition. Have qualified maintenance personnel inspect the problem. If required, contact Nortel for assistance.

When power is restored, continue this procedure at step [23](#).

- 6 Check if the fans at the bottom of the C28B cabinet have failed. If a fan has failed, replace the fan.

- 7 Determine the state of the system.

If the system has	Do
shut down	step 15
not shut down	step 8

- 8 Have qualified power maintenance personnel determine if power is available from the MSP to the CBM.

If power to the system is	Do
available	step 10
not available	step 9

- 9 Have qualified power maintenance personnel restore power. Contact Nortel Networks for assistance, if required.

When power has been restored, continue this procedure at step [23](#).

- 10 Check the Thermal Fail LED on the MSP at the top of the CBM cabinet.

If the Thermal Fail LED is	Do
off	contact your next level of support
on (yellow)	step 11

At the MAP display

- 11 The CBM has shut down due to thermal failure (overheating). Verify this by checking for recent SDM550 logs. If the CBM shut down is due to thermal failure, two logs were generated.

- SDM550 log was generated when the CBM reached its thermal warning threshold (60× C or 140× F)
- SDM550 log was generated to indicate that shutdown will occur in 1 minute because its shutdown thermal threshold has been reached (80 degrees C or 176 degrees F)

At the C28B cabinet containing the CBM

- 12 At the C28B cabinet, determine the cause of the thermal shutdown.

Note: Thermal shutdown can result from high ambient air temperature in the vicinity of the CBM, or excessive heat from an adjacent frame, or a combination of these factors.

If	Do
ambient air temperature is high	step 20
the high temperature is in the vicinity of the CBM	step 13

At the front of the CBM

- 13 Verify that both fan trays are present and fully seated in the main chassis.

If the fan trays are	Do
present and fully seated	step 14
not present or not fully seated	contact your next level of support

At the local VT100 console

- 14 Check for recent CBM-related PM128 logs indicating failure of one or both fan tray units.

If a fan failure log is	Do
generated	step 19
not generated	step 15

- 15 Ensure that the local VT100 console is connected to the CBM with the designated cable, and that the VT100 console is operational.

At the MSP

- 16 At the MSP, cycle power to the CBM by turning the MSP breakers (located at the front of the MSP) off and on. The MSP

breakers supply power to the CBM. Proceed according to the chassis in your system.

If your system contains	Do
a main chassis only	turn top two breakers off and on
a main chassis and I/O expansion chassis	turn all four breakers off and on

At the local VT100 console

- 17** The CBM begins to reboot. Monitor the boot process. When you see the following prompt,

Self Test/Boots about to Begin... Press <BREAK> at any time to Abort ALL.

press the **Break** key repeatedly to interrupt the boot process.

The FX-Bug prompt is then displayed.

At the front of the CBM

- 18** Check the operation of the three fans in each fan tray module by:
- unseating the fan module
 - physically verifying that the fan blades in each fan are rotating, and
 - reseating the fan module

If	Do
all fans are operational	contact your next level of support
one or more fans are faulty	step 19

- 19** Replace the faulty fan module(s), and then continue this procedure at step [22](#).

At the C28B cabinet containing the CBM

- 20** Remove or eliminate the heat source that caused the thermal shutdown.
- 21** Allow the CBM to cool below its thermal shutdown warning threshold (60 degrees C or 140 degrees F).

At the MSP

- 22** Cycle power to the CBM by turning both MSP breakers, located at the front of the MSP, off and on. The MSP breakers supply power to the CBM. Proceed according to the chassis in your system.

If your system contains	Do
a main chassis only	turn top two breakers off and on
a main chassis and I/O expansion chassis	turn all four breakers off and on

At the CBM

- 23** When power is restored, the CBM automatically reboots and returns to service. Monitor the system progress as follows:
- critical alarm LED shows red
 - component Out-of-Service LED flashes
 - component Out-of-Service LED turns solid
 - LEDs on the various service modules show green as they go into service
 - critical alarm LED and the Component Out-of-Service LED turn off: the System in Service LED and the CPU1 service module LED flash
 - System-in-Service LED and the CPU1 service module LED are solid green indicating completion of the reboot
 - all LEDs on the MSP are off

At the MAP display

- 24** When disk reintegration is complete, check the APPL alarm banner for CBM-related alarms. Use the alarm clearing procedures in this document to clear any faults.
- 25** 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.

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 CurrentTmplID 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 SDMBIL 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 3

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 SPFS-based server on page 236](#).
- 4 Determine whether the file system holding the billing files has adequate space by performing the procedure, [Verifying disk utilization on an SPFS-based server on page 232](#).
- 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 7
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 10
is not successful	refer to procedures Verifying the file transfer protocol and Verifying the FTP Schedule , then return to this procedure and repeat step 9 If unsuccessful afterwards, contact your next level of support

- 10 Use Audit to clear the alarm.

If the alarm	Do
cleared	step 17
did not clear	step 11

- 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 13

- 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 14
ownership for a directory is not maint	step 15
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.

If the alarm	Do
cleared	step 17
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 176](#) in this document.

If	Do
alarm fails to clear	contact next level of support
schedule does not exist	step 2

- 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

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.

Clearing an IFT alarm

At the MAP

- 1 Log in to the core manager as maint user.

If the	Do
/home/maint/ftpdirectory directory has write permissions	no action is required
/home/maint/ftpdirectory directory does not have write permissions	step 2 only
<rcLogicalVolumeDirectory>/ftpdirectory directory has write permissions	no action is required
<rcLogicalVolumeDirectory>/ftpdirectory directory does not have write permissions	step 3 only
storage disk has sufficient space	no action is required
storage disk does not have sufficient space	step 4 only
<rcLogicalVolumeDirectory> path is correct	no action is required
<rcLogicalVolumeDirectory> path is incorrect	correct the <rcLogicalVolumeDirectory> path into the CONFSTRM
<rcLogicalVolumeDirectory>/ftpdirectory is a directory	no action is required
<rcLogicalVolumeDirectory>/ftpdirectory is not a directory	step 5 only
IFT alarm persists once you have performed the appropriate steps in this procedure	contact your next level of support

- 2 Change the permissions of the /home/maint/ftpdirectory:

```
> chmod 777 /home/maint/ftpdirectory
```

- 3 Remove the <rcLogicalVolumeDirectory>/ftpdirectory:

```
> rm /<rcLogicalVolumeDirectory>/ftpdirectory
```

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>/ftplib` directory:

```
> rm /<rcLogicalVolumeDirectory>/ftplib
```

<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 176](#) 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.

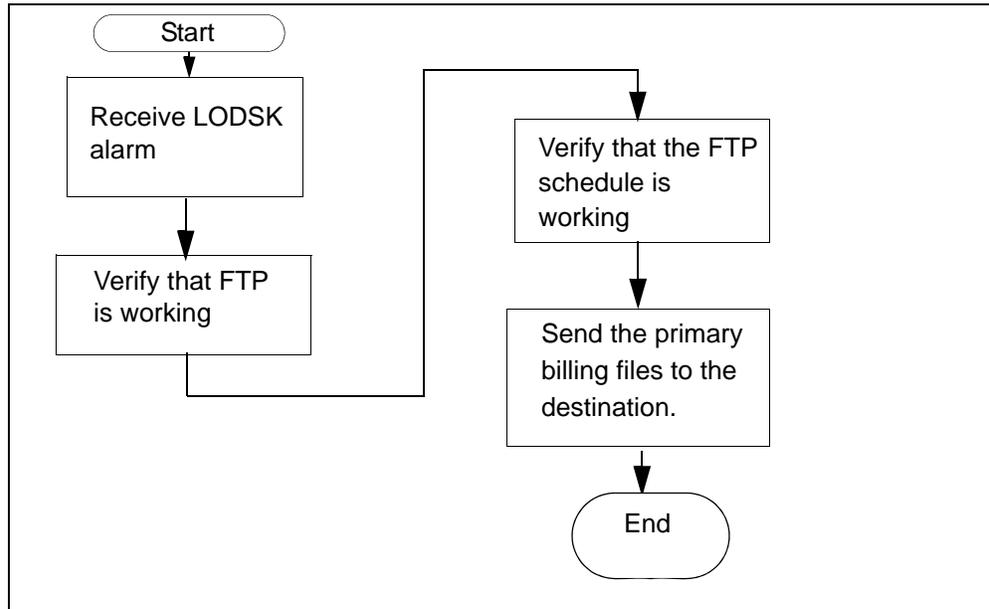
Impact

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 176](#) to determine if the FTP is working properly.

If the alarm	Do
clears	you have completed this procedure
does not clear	refer to procedure Verifying the FTP Schedule on page 183 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

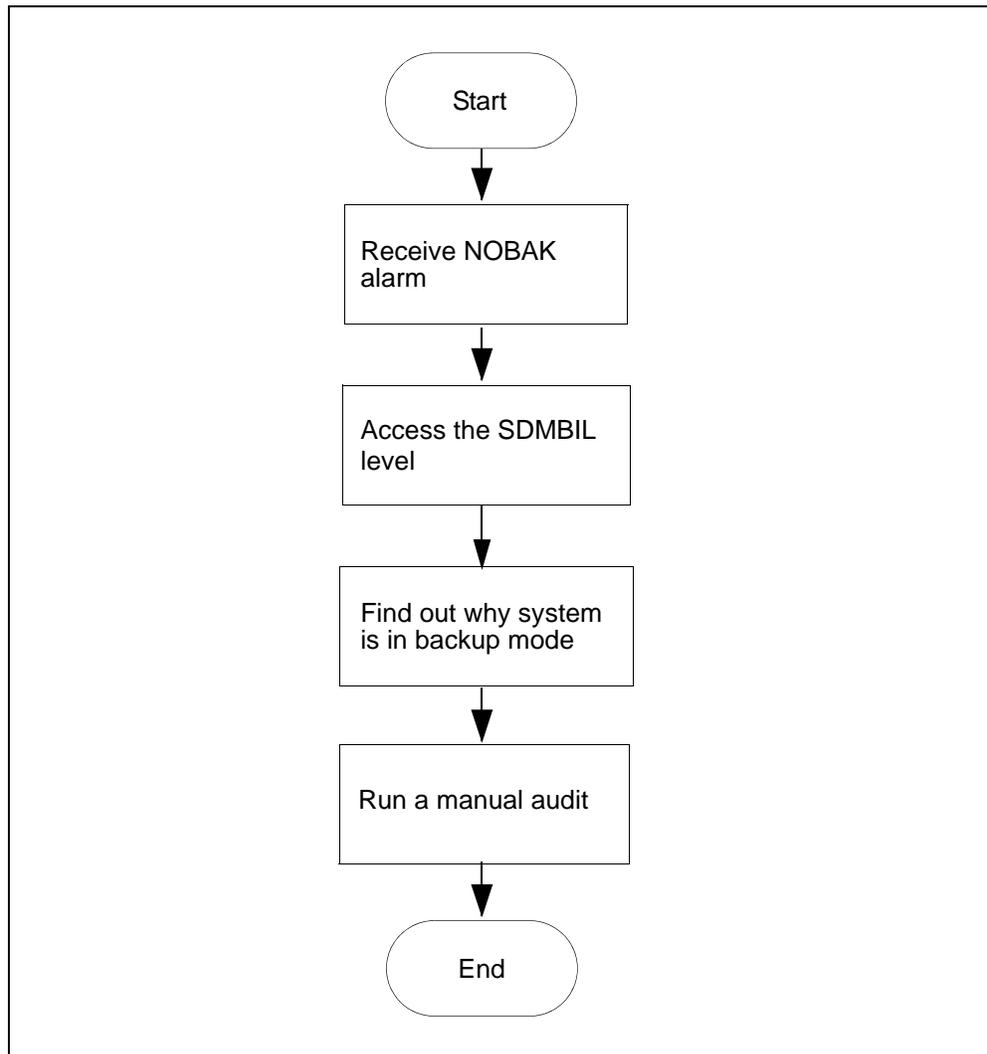
ATTENTION

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



Clearing a NOBAK alarm

At the MAP

- 1 Post the billing stream:

```
> mapci;mtc;appl;sdmbil;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 5 .
RBsy	refer to Clearing a major SBACP alarm on page 167 , and then return to step 5 .
ManB	Go to step 8
Bkup	Go to step 8

5 Use Audit to clear the alarm.

If the alarm	Do
cleared	step 6
did not clear	step 8

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 12
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 114](#)

9 Use Audit to clear the alarm.

If the alarm	Do
cleared	step 10
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 12

If the billing system	Do
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 NOCOM alarm

Purpose

Use this procedure to clear a no communications (NOCOM) alarm.

Indication

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

Meaning

Ethernet infrastructure has failed between the Core and the core manager.

The most likely causes of this alarm are

- OC-3 links are not in-service making the core manager SysB
- core manager power is off, or
- core manager is rebooting

Impact

No data is transferred to the core manager. Data is sent to the configured backup disk on the core.

If the stream is set to `both`, data is still being routed to device independent recording package (DIRP). You can send the billing records to the operating company collector through the previously established network used by DIRP.

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.

Procedure

At the MAP

- 1 Access the APPL SDM Menu level:

```
> mapci;mtc;appl;sdm
```

If the core manager is	Do
Offl or SysB	step 2
ManB	step 3
InSv or ISTb	step 4

- 2 Busy the core manager:

```
> bsy
```

- 3 Return the core manager to service:

```
> rts
```

Note 1: Returning the core manager to service establishes communication between the core and the core manager. If the first attempt fails to return the core manager to service, the system re-attempts to establish communication until it is successful.

Note 2: The SDM Billing Application (SBA) and any streams configured for real-time billing (RTB) are also returned to service when the core manager is returned to service. Log report SDMB375 is generated when a stream configured for RTB fails to return to service.

If the core manager	Do
returns to service successfully	step 4
does not return to service successfully	contact your next level of support

- 4 Determine the status of the alarm.

If the alarm	Do
cleared	step 5
did not clear	contact your next level of support

At the core manager

- 5 Check for log SDMB375.

If the system	Do
generates log SDMB375	step 6
does not generate log SDMB375	you have completed this procedure

- 6 Access the billing maintenance level:

```
# billmtc
```

- 7 Access the schedule level:

```
> schedule
```

- 8 Access the real-time billing level:

```
> rtb
```

- 9 Busy the stream:

```
> bsy <stream_name>
```

where:

<stream_name>

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

- 10 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	you have completed this procedure
does not return to service successfully	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.

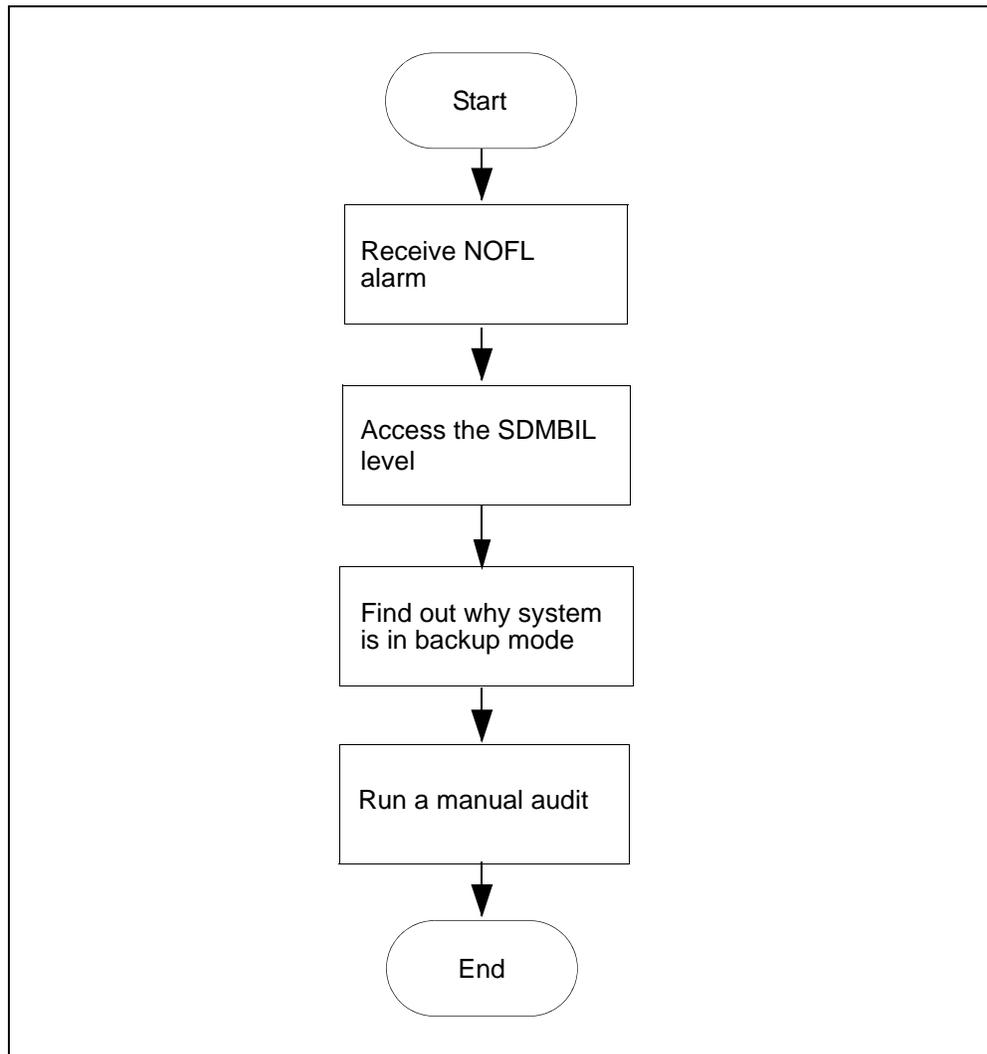
Impact

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



Clearing a NOFL 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 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 5 .
RBsy	refer to Clearing a major SBACP alarm on page 167 , and then return to step 5 .
ManB	Go to step 8
Bkup	Go to step 8

5 Use Audit to clear the alarm.

If the alarm	Do
cleared	step 6
did not clear	step 8

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 12
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 114](#)**9** Use Audit to clear the alarm.

If the alarm	Do
cleared	step 10
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 12
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` 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

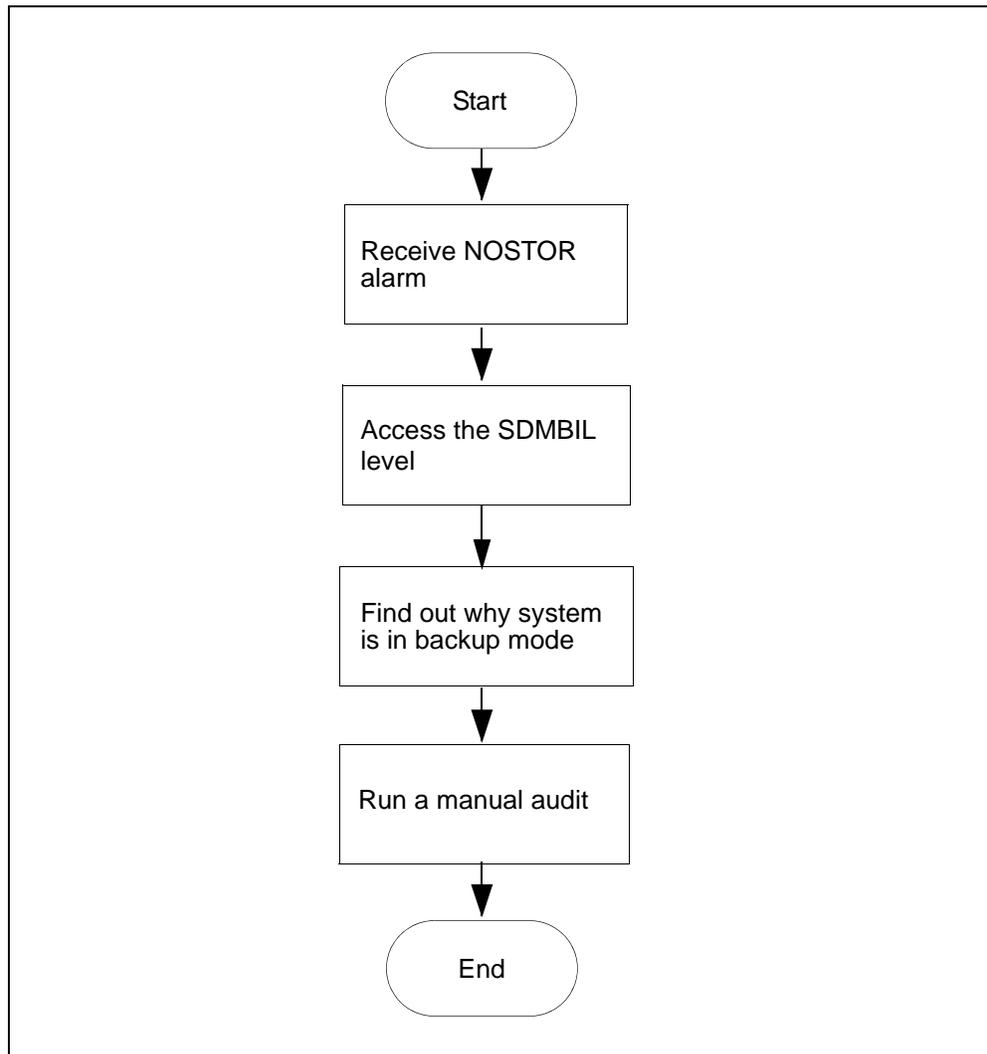
ATTENTION

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 5 .
RBsy	refer to Clearing a major SBACP alarm on page 167 , and then go to step 5 .
ManB	RTS the billing stream
Bkup	Go to step 8

- 5 Use Audit to clear the alarm.

If the alarm	Do
cleared	step 6
did not clear	step 8

- 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 12
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 114](#)

- 9 Use Audit to clear the alarm.

If the alarm	Do
cleared	step 10
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 12
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.

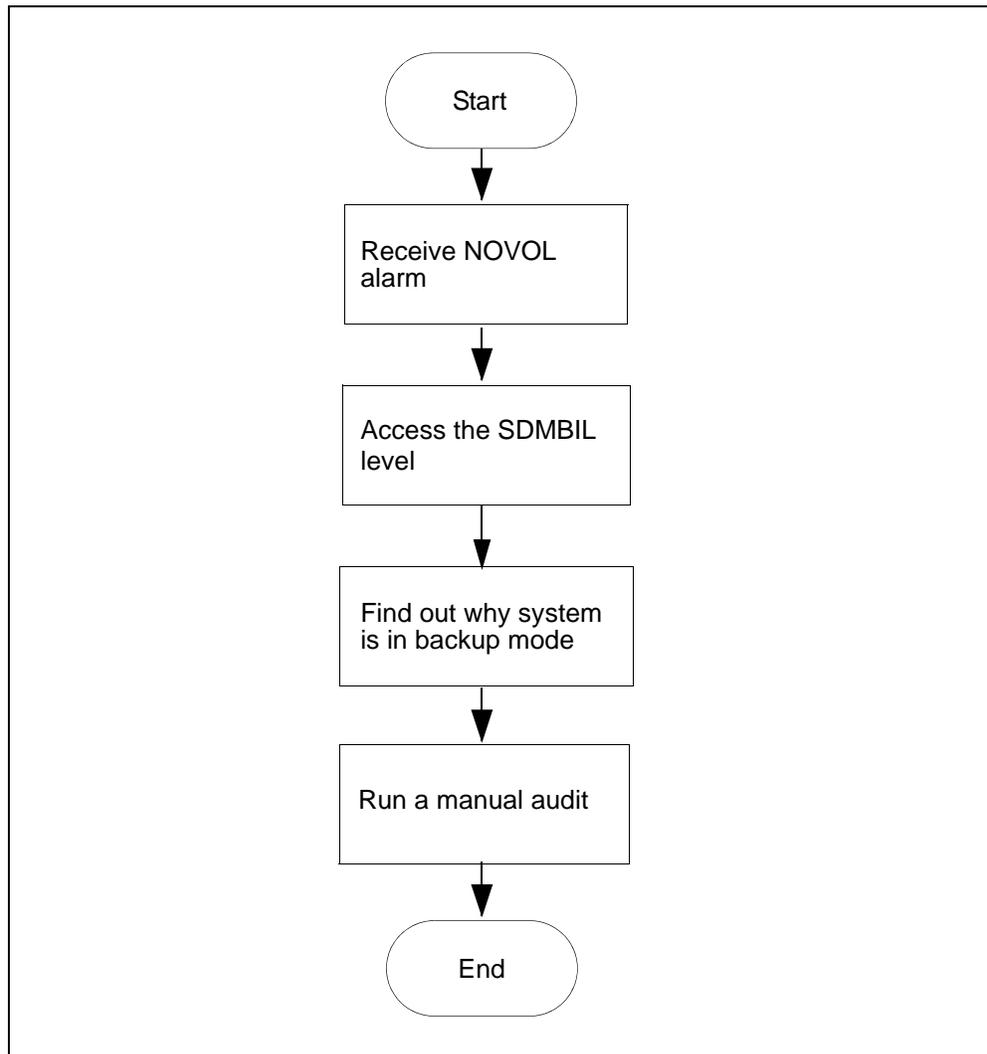
Impact

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;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 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 5 .
RBsy	refer to Clearing a major SBACP alarm on page 167 , and then go to step 5 .
ManB	Go to step 8
Bkup	Go to step 8

- 5 Use Audit to clear the alarm.

If the alarm	Do
cleared	step 6
did not clear	step 8

- 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 12
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 114](#)

- 9 Use Audit to clear the alarm.

If the alarm	Do
cleared	step 10
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 12
is not in recovery	contact your next level of support

12 You have completed this procedure.

Clearing an RTBCD alarm

Indication

At the MTC level of the MAP display, RTBCD appears under the APPL header of the alarm banner and indicates a critical problem for the Real Time Billing (RTB) program.

The core manager generates the SDMB375 log report when this alarm is raised.

Meaning

The RTBCD alarm indicates that the RTB child (rtbChild) process has died abnormally.

Impact

A critical problem for the Real Time Billing (RTB) program exists.

Action

This alarm is cleared when the killed RTB process is restarted properly by the SBA. An SDMB675 log report is generated when the alarm is cleared. Contact your next level of support if this alarm fails to clear.

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 moves to the SysB state and 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 moves to the SysB state.

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 MAP

- 1 Access the APPL SDM Menu level:

```
> mapci;mtc;appl;sdm
```

If the core manager is	Do
Offl or SysB	step 2
ManB	step 3
InSv or ISTb	step 4

- 2 Busy the core manager:

```
> bsy
```

3 Return the core manager to service:

```
> rts
```

Note 1: Returning the core manager to service establishes communication between the core and the core manager. If the first attempt fails to return the core manager to service, the system attempts to establish communication until it is successful.

Note 2: The SDM Billing Application (SBA) and any streams configured for real-time billing (RTB) are also returned to service when the core manager is returned to service.

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

If the core manager	Do
returned to service successfully	step 4
did not return to service successfully	contact your next level of support

At the core manager**4** Go to the Appl level of the cbmmtc tool by typing:

```
cbmmtc appl
```

If the SBA application is	Do
ISTB, Offl, or SysB	step 5
ManB	step 6
InSv, and the alarm is cleared	step 13
InSv, but the alarm is still present	contact your next level of support

5 Busy the SBA application:

```
bsy <SBA_no>
```

where

<SBA_no> is the number next to the SBA application.

- 6 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 7
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

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

```
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> DIRP <destination_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> DIRP <destination_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	you have completed this procedure
does not return to service successfully	contact your next level of support

- 13 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

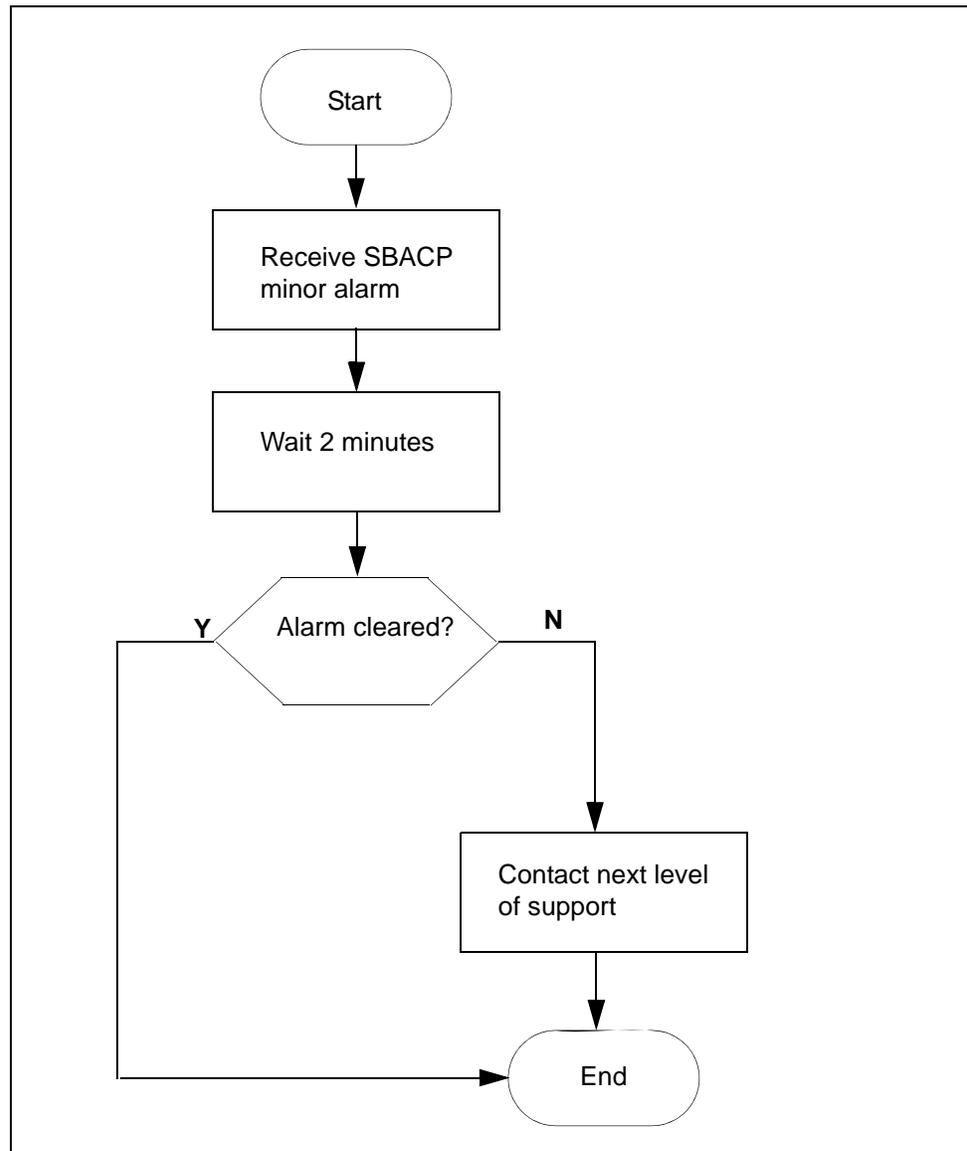
The SBA program is shutting down because one of the processes has failed three times in one minute.

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

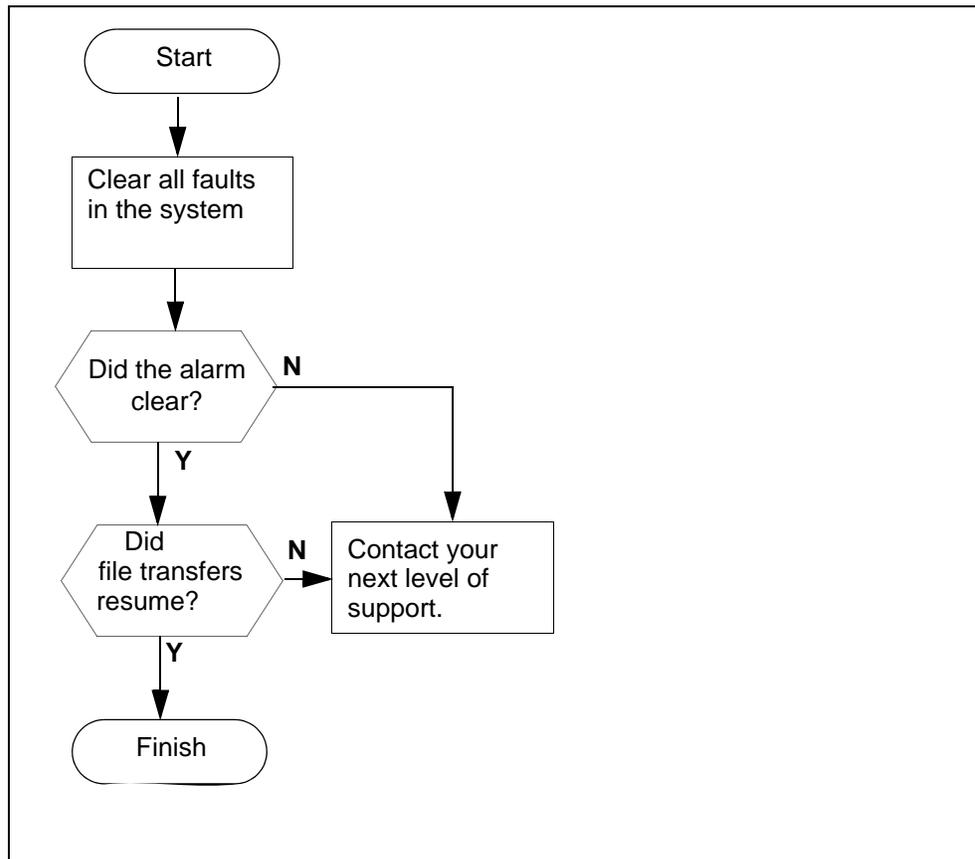
If the alarm does not clear, SBA is not able to transfer files to the downstream destination:

- 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 2
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 4
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 5
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

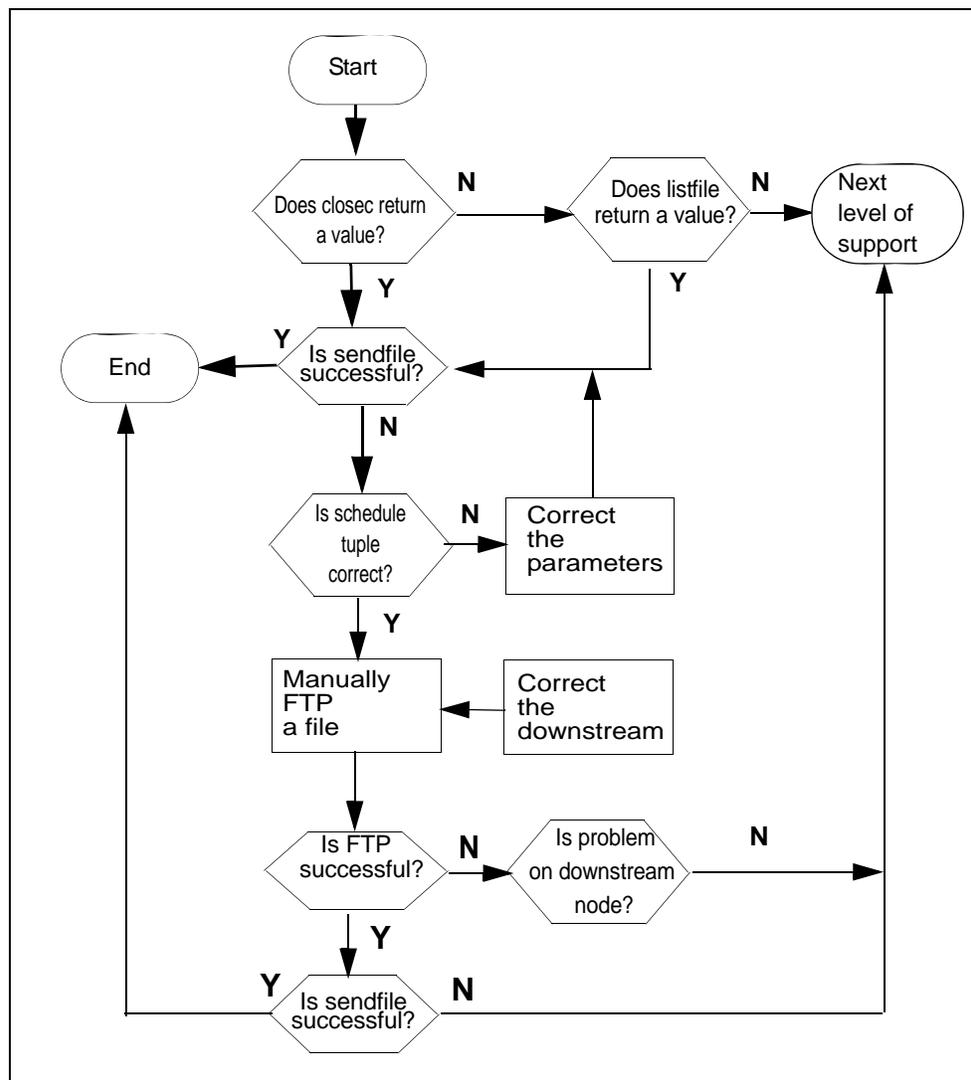
Purpose

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 7
does not return a filename	step 5

- 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 10

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 21
incorrect	step 12

- 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 7
determined that the parameters are correct	<ul style="list-style-type: none"> • step 20 (verify login and write permissions are correct for FTP process without testing a billing file), OR • step 23 (verify login and write permissions are correct for FTP process while testing an actual billing file)

- 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 RNT0 command successful”.

- 35** Exit from the FTP session:

```
ftp> quit
```

If the file transfer is	Do
successful	step 38
unsuccessful because of a permission error	step 36
unsuccessful for a reason other than permission error	step 38

- 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

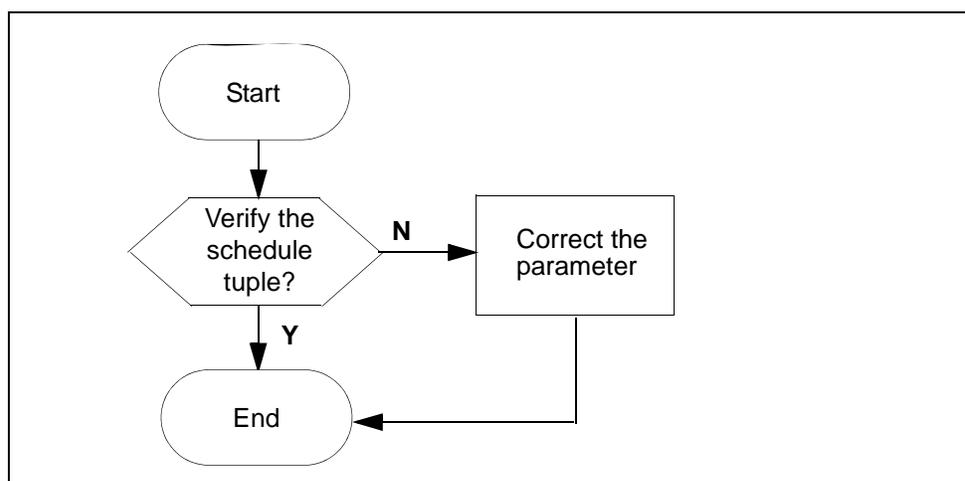
Purpose

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 5

- 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 13

- 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 SPFS-based server

Application

Use this procedure to replace one or more failed disk drives on a Carrier VoIP Server Platform Foundation Software (SPFS)-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 SPFS 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 186](#)
- [Netra 240 on page 187](#)

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:

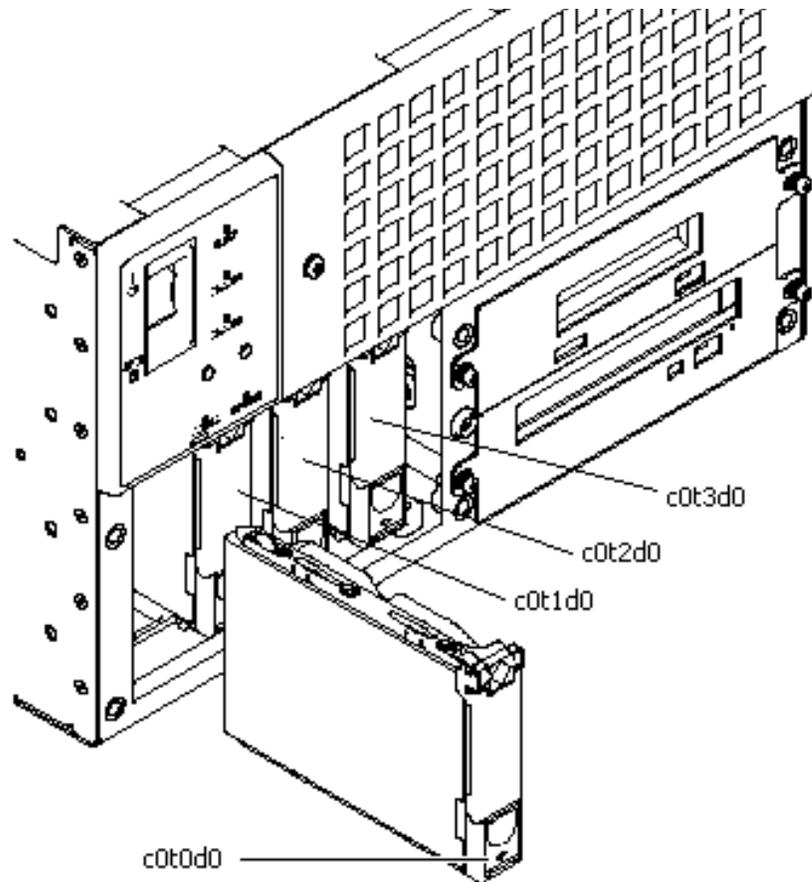
- [Replacing failed disks on a Netra t1400 on page 188](#)
- [Replacing failed disks on a Netra 240 simplex on page 191](#)
- [Replacing failed disks on a Netra 240 cluster \(two-server\) on page 193](#)

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

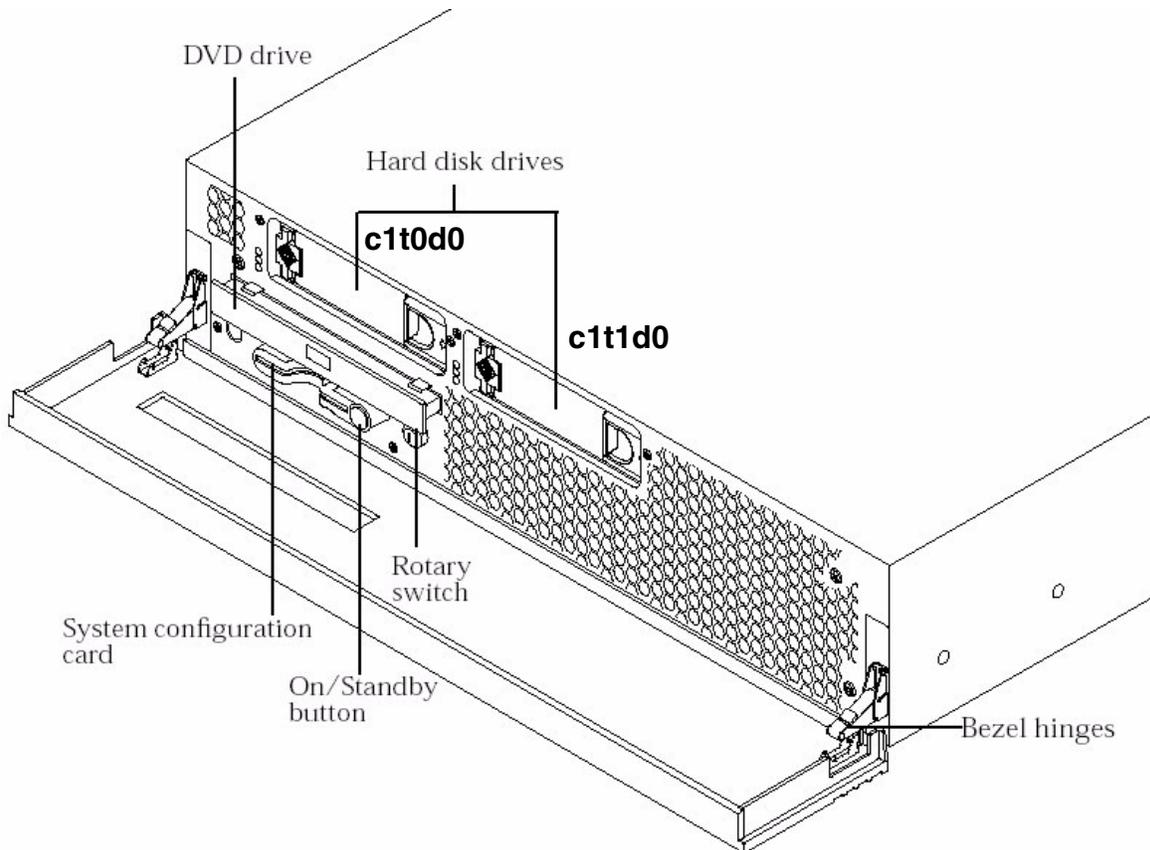


Netra 240

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 186](#).
- 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
c0t1d0	step b
c0t2d0	step c
c0t3d0	step d

- 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 1
do not have another disk to physically replace	step 5

- 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 6
3 disks	step 6
4 disks	step 6

- 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 187](#).
- 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
c1t1d0	step b

- 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/c1t0d0s2 | 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 1
do not have another disk to replace	step 5

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

If you replaced	Do
1 disk	you have completed this procedure
both disks	step 6

- 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 187](#).
- 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
c1t1d0	step b

- 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/c1t0d0s2 | 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 SPFS-based server

Application

Use this procedure to shut down a Carrier VoIP Server Platform Foundation Software (SPFS)-based server, which may be hosting one or more of the following components:

- CS 2000 Management Tools
- Integrated Element Management System (IEMS)
- Audio Provisioning Server (APS)
- Media Gateway (MG) 9000 Manager
- CS 2000 SAM21 Manager
- Network Patch Manager (NPM)
- Core and Billing Manager (CBM)
- Multiservice Data Manager (MDM)

Note: MDM when installed on SPFS-based servers is not configured as a two-server cluster but as two distinct one-server configurations.

ATTENTION

The SPFS-based server may be hosting more than one of the above components, therefore, ensure it is acceptable to shut down the server.

Prerequisites

You must have root user privileges.

Action

Use one of the following procedures according to your office configuration:

- [One-server configuration on page 197](#)
- [Two-server \(cluster\) configuration on page 198](#)

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 SPFS-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 -**
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.
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 SPFS-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 SPFS-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).

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 DVD-RW for use

Application

Use this procedure to verify the 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 DVD into the drive.

Note: Only rewriteable media can be erased. Verify that the DVD you are attempting to erase is a 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 SPFS-based server

- 3 When prompted, enter your user ID and password.
- 4 Use the following table to determine your next step.

If the DVD is	Do
new	step 5
used	step 6

- 5 Verify the DVD is ready for use by typing

```
$ cdrw -1
```

and pressing the Enter key

If the system response	Do
provides the CD device	step 11
indicates “No CD writers found or no media in the drive”	step 6

- 6 Erase the contents of the 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 Reinsert the DVD into the drive.

- 8 Verify the DVD is ready for use by typing

```
$ cdrw -1
```

and pressing the Enter key

If the system response	Do
provides the CD device	step 11
indicates “No CD writers found or no media in the drive” or “Media in the device is not erasable”	step 9

- 9 Eject the DVD 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 DVD 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 DVD from the drive.

10 Obtain another DVD and repeat the process starting with step [4](#).

11 Proceed to use the DVD.

You have completed this procedure.

Increasing the size of a file system on an SPFS-based server

Application

Use one of the following procedures to increase the size of a file system on a Carrier VoIP Server Platform Foundation Software (SPFS)-based server:

- [Simplex configuration \(one server\) on page 204](#)
- [High-availability configuration \(two servers\) on page 209](#)

It is recommended you perform this procedure during off-peak hours.

The Carrier VoIP Server Platform Foundation Software (SPFS) 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.

SPFS 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 procedure [Performing a backup of file systems on an SPFS-based server on page 222](#) 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

```
# /opt/nortel/sspfs/fs/meta.pl fs
```

and pressing the Enter key.

Divide the resulting number by 2048, which 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 b

- b** Use the following table to determine your next step.

If	Do
the value you determined in step 8 (size by which to increase the file system) is greater than the value you obtained in step 9a (amount of free disk space you can allocate to file systems)	contact Nortel Networks for assistance
the value you determined in step 8 (size by which to increase the file system) is less than the value you obtained in step 9a (amount of free disk space you can allocate to file systems)	step 10

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

```
# filesys 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

```
# filesys 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 2
ssh (secure)	step 6

- 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

```
/opt/nortel/sspfs/fs/meta.pl fs
```

and pressing the Enter key.

Divide the resulting number by 2048, which 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 if required.

You have completed this procedure.

## Starting the SAM21 Manager server application

### Application

Use this procedure to start the SAM21 Manager server application on the SPFS-based server that is hosting the CS 2000 Management Tools.

### Prerequisites

None

### Action

Perform the following steps to complete this procedure.

#### ATTENTION

In a two-server configuration, perform the steps that follow on the active server.

#### *At your workstation*

- 1 Establish a login session to the server, using one of the following methods:

| If using          | Do                     |
|-------------------|------------------------|
| telnet (unsecure) | step <a href="#">2</a> |
| ssh (secure)      | step <a href="#">3</a> |

- 2 Log in to the server using telnet (unsecure) as follows:

- a 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 SPFS-based server, or the physical IP address of the active server in a two-server configuration

**b** When prompted, enter your user ID and password.

**c** Change to the root user by typing

```
$ su -
```

and pressing the Enter key.

**d** When prompted, enter the root password.

**Note:** In a two-server configuration, 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.

Proceed to step [4](#).

**3** 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 IP address or host name of the SPFS-based server, or the physical IP address of the active server in a two-server configuration

**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.

**Note:** In a two-server configuration, 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.

- 4 Verify the status of the SAM21 Manager server application by typing

```
servman query -status -group SAM21EM
```

and pressing the Enter key.

---

| If SAM21EM is | Do                     |
|---------------|------------------------|
| not running   | step <a href="#">5</a> |
| running       | step <a href="#">7</a> |

---

- 5 Start the SAM21EM server application by typing

```
servstart SAM21EM
```

and pressing the Enter key.

- 6 Verify the SAM21EM server application started by typing

```
servman query -status -group SAM21EM
```

and pressing the Enter key.

*Example response:*

```
Executing: /opt/servman/bin/servquery -status
-group SAM21EM
```

```
Succession SAM21 Element Manager version:
SAM21EM_9_020_0
```

```
Current status of the Succession SAM21 Element
Manager:
```

```
SNMP Access Gateway is running.
```

```
SAM21 Element Manager Server is running.
```

- 7 You have completed this procedure. If applicable, return to the high level task or procedure that directed you to this procedure.

---

## Stopping the SAM21 Manager server application

---

### Application

Use this procedure to stop the SAM21 Manager server application on the SPFS-based server that is hosting the CS 2000 Management Tools.

### Prerequisites

None

### Action

Perform the steps that follow to complete this procedure.

**ATTENTION**

In a two-server configuration, perform the steps that follow on the active server.

#### *At your workstation*

- 1 Establish a login session to the server, using one of the following methods:

---

| <b>If using</b> | <b>Do</b> |
|-----------------|-----------|
|-----------------|-----------|

---

|                   |                        |
|-------------------|------------------------|
| telnet (unsecure) | step <a href="#">2</a> |
|-------------------|------------------------|

|              |                        |
|--------------|------------------------|
| ssh (secure) | step <a href="#">3</a> |
|--------------|------------------------|

---

- 2 Log in to the server using telnet (unsecure) as follows:

- a 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 CS 2000 Management Tools server, or the physical IP address of the active server in a two-server configuration

**b** When prompted, enter your user ID and password.

**c** Change to the root user by typing

```
$ su -
```

and pressing the Enter key.

**d** When prompted, enter the root password.

**Note:** In a two-server configuration, 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.

Proceed to step [4](#).

**3** 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 IP address or host name of the CS 2000 Management Tools server, or the physical IP address of the active server in a two-server configuration

**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.

**Note:** In a two-server configuration, 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.

- 4 Verify the status of the SAM21 Manager server application by typing

```
servman query -status -group SAM21EM
```

and pressing the Enter key.

---

| If SAM21EM is | Do |
|---------------|----|
|---------------|----|

---

|         |                        |
|---------|------------------------|
| running | step <a href="#">5</a> |
|---------|------------------------|

|             |                        |
|-------------|------------------------|
| not running | step <a href="#">7</a> |
|-------------|------------------------|

---

- 5 Stop the SAM21EM server application by typing

```
servstop SAM21EM
```

and pressing the Enter key.

- 6 Verify the SAM21EM server application stopped by typing

```
servman query -status -group SAM21EM
```

and pressing the Enter key.

*Example response:*

```
Executing: /opt/servman/bin/servquery -status
-group SAM21EM
```

```
Succession SAM21 Element Manager version:
SAM21EM_9_020_0
```

```
Current status of the Succession SAM21 Element
Manager:
```

```
 SNMP Access Gateway is not running.
```

```
 SAM21 Element Manager Server is not running.
```

- 7 You have completed this procedure. If applicable, return to the high level task or procedure that directed you to this procedure.

---

## Performing a backup of file systems on an SPFS-based server

---

### Application

Use this procedure to perform a backup of the file systems on a Carrier VoIP Server Platform Foundation Software (SPFS)-based server (Sun Netra t1400 or Sun Netra 240).

The server can be hosting one or more of the following components:

- CS 2000 Management Tools
- Integrated Element Management System (IEMS)
- Audio Provisioning Server (APS)
- Media Gateway 9000 Manager
- Network Patch Manager (NPM)
- Core and Billing Manager (CBM)

### Prerequisites

This procedure has the following prerequisites:

- You must perform a data backup prior to performing this procedure.

**Note:** The data backup is not required prior to this procedure for the Core and Billing Manager (CBM) or the MG 9000 Manager.

- For a Sun Netra t1400, use a blank 4mm Digital Data Storage (DDS-3) tape of 125m and 12 GB to store the data.
- For a Sun Netra 240, use one or more blank DVD-R or DVD-RW disks to store the data

**Note 1:** The backup utility limits the storage to 4 GB on a DVD-R and DVD-RW.

**Note 2:** If you are using a new DVD-RW, or want to reuse a used DVD-RW and need to erase the contents, complete procedure “Preparing a CD-RW or DVD-RW for use” in *ATM/IP Security and Administration*, NN10402-600.

## Action

### ATTENTION

In a two-server configuration, execute this procedure on the active server.

#### *At the server*

- 1 Insert the blank tape DVD into the drive. In a two-server configuration, insert the blank 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 SPFS-based server on which you are performing the backup

In a two-server configuration, enter the physical IP address of the active server.

- 3 When prompted, enter your user ID and password.

- 4 Change to the root user by typing

```
$ su -
```

and pressing the Enter key.

- 5 When prompted, enter the root password.

In a two-server configuration, 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.

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

| If you are using  | Do                     |
|-------------------|------------------------|
| a tape for backup | step <a href="#">7</a> |
| a DVD for backup  | step <a href="#">8</a> |

- 7** Rewind the tape by typing  
`# mt -f /dev/rmt/0 rewind`  
 and pressing the Enter key.
- 8** Back up the file systems by typing  
`# /opt/nortel/spfs/bks/bkfullsys`  
 and pressing the Enter key.  
*Example response:*  
 Backup Completed Successfully
- Note:** If you are using DVD, the system will prompt you to insert another blank disk if more than one is needed.
- 9** Use the following table to determine your next step.
- | If you are using  | Do                      |
|-------------------|-------------------------|
| a tape for backup | step <a href="#">10</a> |
| a DVD for backup  | step <a href="#">12</a> |
- 10** List the contents of the tape by typing  
`# gtar -tvMf /dev/rmt/0`  
 and pressing the Enter key.
- 11** Eject and remove the tape from the drive, label it, write-protect it, and store it in a safe place.  
 Proceed to step [19](#).
- 12** Insert the backup DVD into the drive. If the backup resides on multiple DVDs, insert the first backup DVD.
- 13** List the contents of the DVD by typing  
`# gtar -tvMf /cdrom/*bkfullsys*/*.tar`  
 and pressing the Enter key.
- | If you                                            | Do                      |
|---------------------------------------------------|-------------------------|
| receive a prompt to prepare another volume        | step <a href="#">14</a> |
| do not receive a prompt to prepare another volume | step <a href="#">16</a> |
- 14** Press the Return key.
- 15** Stop the gtar process by pressing the Ctrl and C keys.

- 16** Ensure you are at the root directory level by typing  
`# cd /`  
and pressing the Enter key.
- 17** Eject the DVD by typing  
`# eject cdrom`  
and pressing the Enter key.  
If the disk drive tray will not open after you have determined that the disk 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 disk drive.
- 18** Remove the DVD from the drive, label it, and store it in a safe place.
- | <b>If the backup</b>    | <b>Do</b>                                                                        |
|-------------------------|----------------------------------------------------------------------------------|
| resides multiple DVDs   | Insert the next backup DVD in the disk drive and go to step <a href="#">13</a> . |
| resides on a single DVD | step <a href="#">19</a>                                                          |
- 19** You have completed this procedure. If applicable, return to the high-level task or procedure that directed you to this procedure.

---

## Performing a full system restore on an SPFS-based server

---

### Application

Use this procedure to perform a full system restore from backup media on a VoIP Server Platform Foundation Software (SPFS)-based server (Sun Netra t1400 or Sun Netra 240).

A full system restore consists of reverting to the previous release of SPFS, restoring the file systems, and restoring the oracle data.

The server can be hosting one or more of the following components:

- CS 2000 Management Tools
- Integrated Element Management System (IEMS)
- Audio Provisioning Server (APS)
- Media Gateway (MG) 9000 Manager
- CS 2000 SAM21 Manager
- Network Patch Manager
- Core Billing Manager (CBM)

**Note:** Restoring the oracle data does not apply to the CBM as it does not use an oracle database.

#### ATTENTION

System logs indicating application and database errors generate until the file systems and oracle data are restored on the system. No database errors generate on the CBM as it does not use an oracle database.

### Prerequisites

To complete this procedure you need

- the SPFS Installation CD disk#1 for the release you are reverting to
- the tape or DVD on which you backed up the file systems
- the tape or DVD on which you backed up the oracle data

### Action

Use one of the methods below according to your office configuration.

- [Simplex configuration \(one server\) on page 227](#)
- [High-availability configuration \(two servers\) on page 229](#)

**Note:** Only the [Simplex configuration \(one server\)](#) uses a full system restore from tape on a Sun Netra t1400 server.

## Simplex configuration (one server)

### At the server console

- 1 Log in to the server through the console (port A) using the root user ID and password.
- 2 Bring the system to the OK prompt by typing  
`# init 0`  
and pressing the Enter key.
- 3 Insert SPFS Installation CD disk#1 into the drive.
- 4 Use the following table to determine your next step.

| If restoring from | Do                     |
|-------------------|------------------------|
| tape              | <a href="#">step 5</a> |
| DVD               | <a href="#">step 6</a> |

- 5 Insert the tape with the backed up file systems into the drive.
- 6 At the OK prompt, restore the system by typing  
`OK boot cdrom - restore`  
and pressing the Enter key.
- 7 When prompted, accept the software license restrictions by typing  
`ok`  
and pressing the Enter key.  
The system reboots.

**Note:** If the restore process fails at this point due to one or more disks not being labeled, which is reported as “Bad Magic Number in Disk Label”.

If restoring from DVD, you will be prompted to insert Volume 1 of the backup DVD into the drive. Insert the DVD on which you backed up the file systems. During the restore process, the system will prompt you for additional Volumes if more than one DVD was used during the backup of file systems.

The restore process can take several hours to complete depending on the number and size of the files that are being restored.

**Note:** Although it can appear as if the system is hanging at times, please do not interrupt the restore process. If you suspect an issue with the restore process, please contact your next level of support.

**8** Eject the backup DVD 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 DVD by typing

```
eject cdrom
```

and pressing the Enter key.

**Note:** If the DVD drive tray does not open (if not busy or 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 backup DVD from the drive.

**9** Use the following table to determine your next step.

| If                                        | Do                      |
|-------------------------------------------|-------------------------|
| this SPFS-based server is hosting the CBM | <a href="#">step 13</a> |
| otherwise                                 | <a href="#">step 10</a> |

**10** List the oracle groups by typing

```
groups oracle
```

and pressing the Enter key.

| If the output is                       | Do                      |
|----------------------------------------|-------------------------|
| oinstall data dba or oinstall dba data | <a href="#">step 11</a> |
| oinstall dba data                      | <a href="#">step 12</a> |

- 11 Correct the oracle groups by typing  

```
usermod -g oinstall -G data,dba oracle
```

and pressing the Enter key.
- 12 Restore the oracle data, if required. Once the data restore is complete, continue to [step 13](#).
- 13 Reboot the server by typing  

```
init 6
```

and pressing the Enter key.  
You have completed this procedure.

### High-availability configuration (two servers)

#### *At the console connected to the inactive node*

- 1 Log in to the inactive node through the console (port A) using the root user ID and password.
- 2 Bring the system to the OK prompt by typing  

```
init 0
```

and pressing the Enter key.

#### *At the console connected to the active node*

- 3 Log in to the active node through the console (port A) using the root user ID and password.
- 4 Access the OK prompt by typing  

```
init 0
```

and pressing the Enter key.
- 5 Insert SPFS Installation CD disk#1 into the drive.
- 6 At the OK prompt, restore the system by typing  

```
OK boot cdrom - restore
```

and pressing the Enter key.
- 7 When prompted, accept the software license restrictions by typing  

```
ok
```

and press the Enter key.  
The system reboots.

- 8** When prompted, insert Volume 1 of the DVD on which you backed up the file systems, into the drive.
- Note:** During the restore process, the system will prompt you for additional Volumes if more than one DVD was used during the backup of file systems.
- The restore process can take several hours to complete depending on the number and size of the files that are being restored.
- Note:** Although it can appear as if the system is hanging at times, please do not interrupt the restore process. If you suspect an issue with the restore process, please contact your next level of support.
- 9** Eject the backup DVD from the drive as follows:
- Ensure you are at the root directory level by typing  
`# cd /`  
and pressing the Enter key.
  - Eject the CD by typing  
`# eject cdrom`  
and pressing the Enter key.
- Note:** If the DVD drive tray does not open (if not busy or 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.
- Remove the backup DVD from the drive.
- 10** Use the following table to determine your next step.
- | If | Do |
|---|-------------------------|
| this SPFS-based server is hosting the CBM | step 14 |
| otherwise | step 11 |
- 11** List the oracle groups by typing
`# groups oracle`

and pressing the Enter key.

If the output is	Do
oinstall data dba or oinstall dbs data	step 12
oinstall dba data	step 13

- 12** Correct the oracle groups by typing
`# usermod -g oinstall -G data,dba oracle`
and pressing the Enter key.
- 13** Restore the data. Once the data restore is complete, execute [step 14](#) and [step 15](#).
- 14** Reboot the server by typing
`# init 6`
and pressing the Enter key.
- 15** Re-image the inactive node using the active node's image. If required.
- You have completed this procedure.

Verifying disk utilization on an SPFS-based server

Application

Use this procedure to verify disk utilization by the file systems on a Carrier VoIP Server Platform Foundation Software (SPFS)-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 SPFS-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 SPFS-based server

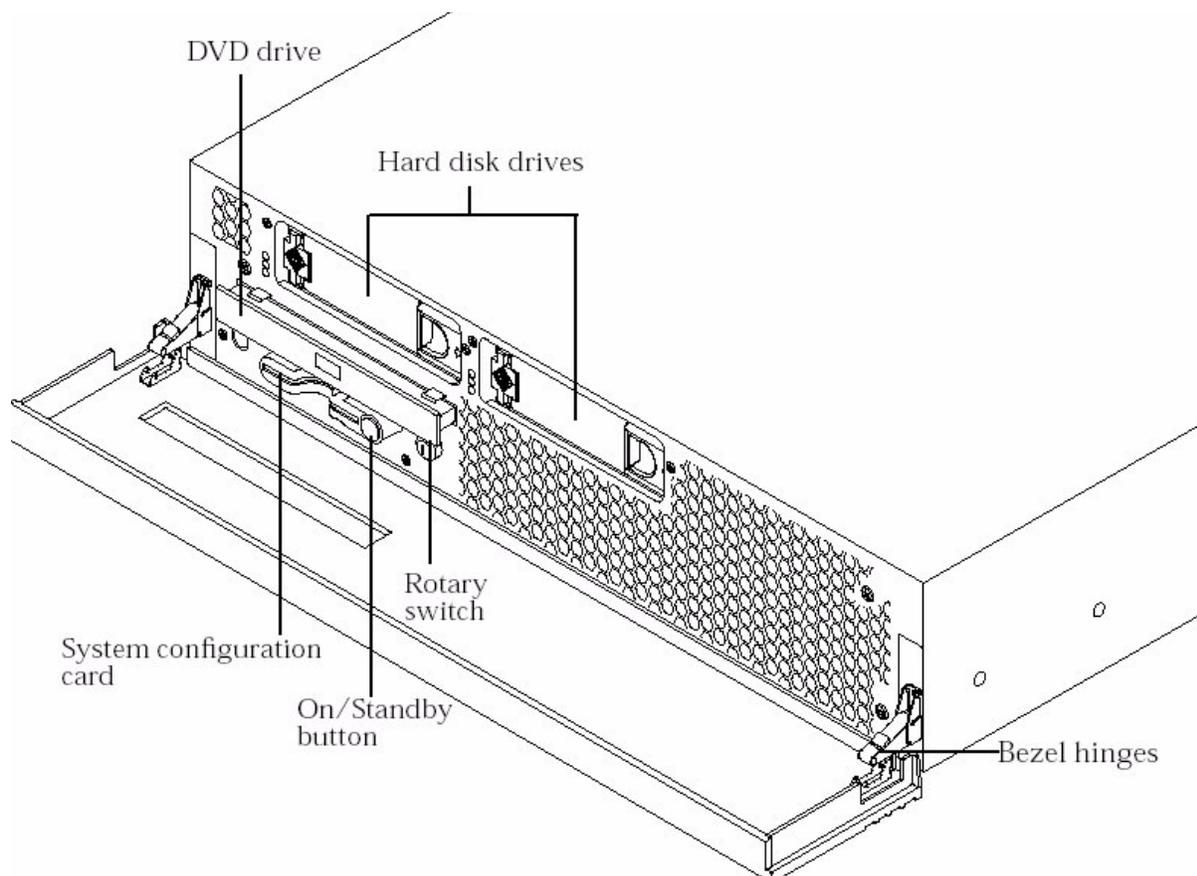
Application

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 SPFS-based server on page 196](#) 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.

If you are replacing the DVD drive on the	Do
active server	step 2
inactive server	step 3

- 2 Initiate a manual failover.
- 3 Once the active server acquires the status of standby (inactive), power down the server. Refer to procedure [Shutting down an SPFS-based server on page 196](#) 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.

Viewing customer logs on an SPFS-based server

Application

Use this procedure to view customer logs for the following components:

- Carrier Voice Over IP Element and Sub-element Manager (ESM)
- Gateway Controller (GWC)
- Media Gateway 9000 (MG 9000)
- Carrier VoIP Server Platform Foundation Software (SPFS)

Customer logs reside in directory `/var/log` on the server. For details on customer logs, refer to the Carrier Voice over IP 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 SPFS-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 only
view specific content of a log file	substep b 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.