Carrier VoIP

Core and Billing Manager 850 Fault Management

NN10351-911

Document status: Standard
Document version: 04.04
Document date: 20 October 2006

The information in this document is sourced in Canada, the United States of America, and the United Kingdom.

Contents

Core and Billing Manager 850 Fault Management

New in this release for Core and Billing Manager 850 Fault Management in SN09U

The following sections detail what's new in the Core and Billing Manager 850 Fault Management document for this release:

- "Features" (page 7)
- "Other changes" (page 8)

Features

The following feature-related changes have been made in the documentation:

- With the addition of new role groups, the CBM user group improvements feature allows you to perform CBM maintenance procedures without having to be the root user. The CBM user group improvements feature required changes to the procedures that require new authorization level and access:
  - addition of a statement in the prerequisites section indicating the authorization level required to complete the procedure
  - if non-restricted shell access is required to complete the procedure, addition of a statement in the prerequisites section indicating that non-restricted shell access is required
  - addition of a table in the prerequisites section listing procedures relating to authorization level and access
- The passphrase protected keys for SSH feature required the addition of log SDM666.
- The record count log support in SBA feature required the modification of log SDMB655.

Other changes

Removed the procedure, Changing a user password on an SPFS-based server.

Fault Management Strategy

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

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

CAUTION

Do not attempt to RTS failed hardware.

If you experience any core manager hardware failure, do not attempt to return this hardware to service (RTS). Replace the failed hardware with an available spare as soon as possible. Contact your next level of technical support for further analysis and instructions as necessary.

Alarms

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

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

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

Logs

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

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

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

A list of the CBM 850 logs can be found in "CBM 850 logs" (page 19).

SDM/CBM logs matrix for SDM logs

Log	SDM	CBM	Comments
SDM300	X		
SDM301	X		
SDM302	X		
SDM303	X	X	
SDM304	X	X	
SDM306	X	X	
SDM308	X		
SDM309	X		
SDM314	X		
SDM315	X	X	
SDM317	X		
SDM318	X	X	
SDM325	X	X	Specific to P-MSC.
SDM330		X	
SDM331	X	X	
SDM333	X	X	
SDM336		X	
SDM375	X	X	
SDM500	X		
SDM501	X		
SDM502	X		
SDM503	X		

Log	SDM	CBM	Comments
SDM504	X		
SDM505	X		
SDM550	X	X	Generated on MTX.
SDM600	X		
SDM601	X		
SDM602	X		
SDM603	X	X	
SDM604	X	X	
SDM608	X		
SDM609	X		
SDM614	X		
SDM615	X		
SDM616	X		
SDM617	X		
SDM618	X		
SDM619	X	X	
SDM620	X		
SDM621	X		
SDM622	X	X	
SDM625		X	Specific to P-MSC.
SDM630	X		
SDM632	X		
SDM636		X	Introduced in SN07.
SDM650	X	X	Generated in MTX.
SDM700	X	X	
SDM739	X		New in SDM20 (MTX13)
SDMO375	X	X	
SPFS310		X	
SPFS320		X	
SPFS330		X	

Log	SDM	CBM	Comments
SPFS350		X	
SPFS400		X	

SDM/CBM logs matrix for SBA logs

SBA Log	SDM	CBM	Comments
SDMB300	X	X	
SDMB310	X	X	
SDMB315	X	X	
SDMB316	X	X	
SDMB320	X	X	
SDMB321	X	X	
SDMB330	X	X	
SDMB350	X	X	
SDMB355	X	X	
SDMB360	X	X	
SDMB365	X	X	
SDMB366	X	X	
SDMB367	X	X	
SDMB370	X	X	Not applicable to CDMA.
SDMB375	X	X	
SDMB380	X	X	
SDMB390	X	X	
SDMB400	X	X	
SDMB530	X	X	
SDMB531	X	X	
SDMB550	X	X	
SDMB600	X	X	
SDMB610	X	X	
SDMB615	X	X	
SDMB620	X	X	
SDMB621	X	X	
SDMB625	X	X	
SDMB650	X	X	
SDMB655	X	X	

SBA Log	SDM	CBM	Comments
SDMB660	X	X	
SDMB665	X	X	Not applicable to CDMA.
SDMB670	X	X	Not applicable to CDMA.
SDMB675	X	X	
SDMB680	X	X	
SDMB820	X	X	
SDMB690	X	X	Introduced in SN07.
SDMB691	X	X	Introduced in SN07.

Fault clearing procedures

The basic strategy for clearing CBM 850 faults is outlined in "Strategy for clearing a CBM 850 fault condition" (page 27).

Tools and utilities

The Succession Platform Foundation Services (SPFS) consists of the Sun hardware, Solaris operating system, third party software, and Nortel platform code. CBM is one of the Nortel products deployed on the Nortel SPFS platform. This document focuses on CBM product maintenance, which is performed through the CBM maintenance interface (CBMMTC) tool and commands. Maintenance for the SPFS platform is performed through a suite of common SPFS commands and 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 follows.

Sample CBMMTC screen

```
CBM         MATE    NET     APPL    SYS      HW    CLLI: OTT3
ISTb          -       .       .     ISTb     .     Host: ucars0033c-unit0
 M          M       M       m       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  13:52  >
```

The alarm banner categories include:

- CBM - status the CBM
- MATE - status of the mate of the active CBM in a CBM 850 cluster
- NET - network status

- APPL - CBM application status
- SYS - system status
- HW - hardware status

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

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 following table.

Alarm Indicator	Description
	cleared
w	warning
m	minor
M	major
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 850 runs. The platform provides the basic resources necessary for the CBM 850 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 (cloning)

CBM 850 maintenance procedures

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

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

Log Delivery procedures

If you want to	Use procedure
access log devices from a remote location	"Accessing TCP and TCP-IN log devices from a remote location" in the Fault Management section
add a TCP, TCP-IN, or file device	"Configuring a CBM for log delivery" in the Configuration Management document
modify parameters for an existing device	"Modifying a log device using logroute" in the Configuration Management document
specify logs to be delivered to a specific device	• for a new device, use "Configuring a CBM for log delivery" in the Configuration Management document • for an existing device, use "Modifying a log device using logroute" in the Configuration Management document
delete a log device	"Deleting a device using logroute" in the Configuration Management document

If you want to	Use procedure
define the set of logs sent from the CM	"Specifying the logs delivered from the CM to the CBM" in the Configuration Management document
change the log delivery global parameters (applicable to all devices)	"Configuring the Log Delivery global parameters" in the Configuration Management document
configure the Generic Data Delivery (GDD) parameter	"Configuring GDD parameter using logroute" in the Configuration Management document
display log records	Retrieving and viewing log records
install log delivery service	"Installing the Log Delivery application" in the Configuration Management document
install the logreceiver tool	"Installing the logreceiver tool on a client workstation" in the Configuration Management document
view logs	Retrieving and viewing log records
store logs in a file	Retrieving and viewing log records
troubleshoot log delivery problems	Troubleshooting Log Delivery problems on a CBM

CBM 850 application fault clearing procedures

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

CBM 850 application
"Strategy for clearing a CBM 850 fault condition" (page 27)
Clearing a minor or major or critical CBM 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 it is not apparent from the alarm or log which specific SBA fault clearing procedure to use, refer to the generic procedure SBA alarm troubleshooting.

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
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

SuperNode Billing Application (SBA)
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
"Clearing a major Heartbeat alarm" (page 43)
Replacing a failed power supply
"Replacing a failed CBM" (page 50)
Replacing failed Ethernet interfaces
Accessing TCP and TCP-IN log devices from a remote location
"Accessing the MATE" (page 86)
"Clearing the MATE alarm" (page 88)
Replacing one or more failed disk drives on an 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
Initiating a manual failover on a Sun Netra 240 server pair

CBM 850 logs

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

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

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

SDM logs

Log	Trigger	Action
SDM303	A core manager application or process has failed more than three times in a day, or has declared itself to be in trouble.	Users with root permissions can examine the log files in /usr/adm to determine the cause of the process failure. If required, contact your next level of support for assistance.
SDM304	The Log Delivery application cannot deliver logs to the specified UNIX file.	Use the Log Delivery online commissioning tool (logroute) to verify the existence and validity of the device name. Refer to the following procedures for more information: • "Configuring a core manager for log delivery" in the Configuration Management document • "Deleting a device using logroute" in the Configuration Management document If required, contact your next level of support for assistance.

Log	Trigger	Action
SDM306	The Table Access Service application on the core manager has detected that the software load on the Core is incompatible with the software load on the core manager.	Upgrade the CM software to a version that is compatible with the SDM software. The software on the core manager must not be at a lower release level than the software on the Core.
SDM315	The Table Access Service application on the core manager has detected corruption in the Data Dictionary on the Core.	Contact your next level of support with the information provided in the log. The log information contains essential information for identifying the Data Dictionary type that is corrupt.
SDM318	An operational measurements (OM) report was not generated. (The OM report failed to complete within one report interval.)	Contact your next level of support.
SDM325	Indicates a lost connection to a Preside network management component.	No action required.
SDM330	Indicates a communication problem between two mated nodes on a CBM850 HA cluster	Use the description field to determine necessary action.
SDM331	OMDD audit deleted files from the OMDD storage volume to free up space.	No action required.
SDM336	No heartbeat response received	Use the logs command from the hw level of the cbmmtc display to check for Ethernet link faults on the CBM. Check on core mapci;mtc;xac level for Ethernet connectivity faults.
SDM338	Audit finds that omdata file system usage exceeds 60% or 80%.	No action required.
SDM375	OMDD discovered a problem while performing outbound file transfer and could not ensure that the OM report got transferred downstream.	Contact your next level of support.
SDM603	A fault on a core manager application or process has cleared.	No action required.

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 *SuperNode Data Manager Log Report Reference Manual*, 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.
SDM619	The OM Access Server has detected a corrupt OM Group during an OM Schema download.	No action required.
SDM622	The SDM log delivery application generates this log when the file device reaches its maximum size.	Check if you have configured enough space for the file device. If there is a software error causing the increase of logs, contact your next level of support for help.
SDM625	Indicates a re-established connection to a Preside network management component.	No action required.
SDM631	Indicates that Audit has deleted a file in the closedNotSent directory to make more than 80% available space in the omdata file system.	No action required.
SDM636	Heartbeat alarm cleared	No action required.
SDM638	Issued when Audit finds that omdata file system usage has gone below 80% or 60%.	No action required.
SDM639	Issued when Audit finds that omdata file system usage exceeds 90%.	Audit deletes all of the OM files in the closedSent directory.
SDM666	Issued if there is a failure in generating the cryptographic keys.	No action required.
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.

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 between the core and the CBM800.	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	One of the following billing processes on the CM has been manually killed: • BUFAUDI • BUFAUDIT • BUFCABKI • BUFDEVP • BUFPROC • BUFRECI • SBCPROCI • SBMTSTRI	Restart the process.
SDMB320	A billing backup-related problem occurred, which affects more than one file.	Ensure that the backup volumes configured for the stream have enough available space.
SDMB321	A billing backup-related problem occurred, which affects one file.	Ensure that the backup volume is not busy or full.
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.

Log	Trigger	Action
SDMB355	A problem with a billing disk has occurred, which can consist of any one of the following problems: • 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	• 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	SBA has lost the connection to the Persistent Store System (PSS) and cannot restore it. When this occurs alarm SBAIF is raised.	Contact your next level of support.
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.

Log	Trigger	Action
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.
SDMB375	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: 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.	Contact your next level of support if log indicates any one of the following errors: • 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

Log	Trigger	Action
		• DPMS FTP service not available • DPMS FTP connection closed • requested file action not taken: <command>. File unavailable Verify FTP if the log indicates any one of the following errors: • not logged in while executing command: <command> • unable to exec FTP process
SDMB380	The file transfer mode for the specified stream has an invalid value	Set the file transfer mode to either Inbound or Outbound.
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.

Log	Trigger	Action
SDMB655	• 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. When the billing file is rotated/moved from open to closedNotSent on the core manager the record count will increase.	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 generated 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.
SDMB691	Identifies events related to the scheduled transfer of billing files.	For the version of this alarm that displays the message, "Unable to initialize file transfer schedule for stream <stream>", make sure the system is free of faults. When the system is free of faults, the SBA will resume the scheduled transfer of billing files.
SDMB820	Minimal backup space is available.	Increase the size of backup volumes.

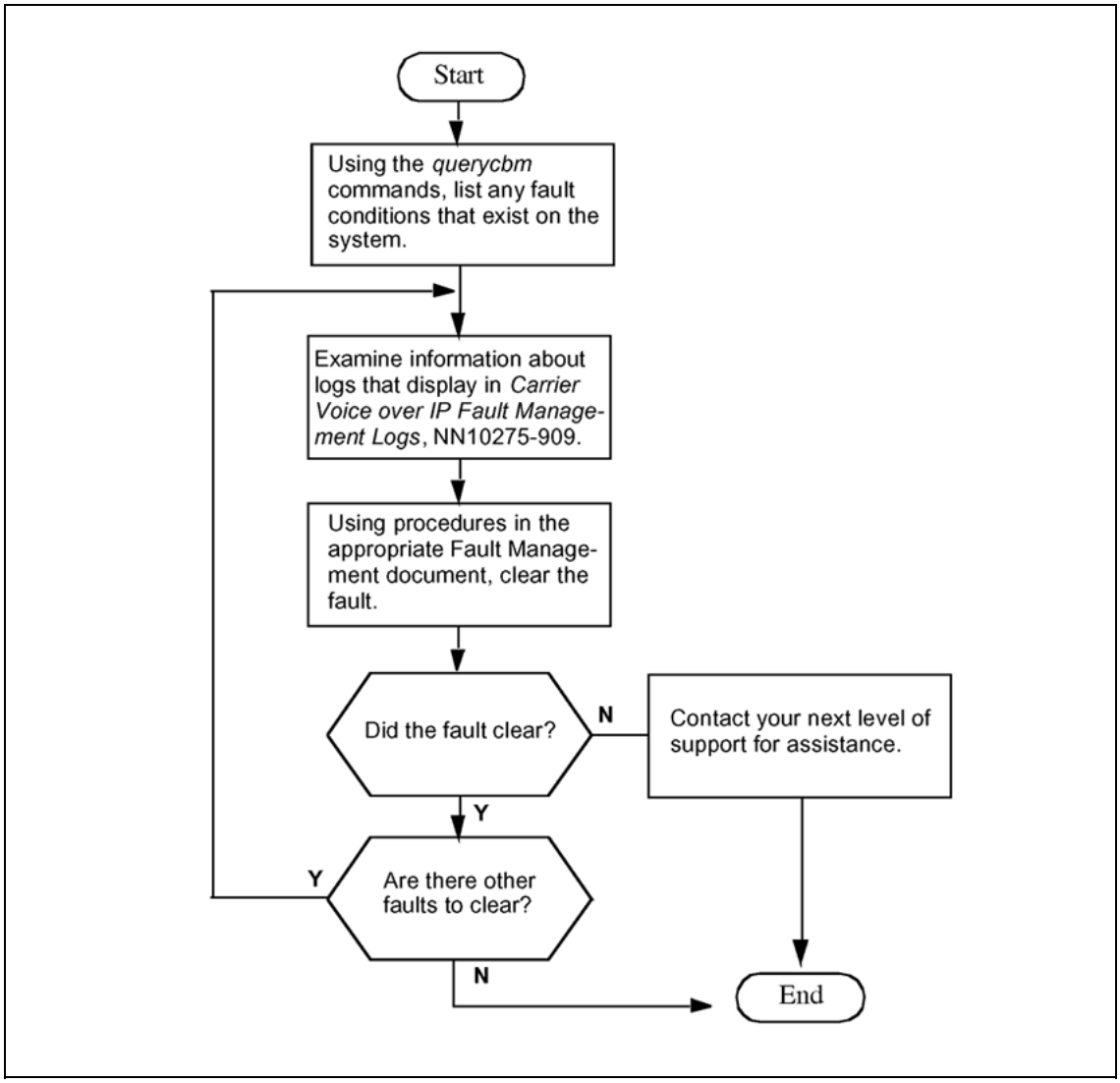
Strategy for clearing a CBM 850 fault condition

This section does not apply to CDMA/GSM and it will not appear in the Preliminary release.

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

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

Basic task flow for clearing faults on the CBM 850



Prerequisites

All users are authorized to perform this procedure.

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

Procedure	Document
Logging in to the CBM	*Core and Billing Manager 850 Security and Administration*, NN10358-611
Displaying actions a role group is authorized to perform	*Core and Billing Manager 850 Security and Administration*, NN10358-611

Procedure

Strategy for clearing a CBM 850 fault condition

Step	Action

At your CBM 850

1 Log into the active unit of the CBM 850, and list any fault conditions that exist on the system:

```
querycbm flt
```

If the alarm is in cbmmtc under the MATE column of the banner (the state is not a dot [.]), enter the following command:

```
querycbm mate
```

2 Log into the core manager and list any fault conditions that exist on the system:

```
querycbm flt
```

If the alarm is in cbmmtc under the MATE column of the banner (the state is not a dot [.]), enter the following command:

```
querycbm mate
```

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

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

Fault type	log number	Description
Platform related	SPFSxx	Specific to the platform, such as a hardware fault or resource exceeded threshold
Mate		Application or platform related fault condition.

4 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.

5 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
Communication problem with the Core (SDM336)	Refer to "Clearing a major Heartbeat alarm" (page 43)
Network Time Protocol problem (SDM327)	First verify with your system administrator that the NTP server is not in a fault condition. If the fault condition is not in the NTP server and can be isolated to the CBM 850, contact your next level of support for assistance.
Application problem (SDM 303)	Clearing a minor or major or critical CBM alarm
SBA related (SDMBxx)	Refer to SuperNode Billing Application (SBA) fault clearing procedures
Mate related	Refer to "Clearing the MATE alarm" (page 88)
SDM330	First verify that the mate unit is not in an alarm condition. If it is not, contact your next level of support.

6 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 7
the fault has not cleared	Contact your next level of support for assistance

7 Check to see if all fault conditions have now cleared:

```
querycbm flt
querycbm mate
```

Note: It may take up to five minutes for a fault indication to clear after a fault is cleared.

If	Do
any fault conditions still exist	step 4
no fault conditions exist	step 8

8 You have completed this procedure.

—End—

Clearing a minor or major or critical CBM alarm

Application

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

Indication

An alarm indication is displayed on the Office Alarm Unit or the INMS Alarm Management System. These alarms generate logs which can be monitored at the client output device. These alarms are also displayed on the APPL;SDM level of the MAPCI.

Meaning

This indicates that there are one or more alarms reported by the CBM.

Impact

If the CBM status at the MTC level of the CBMMTC display does not show InSv, then one or more of the following conditions exist:

- one or more CBM applications have failed.
- CBM application 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.

If all CBM applications fail, the CBM appl state is system busy (SysB). The system generates a minor alarm .

Prerequisites

All users are authorized to perform this procedure.

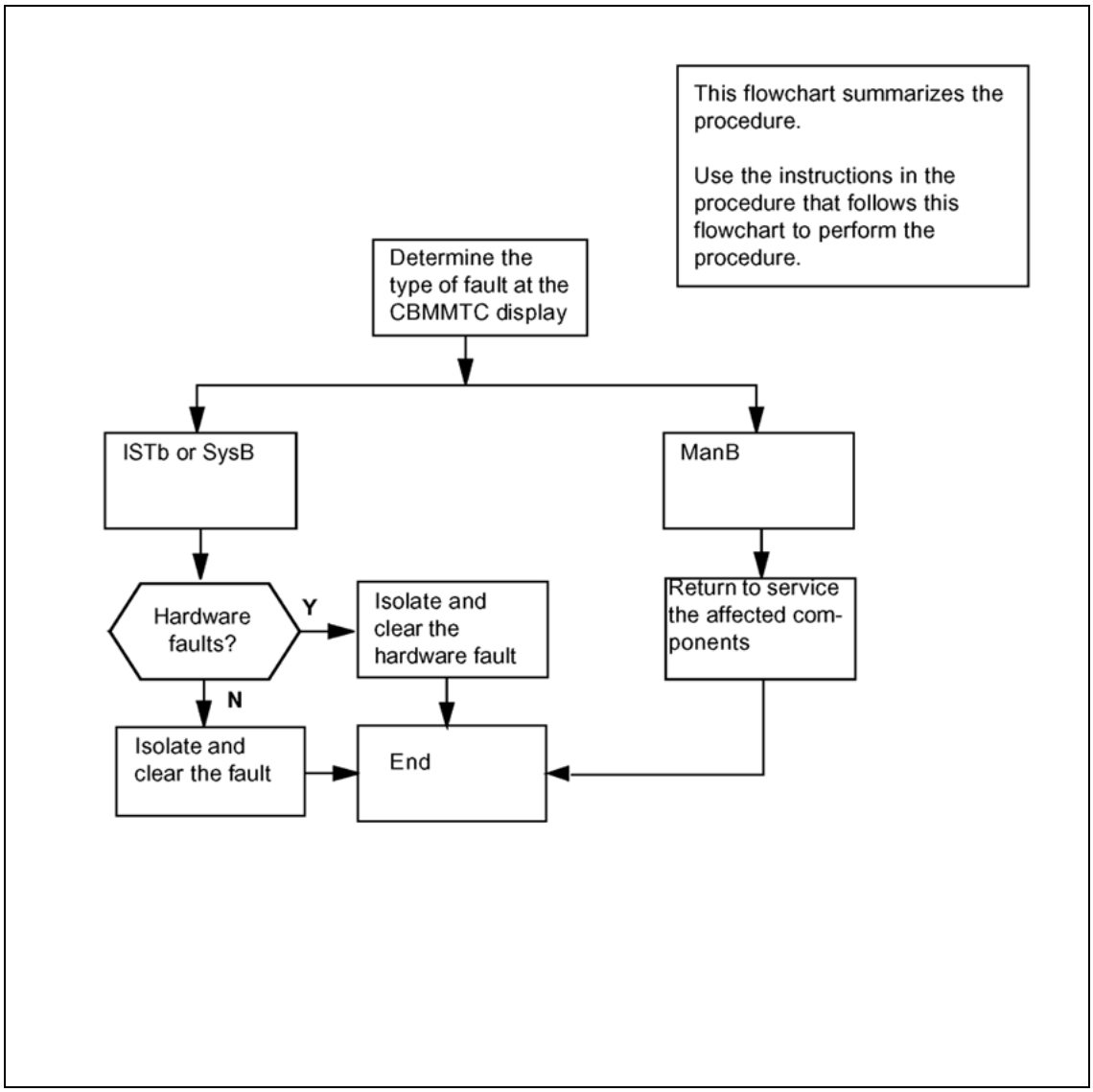
For information on how to log in to the CBM as an authorized user or how to display information about a user or role group, review the procedures in the following table.

Procedure	Document
Logging in to the CBM	*Core and Billing Manager 850 Security and Administration*, NN10358-611
Displaying actions a role group is authorized to perform	*Core and Billing Manager 850 Security and Administration*, NN10358-611

Action

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

Summary of clearing a minor or major or critical CBM alarm



Clearing a minor or major or critical CBM alarm

Step	Action

At the local or remote VT100 terminal

1 Log into the core manager, and obtain fault status information

```
> querycbm flt
```

2 Use the following table 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.
Platform related	SPFSxx	Specific to the platform, such as a hardware fault or resource exceeded threshold

3 Proceed according to the type of fault.

If the fault is	Do
Platform related (SPFSxxx) problem	step 4
Communication problem with the Core (SDM314, SDM 334, SDM335)	Refer to "Clearing a major or minor or critical APPL;SDM alarm"
Network Time Protocol problem	have your system administrator isolate and clear the problem.
Application problem (SDM 303)	step 14

4 If the fault indicates that the logical volume is exceeded, continue with step 5; otherwise, refer to the appropriate SPFS procedure to clear the alarm.

CAUTION
Potential service interruption
A logical volume on the CBM must never reach 100% disk full. The system operation is unpredictable when a logical volume reaches 100% disk full. If a logical volume exceeds its alarm threshold, contact your system administrator. The system administrator must assess the current condition of the logical volume and take appropriate action immediately. If required, contact Nortel for assistance.

5 If the GDD logical volume is exceeded, continue with step 6; otherwise, refer to the appropriate SPFS procedure to increase the size of a logical volume.

6 There are two choices when the GDD logical volume 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.
Decrease the number of days to retain logs	step 7

7 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 ==>
```

8 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 ==>
```

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

```
Enter Option ==> 1
```

10 Enter the number of days to retain the log files:

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

11 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
```

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

13 Go to step 23.

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

```
# cbmmtc
```

15 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
```

16 Determine the affected application from the display and note its key number, shown under the header "#".

17 Proceed depending on the state of the application.

If the state is	Do
ManB	step 18
ISTb	step 19
SysB	step 20
Fail	step 21

18 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...
```

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 24
the application does not return to service	step 17

19 This state can result from a recent change of state, or if this application is dependent on another application that has not completed initialization.

- if you suspect either situation to be true, wait 10 minutes for the applications to complete initializing.

- if you do not suspect either situation to be true, use the value in the reason field to resolve the problem.

If you	Do
can resolve this problem	step 24
cannot resolve this problem	Contact your next level of support.

20 Use the reason given to resolve this problem.

If you	Do
can resolve this problem	step 24
cannot resolve this problem	Contact your next level of support.

21 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 maintenance interface, 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...
```

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

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

22 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...
```

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

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

23 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 documents specific to the application
changes to InSv state	go to step 24

24 Obtain the fault status information from the CBM:

```
> querycbm flt
```

If	Do
more faults are reported	step 2
all faults are cleared	you have completed this procedure.

—End—

Clearing a GDD logical volume size threshold violation

Application

The GDD application stores the formatted logs from the Core on the CBM for a period of 1 to 30 days for use with the CBM tool logquery (which is similar to using logutil;open/back on the Core). Refer to procedure 'Retrieving and viewing log records'. By default, 7 days of storage is preselected. These logs are stored in the /cbmdata/00/gdd file system as files that are rotated twice daily at midnight and noon. Files dated beyond the number of days are deleted automatically by GDD.

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.

Prerequisites

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

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

Step	Action
	At the local or remote VT100 terminal
1	There are four choices when the GDD logical volume size threshold is exceeded: • increase the size of the logical volume • decrease the number of days to keep the logs • reduce the quantity of logs generated by the core

- ensure that only GDD-related files are in the /cbmdata/00/gdd fs

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 253
Decrease the number of days to retain logs	step 2

2 Log in to the active unit of 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
/cbmdata/00/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 /cbmdata/00/gdd:

```
Enter Option ==> 1
```

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

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

The default value is 7 days.

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
logs in /cbmdata/00/gdd.  Log files 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.

—End—

Clearing a major Heartbeat alarm

Application

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

Indication

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

Meaning

The CBM is not receiving responses from the Core. Each CBM unit commences periodic 'heartbeat' messages to the Core once the Core IP is commissioned. The heartbeat message is always sent from the physical IP of the CBM (i.e. not the logical cluster IP for the active unit). The Core learns the CBM cluster IP from the data in heartbeat message, and two way heartbeat communication is established between the Core and that CBM unit.

Active unit loss of heartbeat to the Core never initiates a Swact in either SINGLE LAN or DUAL LAN.

Impact

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

If	Go To
This is a single LAN	"Clearing a major Heartbeat alarm on a single LAN" (page 43)
This is a dual LAN	"Clearing a major Heartbeat alarm on a dual LAN" (page 46)

Action

Clearing a major Heartbeat alarm on a single LAN

Step	Action
	At the CBM
1	Log into each CBM unit on the console as a user authorized to perform fault-admin actions.

2 Verify that the CBM Ethernet uplink0 interfaces are in service. Type: 'querycbm flt' and look for presence of SPFS alarms. If SPFS 310 alarms exist, clear these first.

3 Type 'corecon' on each unit.

—End—

Use "Fault Clearing Actions on a Single Lan" (page 44) to determine the appropriate action to take.

Fault Clearing Actions on a Single Lan

If	Impact	Action
Active unit has heartbeat alarm, Inactive does not	Automatic cluster failover occurs.	Do not manually SWACT. Investigate and resolve the problem on the OAM Lan as indicated by 'querycbm flt'. • perform traceroute, using physical IP, should show 2 hops `traceroute -i uplink0 -s <CBM physical IP-I cm` • perform a manual SWACT • Investigate and resolve the problem on newly inactive unit • ensure inactive CBM unit has the correct Core IP in /etc/hosts • ensure mask as shown with ifconfig -uplink0 aligns with mask in table IPNETWRK • ascertain path using ICMP 'ping -s ' command from inactive CBM unit to Core. • ensure Layer 2 Ethernet switch is configured correctly, especially for. VLAN and ports for CBM and Core • ensure no firewall/access restrictions exist between Core and inactive CBM physical IP

If	Impact	Action
Inactive unit has heartbeat alarm, Active does not	Cannot manually SWACT (disabled).	Do not manually SWACT. Investigate and resolve the problem on the OAM/CALLP LAN as indicated by 'querycbm flt'. • ensure inactive CBM unit has the correct Core IP in /etc/hosts • ensure mask as shown with ifconfig -uplink0 aligns with mask in table IPNETWRK • ascertain path using ICMP 'ping -s ' command from inactive CBM unit to Core. • ensure Layer 2 Ethernet switch is configured correctly, especially for. VLAN and ports for CBM and Core • ensure no firewall/access restrictions exist between Core and inactive CBM physical IP
Both Active and Inactive units have heartbeat alarm	Cannot manually swact (disabled)	Investigate and resolve the problem on the OAM/CALLP LAN as indicated by 'querycbm flt'. • ensure Core is INSV and datafilled correctly in table IPNETWRK and IPHOST and mask • ensure all restrictions on Core IP selection have been observed • ensure each CBM unit has the correct Core IP in /etc/hosts • ensure mask as shown with ifconfig -uplink0 aligns with mask in table IPNETWRK • ascertain path using ICMP 'ping -s ' command from each CBM unit to Core. active unit will ping from cluster IP, not physical IP • ensure Layer 2 Ethernet switch is configured correctly, especially for. VLAN and ports for CBM and Core • ensure no firewall/access restrictions exist between Core and inactive CBM physical IP

Action

Clearing a major Heartbeat alarm on a dual LAN

Step	Action
	At the CBM
1	Log into each CBM unit on the console as a user authorized to perform fault-admin actions.
2	Verify that the CBM Ethernet uplink0 interfaces are in service. Type: 'querycbm flt' and look for presence of SPFS alarms. If SPFS 310 alarms exist, clear these first.
3	Type 'corecon' on each unit.
	—End—

Use "Fault Clearing Actions on a Dual Lan" (page 46) to determine the appropriate action to take.

Fault Clearing Actions on a Dual Lan

If	Impact	Action
Active unit has heartbeat alarm, Inactive does not	Automatic cluster failover occurs.	Do not manually SWACT. Investigate and resolve the problem on the OAM Lan as indicated by 'querycbm flt'. • perform traceroute, using physical IP, should show 2 hops `traceroute -i uplink0 -s <CBM physical IP-I cm` • perform a manual SWACT • Investigate and resolve the problem on newly inactive unit • ensure inactive CBM unit has the correct Core IP in /etc/hosts • ensure mask as shown with ifconfig -uplink0 aligns with mask in table IPNETWRK • ascertain path using ICMP 'ping -s ' command from inactive CBM unit to Core. • ensure Layer 2 Ethernet switch is configured correctly, especially for. VLAN and ports for CBM and Core

If	Impact	Action
		• ensure no firewall/access restrictions exist between Core and inactive CBM physical IP
Inactive unit has heartbeat alarm, Active does not	Cannot manually SWACT (disabled).	Do not manually SWACT. Investigate and resolve the problem on the OAM/CALLP LAN as indicated by 'querycbm flt'. • ensure inactive CBM unit has the correct Core IP in /etc/hosts • ensure mask as shown with ifconfig -uplink0 aligns with mask in table IPNETWRK • ascertain path using ICMP 'ping -s ' command from inactive CBM unit to Core. • ensure Layer 2 Ethernet switch is configured correctly, especially for. VLAN and ports for CBM and Core • ensure no firewall/access restrictions exist between Core and inactive CBM physical IP
Both Active and Inactive units have heartbeat alarm	Cannot manually swact (disabled)	Investigate and resolve the problem on the OAM/CALLP LAN as indicated by 'querycbm flt'. • ensure Core is INSV and datafilled correctly in table IPNETWRK and IPHOST and mask • ensure all restrictions on Core IP selection have been observed • ensure each CBM unit has the correct Core IP in /etc/hosts • ensure mask as shown with ifconfig -uplink0 aligns with mask in table IPNETWRK • ascertain path using ICMP 'ping -s ' command from each CBM unit to Core. active unit will ping from cluster IP, not physical IP • ensure Layer 2 Ethernet switch is configured correctly, especially for. VLAN and ports for CBM and Core • ensure no firewall/access restrictions exist between Core and inactive CBM physical IP

If	Impact	Action

Replacing a failed power supply

Application

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

Prerequisites

Obtain a spare power supply.

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

Step	Action
1	Refer to the manufacturer documentation for the procedure on how to replace the power supply. Go to www.sun.com, click the Documentation tab, and enter **Netra 240 Server Service Manual** in the Search field.
2	You have completed this procedure.

—End—

Replacing a failed CBM

Purpose

Use the following procedures to replace a failed CBM.

Application

The CBM is not a field replaceable unit. The server must be powered down before hardware can be removed from the shelf.

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.

Prerequisites

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

Prerequisites for Core and Billing Manager 850

In order to perform this procedure, you must have the following authorization and access:

- You must be a user in a role group authorized to perform fault-admin actions.
- You must obtain non-restricted shell access.

For more information about how to log in to the CBM as an authorized user, how to request a non-restricted shell access, or how to display actions a role group is authorized to perform, review the procedures in the following table.

Related procedures

Procedure	Document
Logging in to the CBM	*Core and Billing Manager 850 Security and Administration*, NN10358-611
Requesting non-restricted shell access	*Core and Billing Manager 850 Security and Administration*, NN10358-611
Displaying actions a role group is authorized to perform	*Core and Billing Manager 850 Security and Administration*, NN10358-611

Action

Replacing failed CBM

Step	Action

At the shelf

1 Record the stream_name for the stream you wish to busy as determined in the procedure "Preparing for SBA installation and configuration" in the *Accounting* NTP for your core manager.

2 If the server is still powered up, perform the procedure "Shutting down an SPFS-based server" in *ATM/IP Solution-level Security and Administration*, NN10403-900. Otherwise, go to step 3.

3 Remove and replace the CBM server by following instructions provided by the hardware manufacturer.

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

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

At the CBM

5 Log in to the core manager.

6 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
```

7 Proceed depending on the state of the application. If the applications you want to RTS are in the Offline state, go to step 8; otherwise, go to step 10.

8 Manually busy all the applications by entering:

```
bsy group
```

9 Confirm the BUSY operation:

```
y
```

10 Proceed depending on the state of the application. If the applications you want to RTS are in the Offline state, go to step 11; otherwise, go to step 12.

11 Manually busy all the applications which are in the Offl state:

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

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

Do not apply the Bsy command to the applications you do not want to RTS.

12 If the CBM group state is in ManB state, go to step 13; otherwise, go to step 14.

13 RTS all the applications which are in the ManB state by typing:

```
rts group
```

Go to step 15.

14 RTS each application by typing:

```
rts <application number 1><application number 2><....>
```

15 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.

Rcvy indicates that the stream is in-service and also sending previously created backup files to the CS2000 Core Manager.

The state may also be InSv, which indicates that the stream is in a normal working state if recovery has already completed.

16 Clear any application and system alarms if they are present.

17 You have completed this procedure.

—End—

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.

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.

Prerequisites

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

You must have a replacement N240 server with the same PEC code as that which is being replaced.

Prerequisites for Core and Billing Manager 850

In order to perform this procedure, you must have the following authorization and access:

- You must be a user in a role group authorized to perform fault-admin actions.
- You must obtain non-restricted shell access.

  Note: You require root user access to perform a swact in step 30 if the failed ethernet interface is on the ACTIVE node of the CBM 850 clustered pair.

For more information about how to log in to the CBM as an authorized user, how to request a non-restricted shell access, or how to display actions a role group is authorized to perform, review the procedures in the following table.

Related procedures

Procedure	Document
Logging in to the CBM	*Core and Billing Manager 850 Security and Administration*, NN10358-611

Procedure	Document
Requesting non-restricted shell access	*Core and Billing Manager 850 Security and Administration*, NN10358-611
Displaying actions a role group is authorized to perform	*Core and Billing Manager 850 Security and Administration*, NN10358-611

Action

Replacing failed Ethernet interfaces

Step	Action

At the MAP interface on the CM

1 If you are performing this procedure on a CBM800, go to step 2. If you are performing this procedure on a CBM850, go to step 28.

2 Record the stream_name for the stream you wish to busy as determined in the procedure "Preparing for SBA installation and configuration" in the *Accounting* NTP for your core manager.

3 Access the SDMBIL level:

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

where

<stream_name> is the stream name value determined in step 2.

4 Busy the stream at the SDMBIL level by typing:

```
bsy
```

5 Proceed with busying the stream by typing:

```
y
```

6 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 2.

7 Follow the procedure "Sending billing files from disk" in the *Accounting* NTP for your core manager.

At the CBM

8 Log in to the core manager.

9 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
```

10 Manually busy all the applications by entering:

```
bsy group
```

11 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")
```

12 Offline each application by entering:

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

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

13 Offline the CBM group by entering:

```
offl group
```

At the shelf

14 Follow the procedure "Shutting down an SPFS-based server" in *ATM/IP Solution-level Security and Administration*, NN10403-900.

15 Remove and replace the CBM server .

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

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

At the CBM

17 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
```

18 Proceed depending on the state of the application. If the CBM group state is Offl go to step 19; otherwise, go to step 21.

19 Manually busy all the applications by entering:

```
bsy group
```

20 Confirm the BUSY operation:

```
y
```

21 Proceed depending on the state of the application. If the applications you want to RTS are in the Offline state, go to step 22; otherwise, go to step 23.

22 Manually busy all the applications which are in the Offl state:

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

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

Do not apply the Bsy command to the applications you do not want to RTS.

23 If the CBM group state is in ManB state, go to step 24; otherwise, go to step 25.

24 RTS all the applications which are in the ManB state by typing:

```
rts group
```

Go to step 26.

25 RTS each application by typing:

```
rts <application number 1><application number 2><....>
```

26 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 2.

Rcvy indicates that the stream is in-service and also sending previously created backup files to the CS2000 Core Manager.

The state may also be InSv, which indicates that the stream is in a normal working state if recovery has already completed.

27 Clear any application and system alarms if they are present.

28 Log in to the failed unit using the console port.

29 Determine the cluster activity of the failed unit by typing:

```
ubmstat
```

30 If the activity indicates ClusterIndicatorACT, make this unit the inactive unit by typing:

```
swact
```

31 Shut down the failed unit by typing:

```
init 0
```

32 You have completed this procedure.

—End—

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 must have a replacement server.

ATTENTION

Ensure that no provisioning activities are in progress, or scheduled to take place during this procedure.

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

Prerequisites for Core and Billing Manager 850

In order to perform this procedure, you must have the following authorization and access:

- You must be a user in a role group authorized to perform fault-admin actions.
- You must obtain non-restricted shell access.

For more information about how to log in to the CBM as an authorized user, how to request a non-restricted shell access, or how to display actions a role group is authorized to perform, review the procedures in the following table.

Related procedures

Procedure	Document
Logging in to the CBM	*Core and Billing Manager 850 Security and Administration*, NN10358-611
Requesting non-restricted shell access	*Core and Billing Manager 850 Security and Administration*, NN10358-611
Displaying actions a role group is authorized to perform	*Core and Billing Manager 850 Security and Administration*, NN10358-611

Action

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

- "Replacing an SPFS-based server (one-server configuration)" (page 59)
- "Replacing one server in an HA configuration" (page 59)
- "Replacing both servers in an HA configuration" (page 60)

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

Step	Action
	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 Routing customer logs to a remote host. Restoring the oracle data does not apply to the CBM as it does not use an oracle database. You have completed this procedure.

—End—

Replacing one server in an HA configuration

Step	Action
	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. If required, refer to procedure Routing customer logs to a remote host.

You have completed this procedure.

—End—

Replacing both servers in an HA configuration

Step	Action

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 Routing customer logs to a remote host.

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. If required, refer to procedure Routing customer logs to a remote host.

You have completed this procedure.

—End—

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 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.

ATTENTION

After performing a full system restore on IEMS you must also perform a subsequent central server restore. Refer to: *Restoring the Central Security Server* in *IEMS Administration and Security*, NN10336-611

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)

Restoring the oracle data is not applicable to the CBM as it does not use an oracle database.

ATTENTION

System logs indicating application and database errors, will be generated until the file systems and oracle data are restored on the system using this procedure and procedure "Restoring the oracle data on an SPFS-based server" (page 221). No database errors will be generated on the CBM as it does not use an oracle database.

Prerequisites

This procedure has the following prerequisites:

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

Action

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

- "Simplex configuration (one server)" (page 62)
- "High-availability configuration (two servers)" (page 64)

Only the is applicable to perform a full system restore from tape on a Sun Netra t1400 server.

Simplex configuration (one server)

Step	Action

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 CD disk#1 into the drive.

4 Use the following table to determine your next step.

If restoring from	Do
tape	step 5
DVD	step 6

5 Insert the tape on which you backed up the 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.

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’, refer to procedure ‘Labelling disks on an SPFS-based server’.

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.

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.

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 backup DVD from the drive.

9 Use the following table to determine your next step.

If the server is hosting	Do
this SPFS-based server is hosting the CBM	step 13
otherwise	step 10

10 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 11

11 Correct the oracle groups by typing

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

and pressing the Enter key.

12 Restore the oracle data using procedure "Restoring the oracle data on an SPFS-based server" (page 221). Once the data restore is complete, execute step 13 of this procedure.

13 Reboot the server by typing

```
# init 6
```

and pressing the Enter key.

14 Ensure the node is active by typing

```
# cd/opt/nortel/sspfs/ha
# ./ActivateNode
```

—End—

High-availability configuration (two servers)

Step	Action

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 Bring the system to the OK prompt by typing

```
# init 0
```

and pressing the Enter key.

5 Insert SPFS DVD 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.

During the restore process, the system will prompt you for additional Volumes if more than one CD or 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.

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:

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.

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 backup CD or DVD from the drive.

10 Use the following table to determine your next step.

If the server is hosting	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 dba data	step 13
oinstall data dba or oinstall dbs data	step 12

12 Correct the oracle groups by typing

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

and pressing the Enter key.

13 Restore the data using procedure "Restoring the oracle data on an SPFS-based server" (page 221). Once the data restore is complete, execute steps 14 and 15 of this procedure.

14 Reboot the server by typing

```
# init 6
```

and pressing the Enter key.

15 Ensure the node is active by typing

```
# cd/opt/nortel/sspfs/ha
```

```
# ./ActivateNode
```

16 Re-image the inactive node using the active node's image. If required, refer to procedure Cloning the image of one node in a cluster to the other node.

You have completed this procedure.

—End—

Cloning the image of one server in a cluster to the other server

Application

Use this procedure to clone the image of the active server in a cluster to the inactive server.

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 and Billing Manager (CBM)

Prerequisites

This procedure has the following prerequisites:

- you need the root user ID and password
- you need console access to the inactive server under the following circumstances
  - — this is the first time you clone
  - — you replaced the inactive server
  - — you executed a reverse restore (that is, you switched unit 0 and 1)

  Under any of the previous circumstances, the inactive server will have a different ethernet address from the one retained in the system. Therefore, console access is required to obtain the ethernet address of the inactive server.

ATTENTION

Ensure that no provisioning activities are in progress, or are scheduled to take place during this procedure.

Prerequisites for Core and Billing Manager 850

In order to perform this procedure, you must have the following authorization and access:

- You must be a user in a role group authorized to perform config-admin actions.
- You must obtain non-restricted shell access.

Note: The root user ID and password are not required in steps 2c, 2d, 3 and 18. The user can use their own ID and execute the procedure.

For more information about how to log in to the CBM as an authorized user, how to request a non-restricted shell access, or how to display actions a role group is authorized to perform, review the procedures in the following table.

Related procedures

Procedure	Document
Logging in to the CBM	*Core and Billing Manager 850 Security and Administration*, NN10358-611
Requesting non-restricted shell access	*Core and Billing Manager 850 Security and Administration*, NN10358-611
Displaying actions a role group is authorized to perform	*Core and Billing Manager 850 Security and Administration*, NN10358-611

Action

Perform the following steps to complete this procedure.

ATTENTION
Perform the steps that follow on the active server.

Step Action

At your workstation

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

If using	Do
telnet (unsecure)	step 2
ssh (secure)	step 3

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 physical IP address of the active server

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.

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 physical IP address of the active server

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.

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.

On the active server

4 Access the command line interface to determine the server profile by typing

```
# cli
```

and pressing the Enter key.

Example response

```
Command Line Interface
1 - View
2 - Configuration
3 - Other
X - exit
select -
```

5 Enter the number next to the View option in the menu.

Example response

```
View
 1 - sspfs_soft (Display Software
     Installation Level Of SPFS)
 2 - chk_sspfs (Check SPFS Processes)
 3 - sw_conf (The software configuration
of       the wrtypyxp)
 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 -
```

6 Enter the number next to the sspfs_soft option in the menu.

Example response

```
=== Executing "sspfs_soft"
SPFS version:  09.0 Build:  200508421 Server
Profile:  cbm850
==="sspfs_soft" completed successfully
```

7 Note the server profile.

8 Exit the CLI by typing **x** until you return to the command prompt.

9 Use the following table to determine your next step.

If	Do
the Server Profile is cbm850	step 16
otherwise	step 10

10 Verify that all applications on the server are running by typing

servquery -status all

and pressing the Enter key.

Example response:

```
APP NAME                        STATUS
========                        ======
SNMP_POLLER                     RUNNING
DELEGATE                        RUNNING
PROP_SRV                        RUNNING
WEBSERVER                       RUNNING
DATABASE                        RUNNING
SAM21EM                         RUNNING
SESMService                     RUNNING
CORBA                           RUNNING
ORA_ARCHIVE_ROTATOR             RUNNING
OMPUSH                          RUNNING
BOOTP                           RUNNING
WEBSERVICES                     RUNNING
ORA_AUTO_BACKUP                 RUNNING
IEMS                            RUNNING
APS                             RUNNING
NPM                             RUNNING
```

11 Use the following table to determine your next step.

If	Do
all applications are running	step 14
otherwise	step 12

12 Start each application that is not running by typing

servstart <app_name>

and pressing the Enter key.

where

app_name is the name of the application that is not in a RUNNING state, for example, SAM21EM

13 Use the following table to determine your next step.

If	Do
all applications started	step 14
otherwise	contact your next level of support

14 Verify the Patching Server Element (PSE) server application is running by typing

pse status

and pressing the Enter key.

If	Do
PSE is running	step 16
otherwise	step 15

15 Start the PSE server application by typing

pse start

and pressing the Enter key.

If	Do
PSE starts	step 16
otherwise	contact your next level of support

16 Use the following table to determine your next step.

If	Do
this is the first time you are cloning the server, or you replaced the server, or you executed a reverse restore (that is, switched unit 0 and unit 1) Under any of the previous circumstances, the inactive server will have a different ethernet address from the one retained in the system. Therefore, console access is required to obtain the ethernet address of the inactive server.	step 17
otherwise	step 21

17 Use the following table to determine your next step.

If	Do
you do not know the Ethernet address of the inactive server	step 18
otherwise	step 19

At the console connected to the inactive server

18 Determine the Ethernet address of the inactive server as follows:

a. Log in to the inactive server through the console (port A) using the root user ID and password.

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. The response must display ClusterIndicatorSTBY, which indicates you are on the inactive server.

b. Bring the system to the OK prompt by typing

init 0

and pressing the Enter key.

c. At the OK prompt, display the Ethernet address of the inactive server by typing

OK **banner**

and pressing the Enter key.

Example response:

```
Sun Fire V240, No keyboard
Copyright 1998-2002 Sun Microsystems, Inc.
All rights reserved.  OpenBoot 4.8.0.build_04,
2048 MB memory installed, Serial #52964131.
Ethernet address 0:3:ba:28:2b:23, Host ID:
83282b23.
```

d. Record the Ethernet address that is displayed.

On the active server

19 Start the cloning process on the active server by typing

startb <Ethernet address>

and press the Enter key.

where

Ethernet address is the Ethernet address of the inactive server

20 Proceed to step 22

On the active server

21 Start the cloning process on the active server by typing

startb

and press the Enter key.

22 Use the following table to determine your next step.

If	Do
the system prompts you to enter the command "boot net - image"	step step 86
otherwise	step 27

23 Connect to the console port of the inactive server.

If the console displays the	Do
login prompt	step 24
OK prompt	step 26

At the console connected to the inactive server

24 Log in to the inactive server using the root user ID and password.

25 Bring the system to the OK prompt by typing

```
# init 0
```

and pressing the Enter key.

26 At the OK prompt, boot the inactive server from the image of the active server by typing

```
OK boot net - image
```

and press the Enter key.

There must be a space between the "-" and "image".

Example response

```
SC Alert: Host System has Reset
Sun Fire V240, No Keyboard
Copyright 1998-2002 Sun Microsystems, Inc.  All
rights reserved. OpenBoot 4.8.0.build_04, 2048
MB memory installed, Serial #52964131. Ethernet
address 0:3:ba:28:2b:23, Host ID: 83282b23.
Rebooting with command: boot net - image
.
.
.
SC Alert: Host System has Reset
```

On the active server

27 Monitor the progress of the cloning from the active server. Cloning the inactive server takes approximately 40 minutes to complete, but the time can vary depending on system configuration.

Example response:

```
Waiting for network response from unit1-priv0...
received network response from unit1-priv0...
Waiting for unit1-priv0 to clone data...
waiting...1
waiting...2
waiting...3
unit1-priv0 is cloning:  /export/d2
.
.
.
Verifying cluster status of unit1-priv0
waiting for cluster filesystem status to become normal.
Jun 27 16:01:38 ucary0883c unix:  /data:  active up
repair - standby reflected (normal)
Deleted snapshot 2.
Deleted snapshot 1.
Deleted snapshot 0.
ucary0883c-unit0(active):/>
```

28 Once cloning is complete, wait approximately 5 minutes before you proceed to the next step.

On the active server

29 Verify the status of replicated disk volumes on the active server by typing

udstat

and pressing the Enter key.

If	Do
all file systems are ACTIVE normal UP clean	step 30
otherwise	contact your next level of support

At your workstation

30 Establish a login session to the inactive server using one of the following methods:

If using	Do
telnet (unsecure)	step 31
ssh (secure)	step 36

31 Log in to the inactive server using telnet (unsecure) by typing

> telnet <server>

and pressing the Enter key.

where

server is the physical IP address of the inactive server in the cluster

32 When prompted, enter your user ID and password.

33 Change to the root user by typing

```
$ su -
```

and pressing the Enter key.

34 When prompted, enter the root password.

35 Proceed to step 41.

36 Log in to the inactive server by typing

```
> ssh -l root <server>
```

and pressing the Enter key.

where

server is the physical IP address of the inactive server in the cluster

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.

37 When prompted, enter the root password.

On the inactive server

38 Verify the status of replicated disk volumes on the inactive server by typing

```
# udstat
```

and pressing the Enter key.

If	Do
all file systems are STANDBY normal UP clean	step 39
otherwise	contact your next level of support

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

—End—

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.

Prerequisites

All users are authorized to perform this procedure.

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

Procedure	Document
Logging in to the CBM	*Core and Billing Manager 850 Security and Administration*, NN10358-611
Displaying actions a role group is authorized to perform	*Core and Billing Manager 850 Security and Administration*, NN10358-611

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" (page 78).

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 "Displaying or storing log records using logreceiver" (page 100)
TCP-IN	Accessing a TCP-IN device from a remote location	"Configuring a core manager for log delivery" in the Configuration Management document

Log device	Procedure	Applies to
		"Deleting a device using logroute" in the Configuration Management document

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

Step	Action

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" (page 78).

3 You have completed this procedure.

—End—

Accessing a TCP-IN device from a remote location

Step	Action

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 When prompted, enter your user ID and password.

3 Start the logroute tool:

```
logroute
```

4 Continue with the desired procedure from the table "Remote access to log devices procedures" (page 78).

5 You have completed this procedure.

—End—

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.

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" (page 186)
- "Verifying the FTP Schedule" (page 206)

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" (page 136)

- "Clearing a major SBACP alarm" (page 176)
- "Clearing a minor SBACP alarm" (page 180)

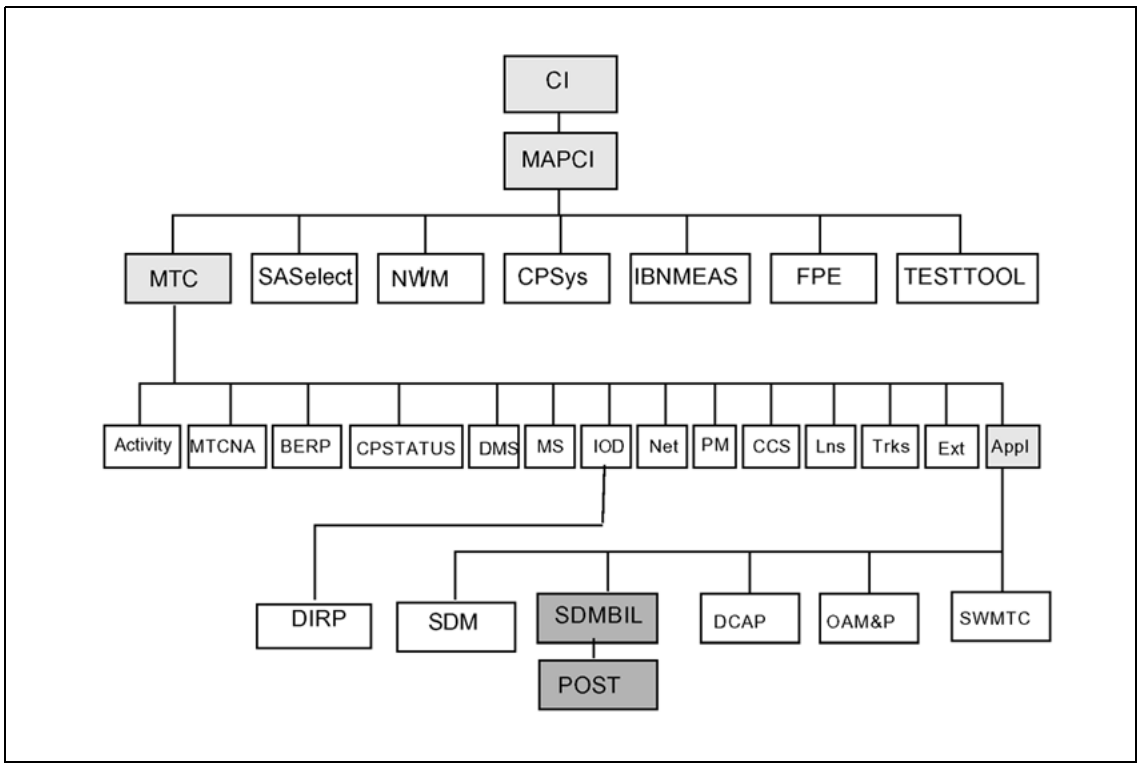
Prerequisites

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

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" (page 82)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" (page 186) helps you determine that the FTP process is configured correctly and is able to transfer files
- "Verifying the FTP Schedule" (page 206) 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" (page 116)
- "Clearing a BAK70 alarm" (page 120)
- "Clearing a BAK90 alarm" (page 124)
- "Clearing a BAKUP alarm" (page 128)
- "Clearing a NOBAK alarm" (page 151)
- "Clearing a NOREC alarm" (page 160)
- "Clearing a NOSTOR alarm" (page 162)

- "Clearing a NOVOL alarm" (page 166)

Accessing the MATE

Purpose

Use this procedure to access the MATE.

Prerequisites

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

Procedure

Use the following procedure to access the MATE.

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

Accessing the MATE

Step	Action

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

1 Log onto the CBM.

2 Get the current hostname by entering:

```
GetCurrentHostName
```

Example response:

<CBM hostname>-<unit0 / unit1>

3 Access the Report Registration Menu:

If	Then
the hostname returned in step 2 contains "unit0"	the MATE hostname is "unit1"
the hostname returned in step 2 contains "unit1"	the MATE hostname is "unit0"

4 Determine if the MATE is running by entering:

```
ping <mate hostname>
```

The <mate hostname> is the one determined in .

5

If	Do
step 4 indicates the MATE is Active	step 6
otherwise	step 8

6 Access the MATE using SSH by typing:

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

where

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

7 You have completed this procedure.

8 You need to access the MATE through a local VT100 terminal.

—End—

Clearing the MATE alarm

Purpose

Use this procedure to clear the MATE alarm.

Procedure

Use the following procedure to clear the MATE alarm.

Step	Action
	At the workstation UNIX prompt or VT-100 terminal prompt:
1	Log in to the CBM using the root user ID and password.
2	Start the cbmmtc tool by typing: `# cbmmtc` Check the MATE column on the banner. If the state is not "." (dot), this indicates the presence of an alarm.
3	Access the MATE by performing the procedure "Accessing the MATE" (page 86).
4	Clear the alarms by performing the procedure Clearing a minor or major or critical CBM alarm.
5	Check to see if all fault conditions have now cleared: `querycbm flt`
6	Log out of the MATE.
7	You have completed this procedure.
	—End—

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

You must be a user in a role group authorized to perform accounting-manage actions.

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

Procedure	Document
Logging in to the CBM	*Core and Billing Manager 850 Security and Administration*, NN10358-611
Displaying actions a role group is authorized to perform	*Core and Billing Manager 850 Security and Administration*, NN10358-611

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

Step	Action
	At any workstation or console
1	Log into the core manager as a user authorized to perform accounting-manage actions.
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.

—End—

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 MAPCI 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

You must be a user in a role group authorized to perform fault-view actions.

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

Procedure	Document
Logging in to the CBM	*Core and Billing Manager 850 Security and Administration*, NN10358-611
Displaying actions a role group is authorized to perform	*Core and Billing Manager 850 Security and Administration*, NN10358-611

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

Step	Action
	At any workstation or console
1	Log into the core manager as a user authorized to perform fault-view actions.
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.

—End—

Collecting DEBUG information using the CBMGATHER command

Purpose

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

Application

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

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

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

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.

Prerequisites

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

You may log into the server as root or emsadmin.

Procedure

Step	Action
	At the core manager command line (UNIX prompt) of the active node
1	Log into the core manager.
2	Run the utility to collect the output: **`cbmgather`** The output file from this command is located under /var/adm and has a name in the format: cbmgather_<machine>_<date_and_time>.tar.Z *Example:* /var/adm/cbmgather_hadry2_20050221141300.tar.Z
3	Tar and compress the content of directory /var/adm:

```
cd /var/adm

tar cvf varadm_active.tar *.day* *log

compress varadm_active.tar
```

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

4 Move the files generated by commands executed in step 2and step 3 out the system to a secure location using FTP (in BINary mode).

5 Remove the gathered output/files from the system:

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

and use the rm command to delete each one.

If	Do
your system is a CBM 850 cluster configuration	step 6
your system is not a CBM 850 cluster configuration	step10

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

6 Run the utility to collect the output:

```
cbmgather
```

7 Tar and compress the content of directory /var/adm:

```
cd /var/adm

tar cvf varadm_inactive.tar *.day* *log

compress varadm_inactive.tar
```

Example response:

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

8 Move the files generated by commands executed in step 6and step 7out the system to a secure location using FTP (in BINary mode).

9 Remove the gathered output/files from the system:

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

and use the rm command to delete each one.

10 You have completed this procedure.

—End—

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 be a user in a role group authorized to perform accounting-manage actions.

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

Procedure Document

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

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

Step	Action
	At any workstation or console
1	Log in to the core manager as a user authorized to perform accounting-manage actions.
2	Access the Application level: `cbmmtc appl` The system displays a list of applications.

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

If you want to	Do
busy the CBM billing application	step 7
return the CBM to service	step 9

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

3 Busy the SDM Billing Application:

```
bsy <x>
```

where

<x> is the number next to the SDM 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 17
did not busy successfully	contact your next level of support

5 Return the SDM Billing Application to service:

```
rts <x>
```

where

<x> is the number next to the SDM Billing Application

This command causes SBA streams to go into a recovery mode.

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 11
does not generate log SDM375	you have completed this procedure

7

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

Busy the CBM 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"):
```

8 Confirm the busy command:

```
y
```

If the SBA	Do
busied successfully and you want to return the SBA to service	step 9
busied successfully but you do not want to return the SBA to service at this time	step 17
did not busy successfully	contact your next level of support

9 Return the CBM Billing Application to service:

```
rts <x>
```

where

`<x>` is the number next to the CBM Billing Application

This command causes SBA streams to go into a recovery mode.

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 10
did not return to service successfully	contact your next level of support

10 Determine if log SDMB375 was generated.

If the system	Do
generates log SDMB375	step 11
does not generate log SDM375	you have completed this procedure

11 Return the RTB streams to service. Exit the Application level:

```
quit all
```

12 Access the billing maintenance level:

```
billmtc
```

13 Access the schedule level:

```
schedule
```

14 Access the real-time billing level:

```
rtb
```

15 Busy the stream:

```
bsy <stream name> <file format> <destination>
```

where

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

16 Return the stream to service:

```
rts <stream name> <file format> <destination>
```

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 17
does not return to service successfully	contact your next level of support

17 Quit the billing maintenance level:

```
quit all
```

18 You have completed this procedure

—End—

Displaying or storing log records using logreceiver

The following procedure explains how to display or store log records on a workstation using the logreceiver tool.

The command 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 in configuring the TCP device on the CBM. 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 xxx, exiting
```

You must change the port number used in configuring the TCP device on the CBM.

Checking the port numbers in use on a workstation

Step	Action
	At the client workstation
1	Check the port numbers in use by typing **`more/etc/services`** and pressing the Enter key. You will see the list of port numbers in use on the display. Scroll through the display by pressing the Enter key again.

—End—

Storing logs in a file

Step	Action
	At the client workstation
1	Start the logreceiver tool to store logs in a file by typing **`logreceiver <port> -f <filename>`** and pressing the Enter key. where **`<port>`** is the port number used when configuring the TCP device on the CBM **`<filename>`** is the name of the file

If the file does not exist, it will be created automatically. The logs from theCBM will be stored in this file. If the file exists, the logs from theCBM will be added to it provided its UNIX access permissions allow writing to the file. In either case, a message '`Accepted connection request from host xxx`' will be displayed on the screen just before the first log received is written to the file. Type "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. Type "control -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.

—End—

Displaying log records on a workstation

Step	Action
	At the client workstation
1	Start the logreceiver tool to display the log records on the screen by typing **`logreceiver <port>`** and pressing the Enter key. where **`<port>`** is the port number used when configuring the TCP device on the CBM
2	You have completed this procedure.

—End—

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.

Prerequisites

All users are authorized to perform this procedure.

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

Procedure	Document
Logging in to the CBM	*Core and Billing Manager 850 Security and Administration*, NN10358-611
Displaying actions a role group is authorized to perform	*Core and Billing Manager 850 Security and Administration*, NN10358-611

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

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

Step	Action
	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 permisssion 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 permisssion 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.

—End—

Troubleshooting RTB problems

Purpose

Use this procedure when troubleshooting real time billing (RTB) problems.

Prerequisites

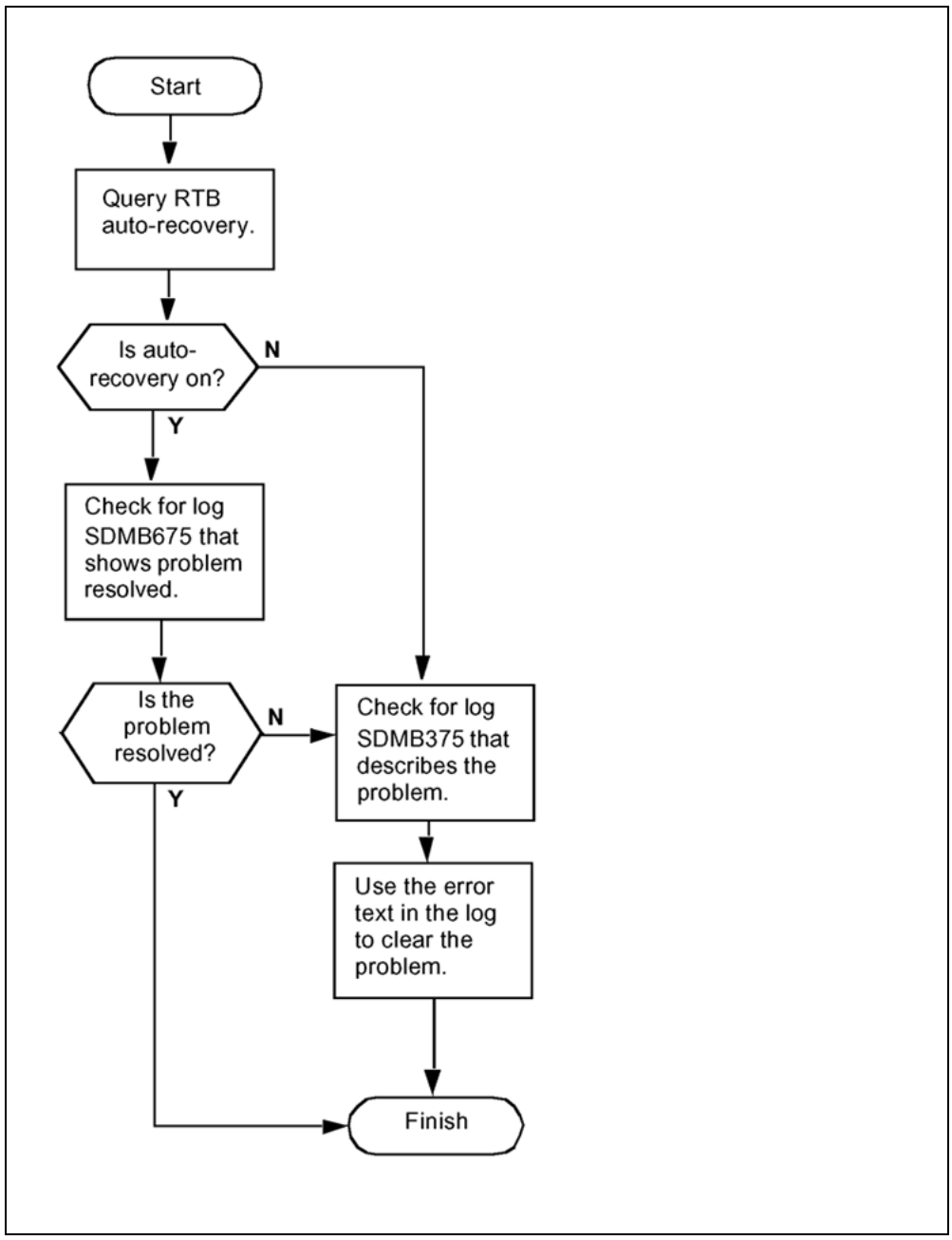
You must be a user in a role group authorized to perform accounting-manage actions.

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

Procedure	Document
Logging in to the CBM	*Core and Billing Manager 850 Security and Administration*, NN10358-611
Displaying actions a role group is authorized to perform	*Core and Billing Manager 850 Security and Administration*, NN10358-611

Action

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



Procedure

Use the following procedure to troubleshoot RTB problems.

Troubleshooting RTB problems

Step	Action
	At the core manager

1 Log in to the core manager as a user authorized to perform accounting-manage actions.

2 Query the RTB auto-recovery.

3 In the display look for the status of the auto-recovery.

If auto-recovery is	Do
on	step 4
off	step 6

4 Check for log SDMB675.

5 In the log look for the status of the problem.

If problem is	Do
resolved	step 8
not resolved	step 6

6 Check for log SDMB375.

7 In the log look for the description of the problem and use the error text to clear the problem.

8 You have completed this procedure.

—End—

Troubleshooting problems with scheduled billing file transfers

Purpose

Use this procedure when troubleshooting problems with Scheduled billing file transfers.

Prerequisites

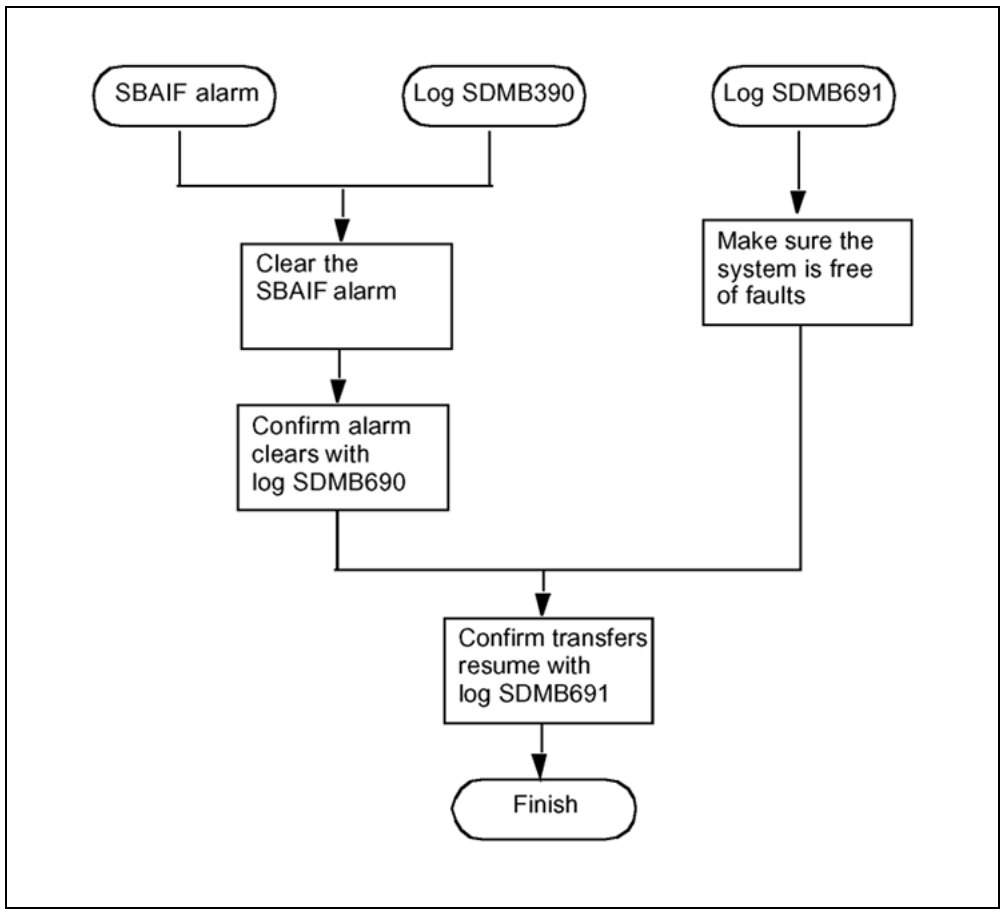
You must be a user in a role group authorized to perform accounting-manage actions.

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

Procedure	Document
Logging in to the CBM	*Core and Billing Manager 850 Security and Administration*, NN10358-611
Displaying actions a role group is authorized to perform	*Core and Billing Manager 850 Security and Administration*, NN10358-611

Action

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.



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

Procedure

Use the following procedure to troubleshoot problems with scheduled billing file transfers.

Troubleshooting problems with scheduled billing file transfers

Step	Action
	At the core manager
1	Log in to the core manager as a user authorized to perform accounting-manage actions.
2	Query the SBAIF alarm.

3 In the display look for the status of the SBAIF alarm.

If alarm is	Do
on	step 6
cleared	step 4

4 Check for log SDMB390.

5 In the log look for the status of the problem.

If problem is	Do
resolved	step 9
not resolved	step 6

6 Clear the SBAIF alarm.

7 Check for log SDMB690.

8 In the log look for the status of the problem.

If problem is	Do
resolved	step 11
not resolved	step 2

9 Check for log SDMB691.

10 In the log confirm that system is free of faults.

If problem is	Do
free of faults	step 12
not free of faults	step 2

11 Check for log SDMB691.

12 In the log confirm that transfers have resumed.

13 You have completed this procedure.

—End—

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

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.

Prerequisites

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

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

Step	Action
	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

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
```

ATTENTION
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.

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:

ATTENTION
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. Perform procedure "Increasing the size of a file system on an SPFS-based server" (page 242).

ATTENTION
Once you have increased the size of a file system, you cannot decrease it.

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.

For example:

3Mb x 2 x 50 days = 300 Mb

where

3 Mb

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

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.

—End—

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.

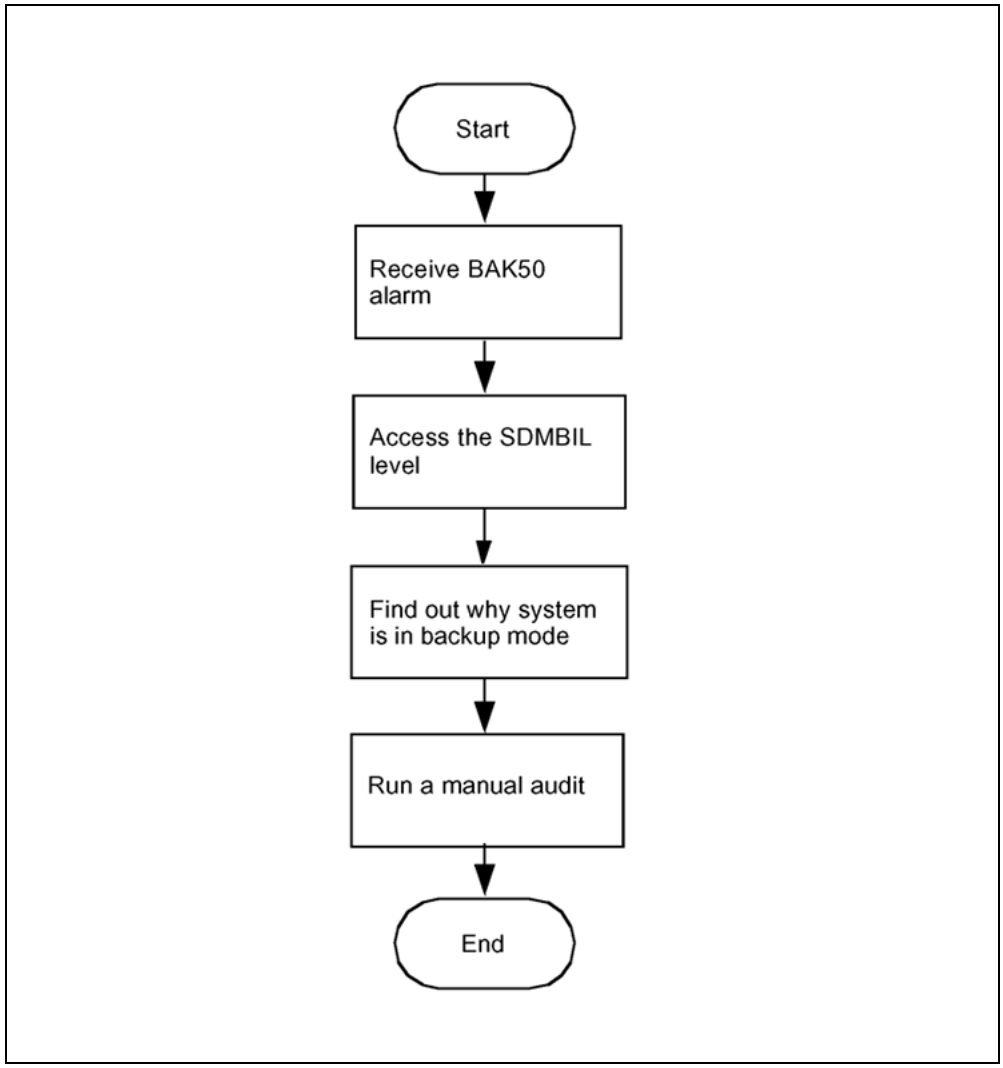
Impact

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

Step	Action

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" (page 176), 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" (page 132)

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.

—End—

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.

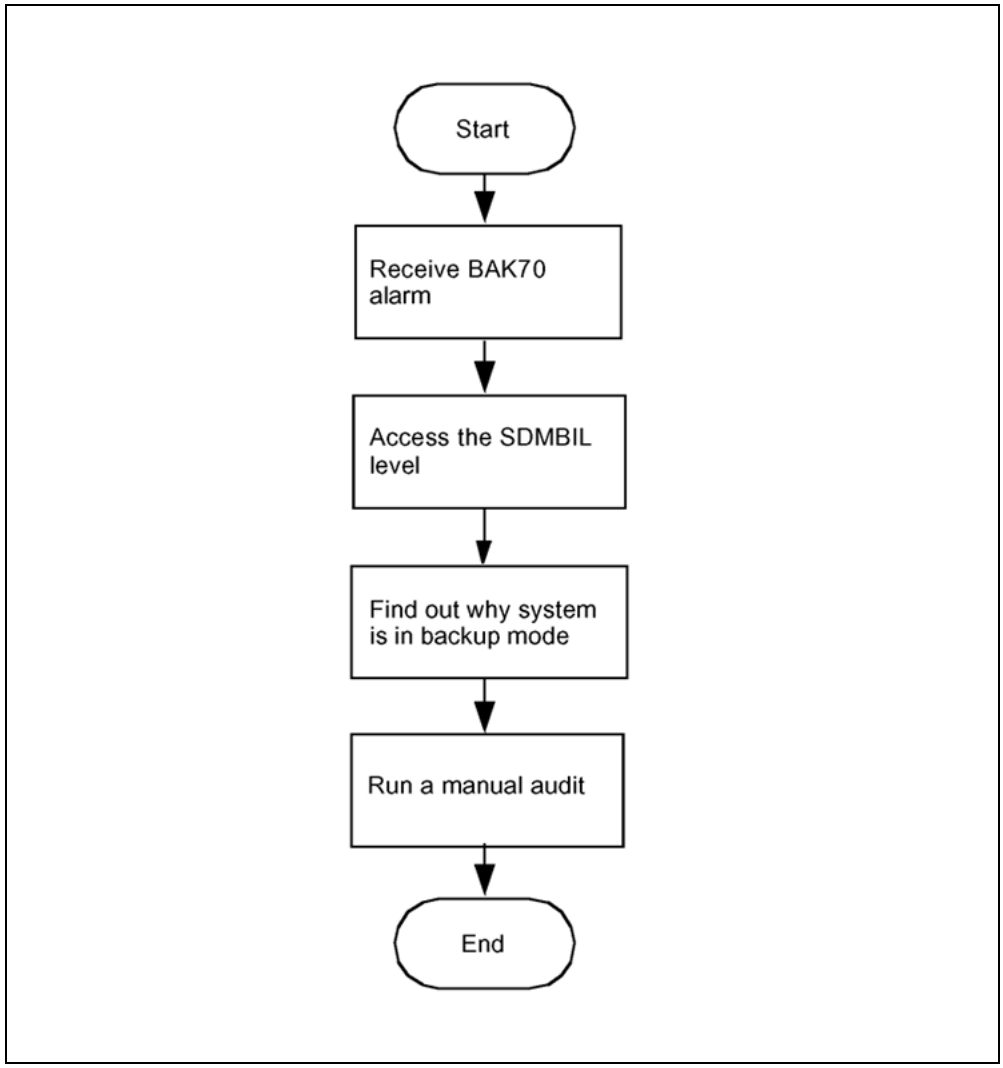
Impact

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

Step	Action

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" (page 176), 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" (page 132)

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.

—End—

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.

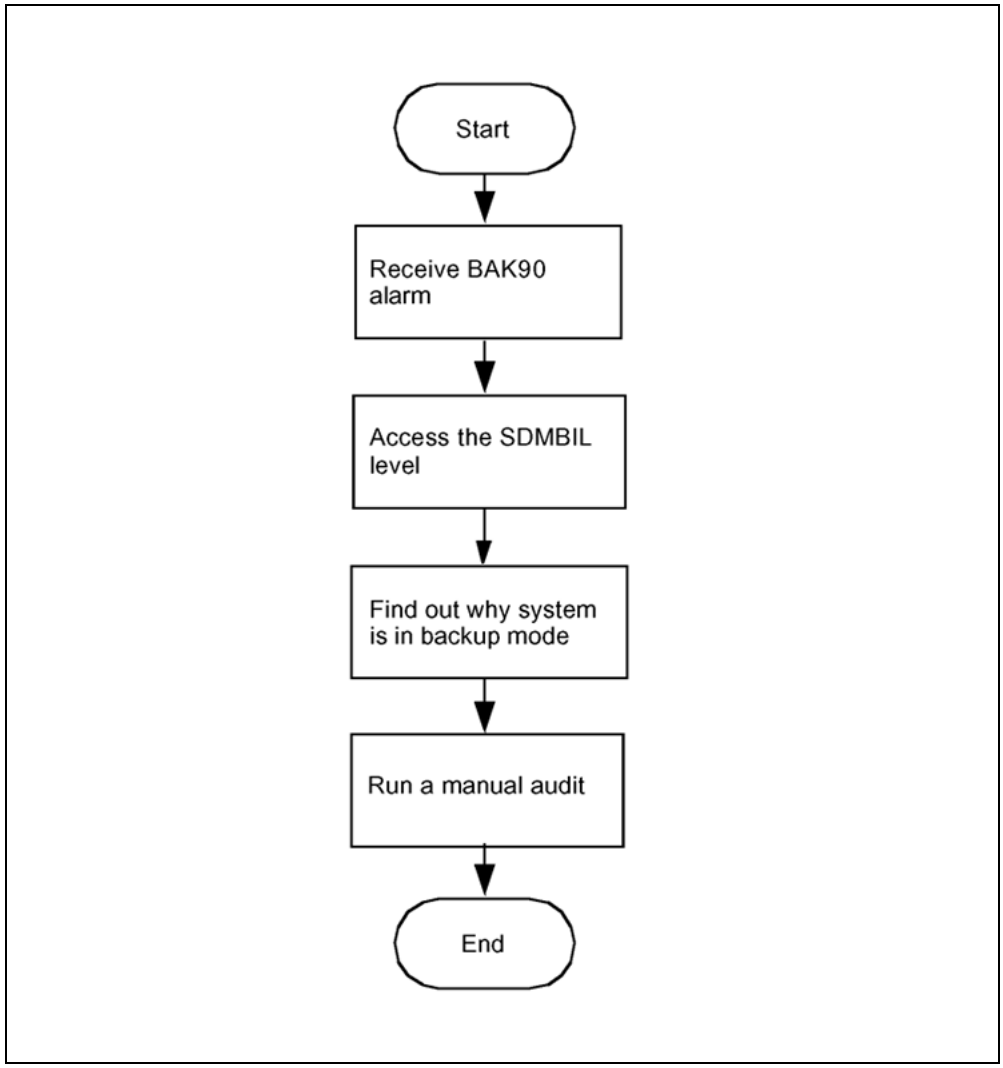
Impact

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

Step	Action

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 , 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

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.

—End—

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 major 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 major

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.

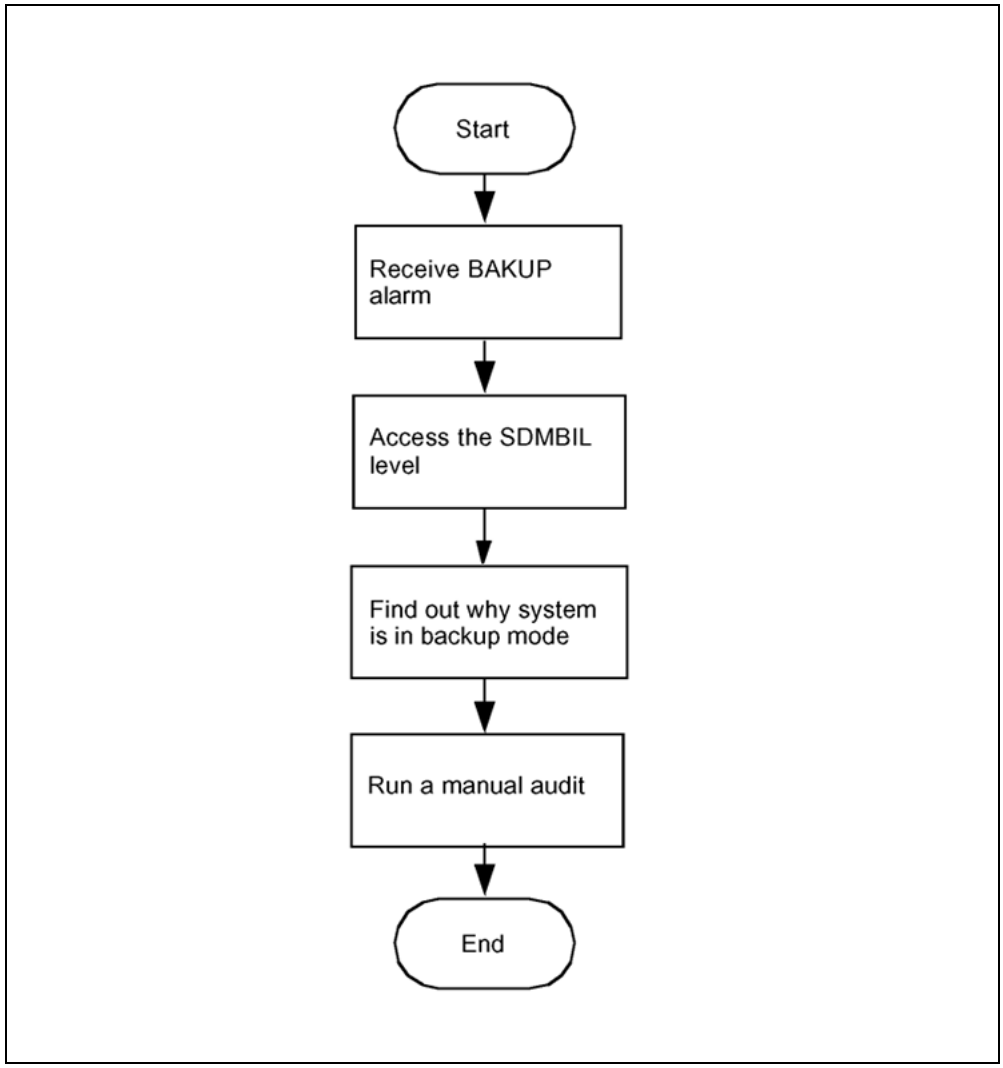
Impact

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

Step	Action

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 , 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

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.

—End—

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.

Procedure

Adjusting disk space in response to SBA backup file system alarms

Step	Action

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:

```
> dskut;sv <volume name>
```

where

<volume name> is the name of one of the volumes that you obtained and recorded in step 2

4 Repeat step3 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 step5 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.

—End—

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 CurrentTmpltID 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 currentTmpltID.

Impact

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

Action

If this alarm occurs:

- set the value of the CurrentTmpltID 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.

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.

Step	Action
	At the MAP
1	Determine the value of the active template ID on the DMS/CM: `CTMPLT "template all"`
2	Set the CurrentTmpltID mib parameter to match the value of the active template ID:

mib cdr set CurrentTmpltID <template_ID>

where

<template_ID> is the value of the active template on the DMS/CM.

3 If you change the CurrentTmpltID 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.

—End—

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

Step	Action
	At the MAP interface on the CM
1	Access the SDMBIL level: `> mapci;mtc;appl;sdmbil`
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 NN-20000-247, *CBM Accounting for Wireless Networks*.
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 a Sun server".

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 275.

5 If you want to back up the billing files, perform the procedure "Copying files to DVD" in the *Core and Billing Manager 850 Accounting*, NN10363-811.

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.

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" (page 186)and "Verifying the FTP Schedule" (page 206), 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 18
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 /<directory>/<stream_name>/orphan
```

where

<directory> 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>
```

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 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 -R 755 / <stream> / <stream_name>
```

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

15 Change the ownership of a directory:

```
>chmod -R maint:maint / <stream> / <stream_name>
```

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

16 Perform procedure "Controlling the SDM Billing Application" (page 95).

17 Use Audit to clear the alarm.

If the alarm	Do
cleared	step 18
did not clear	contact your next level of support

18 You have completed this procedure.

—End—

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.

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), and
- did not delete the associated schedule tuple on the core manager first

Impact

The core manager cannot send files to the downstream destinations. The core manager has possibly reached 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 are lost.

Action

Clearing an FTPW alarm

Step	Action

At the core manager

1 Complete procedure Verifying the file transfer protocolin 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 SDM CBM Accounting document, then return to this procedure.

3 Once the alarm is cleared, delete the tuple that you added in 2.

4 You have completed this procedure.

—End—

Clearing an SFTPW alarm

Purpose

Use this procedure to clear an SFTPW alarm.

Indication

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

Meaning

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

The SFTPW alarm can be present on the CM for a non-existent schedule. For example, the SFTPW alarm is generated if an operator shuts down the server (making the sftp 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 SFTPW alarm

Step	Action
	At the core manager
1	Log in to the core manager as a user authorized to perform accounting-admin actions.
2	Complete procedure "Verifying the secure file transfer protocol" (page 199) in this document.
3	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 SDM CBM Accounting document, then return to this procedure.

4 Once the alarm is cleared, delete the tuple that you added in step 3.

5 You have completed this procedure.

—End—

Clearing a KSFTP alarm

Purpose

Use this procedure to clear an KSFTP alarm.

Indication

At the MTC level of the MAP display, KSFTP appears under the APPL header of the alarm banner and indicates an alarm for Key-based SFTP.

Meaning

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

The SFTPW alarm can be present on the CM for a non-existent schedule. For example, the SFTPW alarm is generated if an operator shuts down the server (making the SFTP 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 a KSFTP alarm

Step	Action
	At the core manager
1	Log in to the core manager as a user authorized to perform accounting-admin actions.
2	Complete procedure "Verifying the Key-based secure file transfer protocol (KSFTP)" (page 194) in this document.
3	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 SDM CBM Accounting document, then return to this procedure.

4 Once the alarm is cleared, delete the tuple that you added in step 3.

5 You have completed this procedure.

—End—

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

Step	Action
	At the MAP

1 Log in to the core manager as maint user.

If the	Do
/home/maint/ftpdir directory has write permissions	no action is required
/home/maint/ftpdir directory does not have write permissions	step 2only
<rcLogicalVolumeDirectory>/ftpdir directory has write permissions	no action is required
<rcLogicalVolumeDirectory>/ftpdir directory does not have write permissions	step 3only
storage disk has sufficient space	no action is required
storage disk does not have sufficient space	step 4only
<rcLogicalVolumeDirectory> path is correct	no action is required
<rcLogicalVolumeDirectory> path is incorrect	correct the <rcLogicalVolumeDirectory> path into the CONFSTRM
<rcLogicalVolumeDirectory>/ftpdir is a directory	no action is required
<rcLogicalVolumeDirectory>/ftpdir is not a directory	step 5only
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/ftpdir directory:

```
> chmod 777 /home/maint/ftpdir
```

3 Remove the <rcLogicalVolumeDirectory>/ftpdir directory:

```
> rm / <rcLogicalVolumeDirectory> /ftpdir
```

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.

The next interval recreates the correct permissions and recreates all links.

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

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.

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>/ftpdir directory:

```
> rm /<rcLogicalVolumeDirectory>/ftpdir
```

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.

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

6 You have completed the procedure.

—End—

Clearing an LODSK alarm

Purpose

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

Prerequisites

You must be a user in a role group authorized to perform accounting-admin actions.

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

Procedure	Document
Logging in to the CBM	*Core and Billing Manager 850 Security and Administration*, NN10358-611
Displaying actions a role group is authorized to perform	*Core and Billing Manager 850 Security and Administration*, NN10358-611

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" (page 186)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.

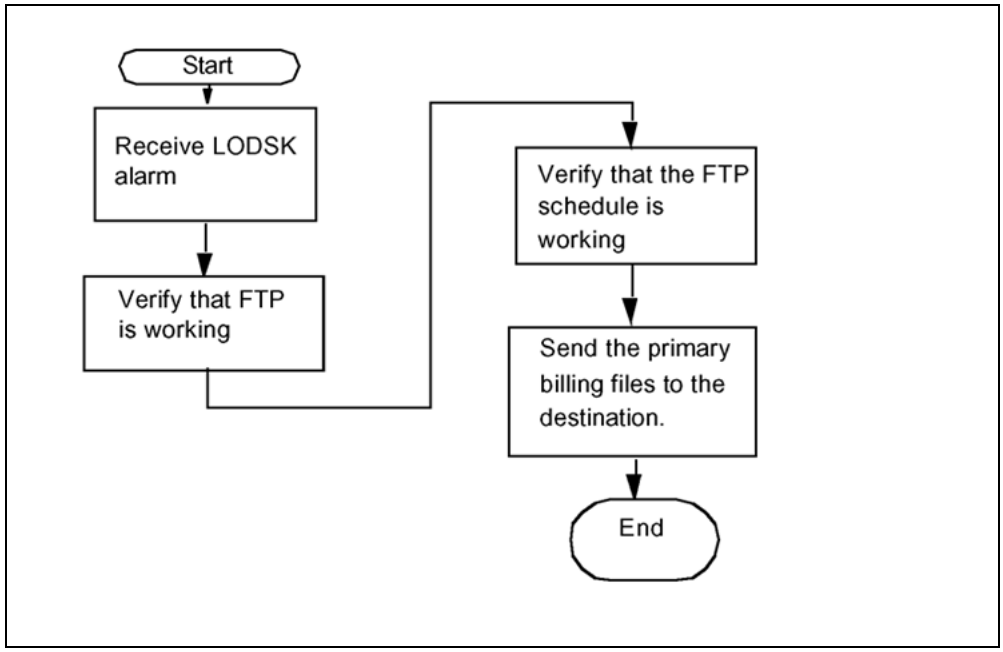
Impact

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

Step	Action

At the MAP

1 Use the procedure "Verifying the file transfer protocol" (page 186)to determine if the FTP is working properly.

If the alarm	Do
clears	step 2
does not clear	refer to procedure "Verifying the FTP Schedule" (page 206) if the alarm persists, contact your next level of support

2 You have completed this procedure.

—End—

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

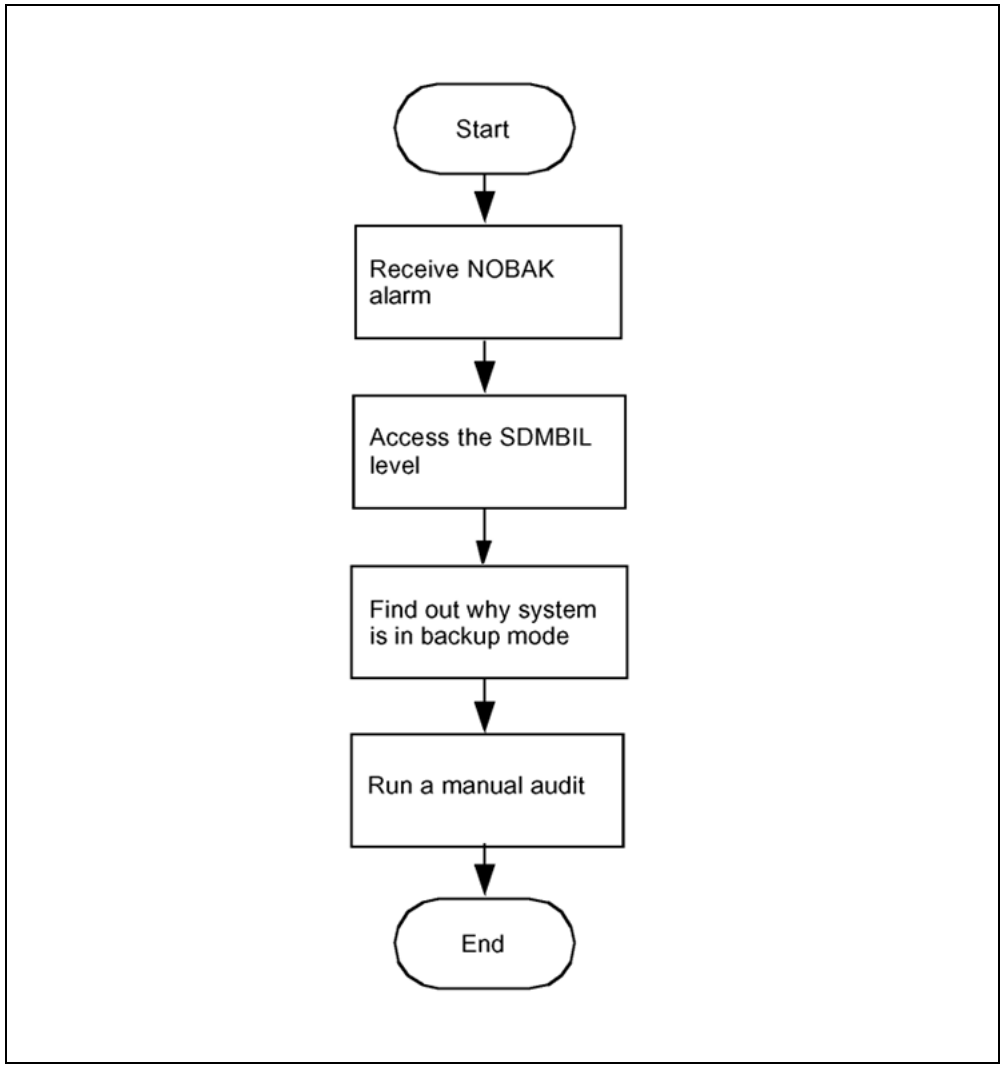
ATTENTION

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

Step	Action

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" (page 176), 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" (page 132)

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.

—End—

Clearing a NOCLNT alarm

Purpose

Use this procedure to clear a NOCLNT alarm.

Indication

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

Meaning

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

- `on`

  the alarm is critical

- `both`

  the alarm is major

ATTENTION

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

Impact

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

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

Action

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

Clearing a NOFL alarm

Purpose

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

Indication

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

Meaning

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

- `both`

  the alarm severity level is major

- `on`

  the alarm severity level is critical

ATTENTION

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

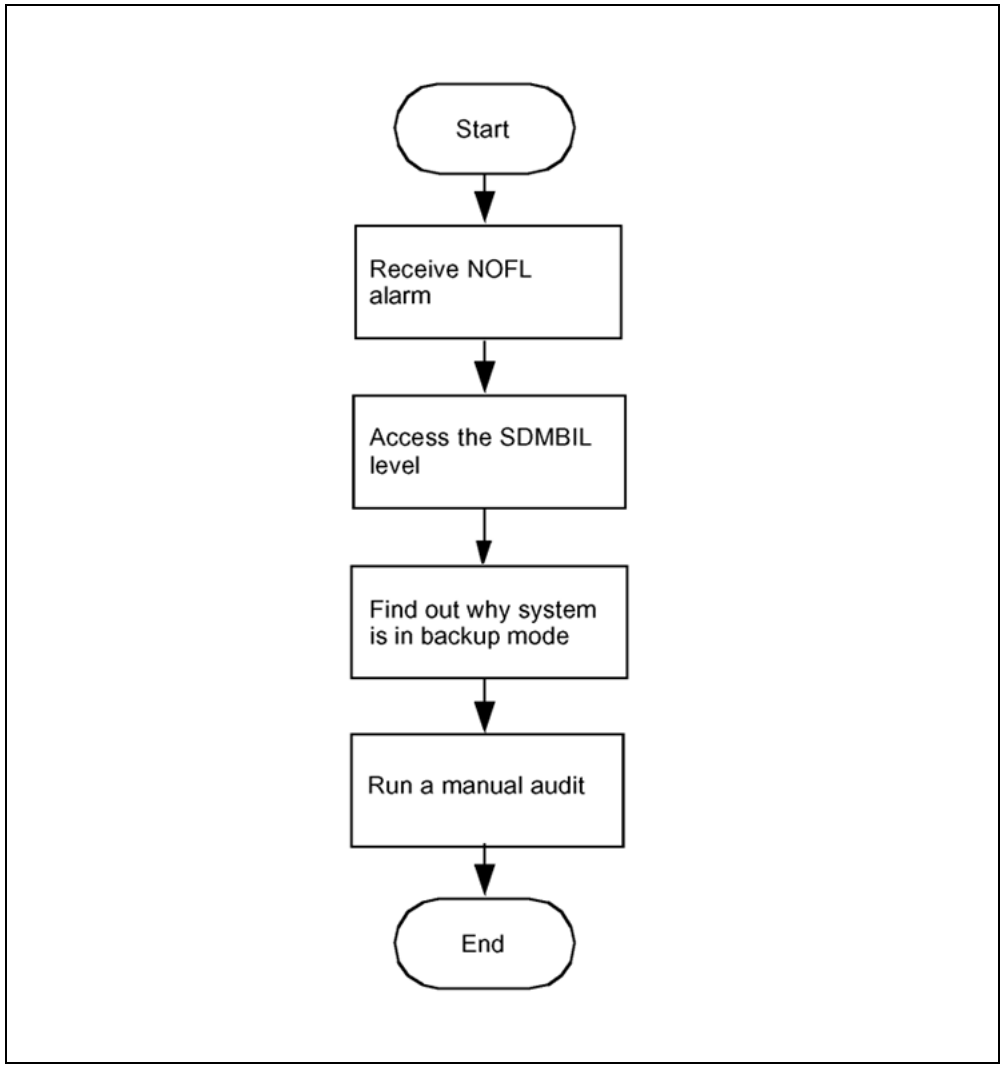
Impact

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

Procedure

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

NOFL alarm clearing flowchart



Clearing a NOFL alarm

Step	Action

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" (page 176), 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" (page 132)

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.

—End—

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 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.

If the fixed template id 0 or if the CurrrentTmpltID 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

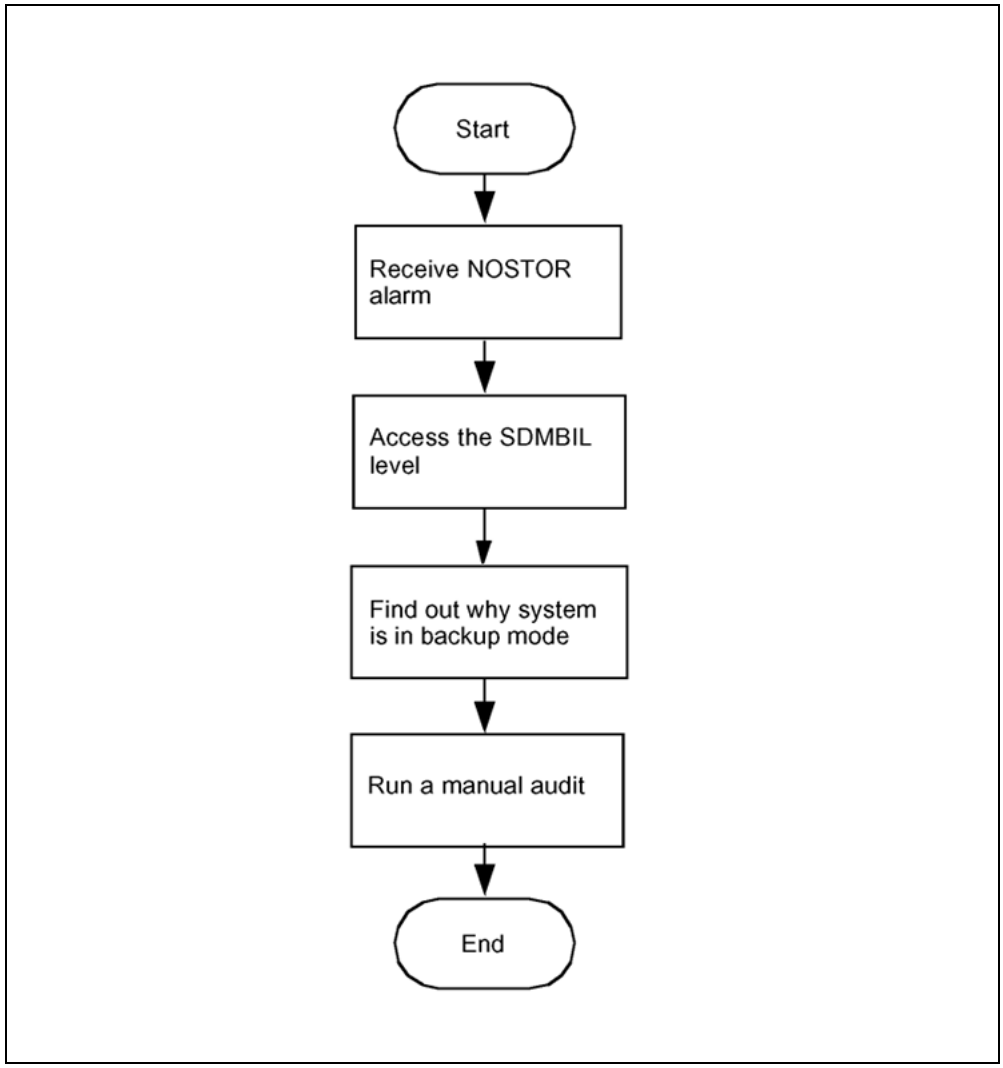
ATTENTION

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



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

Step	Action
	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" (page 176), 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" (page 132)

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.

—End—

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.

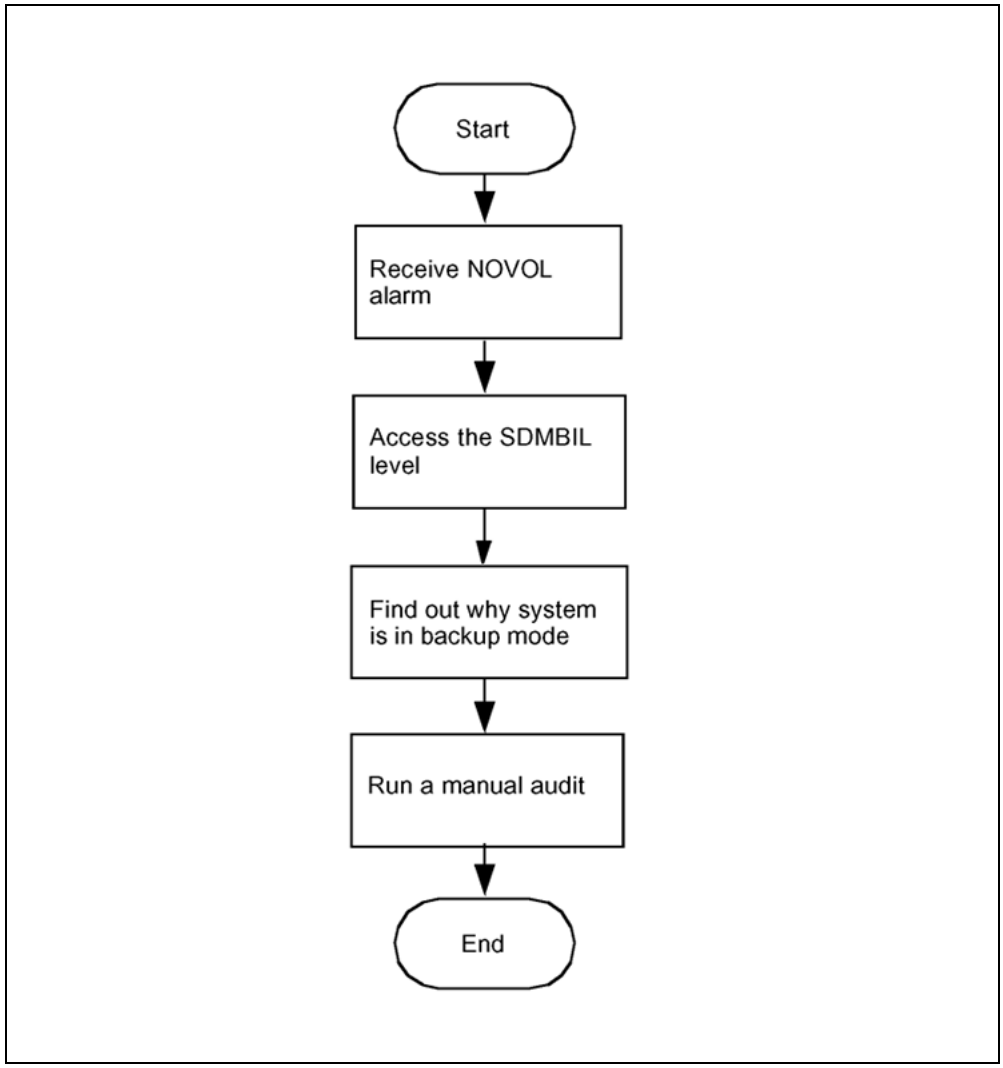
Impact

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



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

Step	Action
	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" (page 176), 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" (page 132)

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.

—End—

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

Step	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.
	—End—

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.

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.

Prerequisites

You must be a user in a role group authorized to perform accounting-manage actions.

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

Procedure	Document
Logging in to the CBM	*Core and Billing Manager 850 Security and Administration*, NN10358-611
Displaying actions a role group is authorized to perform	*Core and Billing Manager 850 Security and Administration*, NN10358-611

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.

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.

ATTENTION

This alarm will not clear until at least one billing stream is in service.

Step	Action

At the MAP

1 Do one of the following:

If	Do
performing this procedure on a CBM800	step 2
performing this procedure on a CBM850	step 5

2 Access the APPL SDM Menu level:

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

If the core manager is	Do
Offl or SysB	step 3
ManB	step 4
InSv or ISTb	step 6

3 Busy the core manager:

```
> bsy
```

4 Return the core manager to service:

```
> rts
```

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.

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 6
did not return to service successfully	contact your next level of support

At the core manager

5 Log in to the core manager as a user authorized to perform accounting-manage actions.

6 Go to the Appl level of the cbmmtc tool by typing:

```
cbmmtc appl
```

If the SBA application is	Do
ISTB, Offl, or SysB	step 7
ManB	step 8
InSv, and the alarm is cleared	step 15
InSv, but the alarm is still present	contact your next level of support

7 Busy the SBA application:

```
bsy <SBA_no>
```

where

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

8 Return the SBA application to service:

```
rts <SBA_no>
```

where

<SBA_no> is the number of the SBA application.

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 9
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

9 Return the RTB streams to service. Exit the maintenance interface.

```
quit all
```

10 Access the billing maintenance level:

```
billmtc
```

11 Access the schedule level:

```
schedule
```

12 Access the real-time billing level:

```
rtb
```

13 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)

14 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

15 You have completed this procedure.

—End—

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.

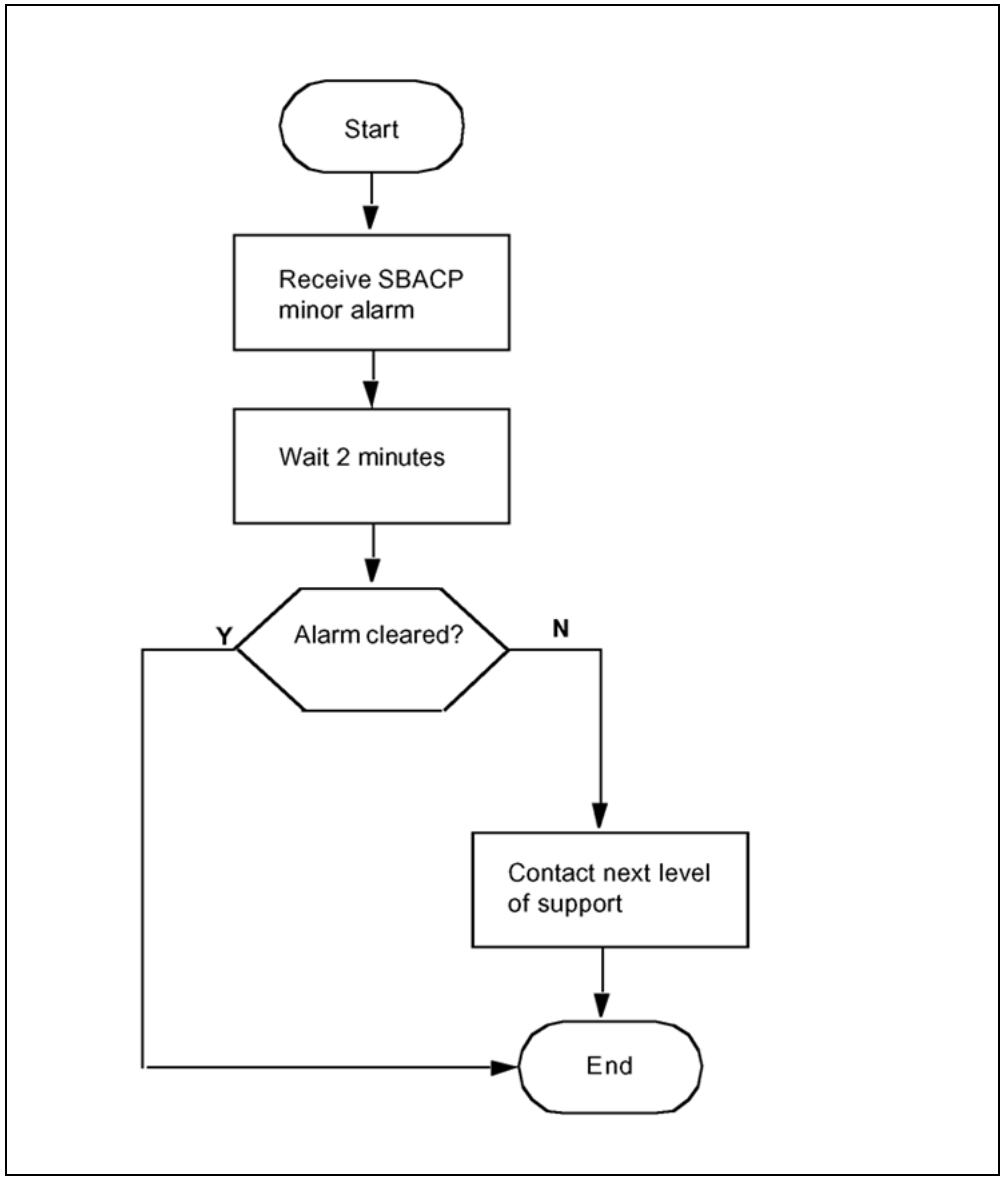
Impact

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

Step	Action
	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.

—End—

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.

Prerequisites

You must be a user in a role group authorized to perform accounting-manage actions.

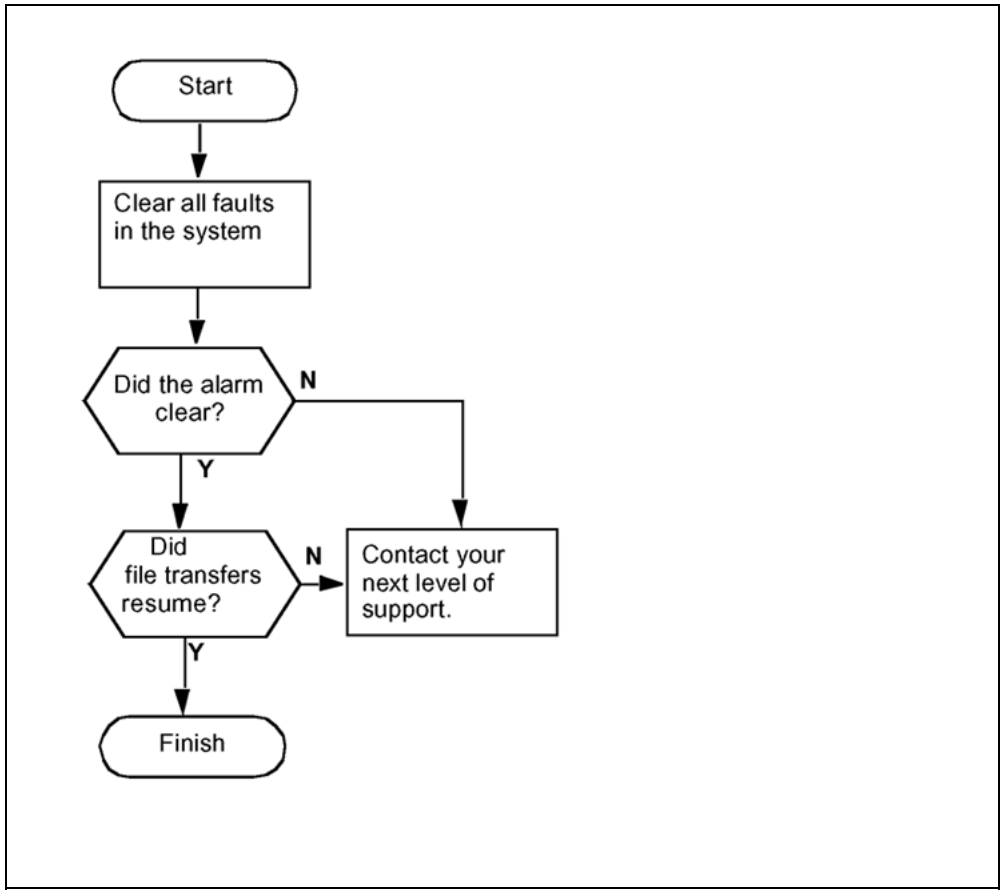
For information on how to log in to the CBM as an authorized user or how to display information about a user or role group, review the procedures in the following table.

Procedure	Document
Logging in to the CBM	*Core and Billing Manager 850 Security and Administration*, NN10358-611
Displaying actions a role group is authorized to perform	*Core and Billing Manager 850 Security and Administration*, NN10358-611

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

Step	Action

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 Log in to the core manager as a user authorized to perform accounting-manage actions.

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.

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.

—End—

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.

Prerequisites

In order to perform this procedure, you must have the following authorization and access.

- You must be a user in a role group authorized to perform accounting-admin actions.
- You must obtain non-restricted shell access.

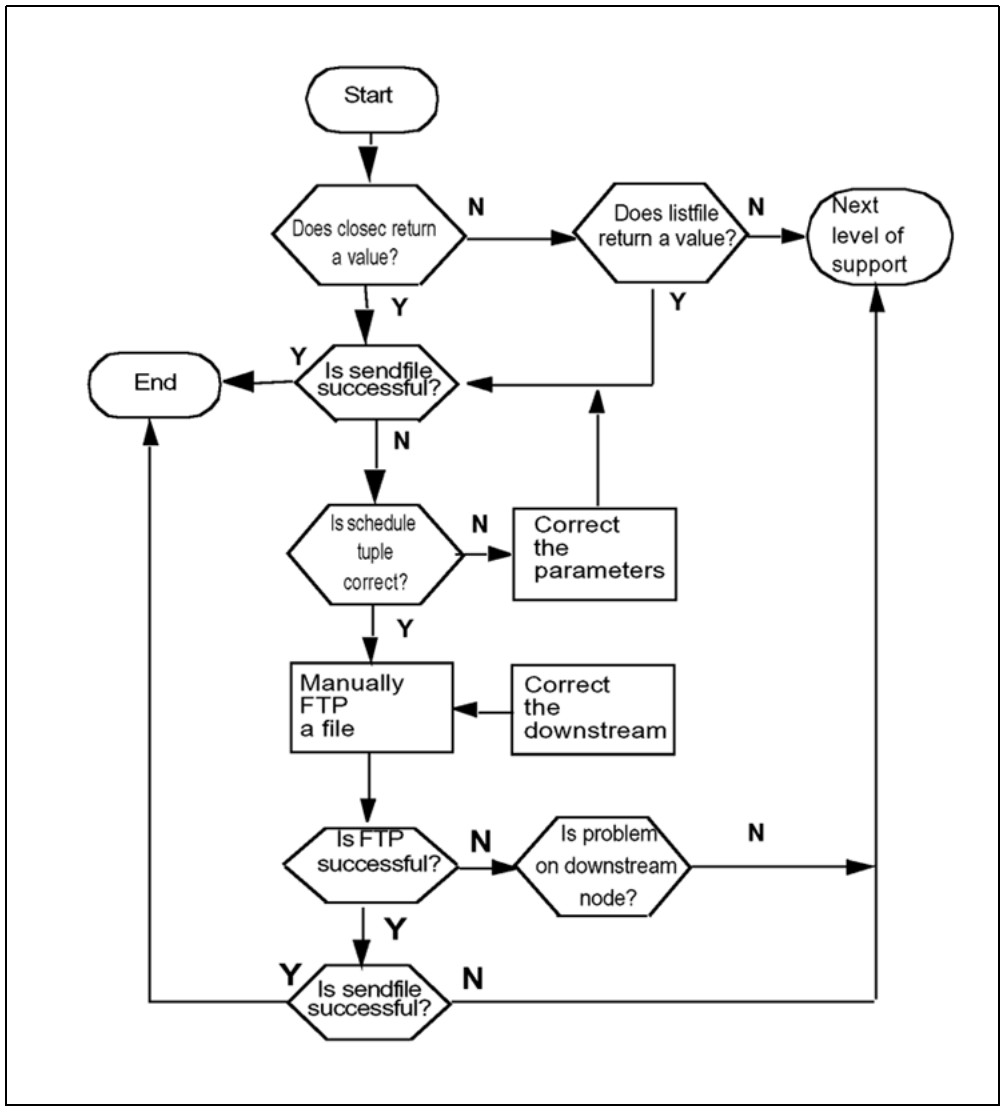
For more information on how to log in to the CBM as an authorized user, how to request a non-restricted shell access, or how to display actions a role group is authorized to perform, review the procedures in the following table.

Procedure	Document
Logging in to the CBM	*Core and Billing Manager 850 Security and Administration*, NN10358-611
Requesting non-restricted shell access	*Core and Billing Manager 850 Security and Administration*, NN10358-611
Displaying actions a role group is authorized to perform	*Core and Billing Manager 850 Security and Administration*, NN10358-611

Action

The following flowchart summarizes the steps outlined in the procedure.

FTP verification flowchart



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

Step	Action
	At the core manager
1	Log in to the core manager as a user authorized to perform accounting-admin actions.
2	Access the bill maintenance level:

billmtc

3 Access the file system:

filesys

4 Close active billing files:

closec <stream_name>

where

<stream_name> is the name of the stream.

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

5 Determine the results of the closec command.

If the "closec" command	Do
returns a filename	step 8
does not return a filename	step 6

6 List the primary file (closedNotSent directory):

listfile <stream_name>

where

<stream_name> is the name of the stream

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

8 Send the primary file (closedNotSent directory):

sendfile <stream_name>

where

<stream_name> is the name of the stream.

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

9 Go to the previous level:

quit

10 Determine the results of the sendfile command.

If the "sendfile" command is	Do
successful	you have completed this procedure
not successful	step 11

Observe the SDMB logs on the CM in logutil to determine why the **`sendfile`** command is not successful prior to continuing with step 11.

11 Access the schedule level:

```
schedule
```

12 List the parameters of the schedule tuple:

```
list
```

If the parameters are	Do
correct, but you are receiving an alarm	step 22
incorrect	step 13

13 Reset the schedule tuple parameters:

```
change
```

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

15 Enter the file format.

16 Enter the destination name.

The destination name can be up to 15 alphanumeric characters.

17 Observe the schedule tuple displayed.

18 Enter the corrected parameters.

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

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

20 Save the changed parameters:

save

If you have	Do
corrected the parameters in the schedule tuple	step 8
determined that the parameters are correct	• step 21(verify login and write permissions are correct for FTP process without testing a billing file), OR • step 25(verify login and write permissions are correct for FTP process while testing an actual billing file)

21 Exit the maintenance interface:

quit all

22 Login as root user.

23 Login as an authorized user.

24 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.

You can use any billing file for step 24because you are only verifying login and write ability on the downstream node.

25 Exit back to the command prompt:

quit all

26 Login as root user.

27 Login as an authorized user.

28 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

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

29 Access the /tmp directory:

```
cd /tmp
```

30 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

31 Log onto the node when prompted by the FTP (Remote_Login and Remote_Password defined in the schedule tuple):

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.

32 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.

A successful login is confirmed by a "250 CWD command successful" message returned by the FTP.

33 If the "cd" command is unsuccessful, obtain a valid directory from the downstream node and update the schedule tuple with the valid values.

34 Set the file transfer mode to binary:

```
ftp> binary
```

A successful command is confirmed by a "200 Type set to I" message returned by the FTP.

35 Execute the "structure" command and verify the returned message:

```
ftp> stru f
```

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".

36 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 28.
<file.tmp> is the name of the billing file with the .tmp extension appended.

The responses from a UNIX machine for a valid command would be "200 PORT command successful" and "226 Transfer complete".

37 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 36.
<file> is the name of billing file to which the .tmp extension was appended in step 36.

The responses from a UNIX machine for a valid command would be "350 File exists, ready for destination name" and "250 RNTO command successful".

38 Exit from the FTP session:

```
ftp> quit
```

If the file transfer is	Do
successful	step 41
unsuccessful because of a permission error	step 39
unsuccessful for a reason other than permission error	step 41

39 Correct the directory permissions to allow write access.

40 Repeat steps 22through 38.

41 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).

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

—End—

Verifying the Key-based secure file transfer protocol (KSFTP)

Purpose

You can use this procedure on the core manager to verify that the key-based secure file transfer protocol (KSFTP) is configured correctly to transfer files.

Prerequisites

In order to perform this procedure, you must have the following authorization and access.

- You must be a user in a role group authorized to perform accounting-admin actions.
- You must obtain non-restricted shell access.

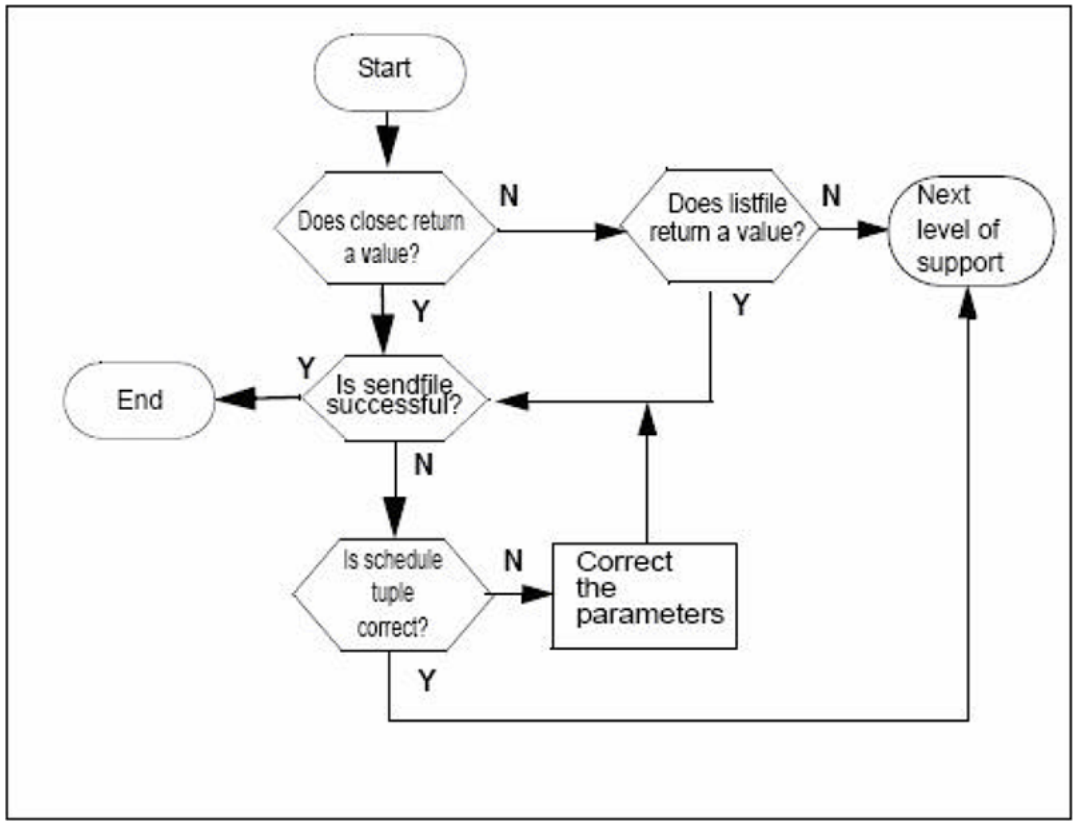
For more information on how to log in to the CBM as an authorized user, how to request a non-restricted shell access, or how to display actions a role group is authorized to perform, review the procedures in the following table.

Procedure	Document
Logging in to the CBM	*Core and Billing Manager 850 Security and Administration*, NN10358-611
Requesting non-restricted shell access	*Core and Billing Manager 850 Security and Administration*, NN10358-611
Displaying actions a role group is authorized to perform	*Core and Billing Manager 850 Security and Administration*, NN10358-611

Action

The following flowchart summarizes the steps outlined in the procedure.

KSFTP verification flowchart



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 key-based file transfer using SFTP

Step	Action
	At the core manager
1	Log in to the core manager as a user authorized to perform accounting-admin actions.
2	Access the bill maintenance level: `billmtc`
3	Access the file system: `filesys`
4	Close active billing files: `closec <stream_name>`

where

<stream_name> is the name of the stream.

ATTENTION
You must close any active billing files prior to the SFTP process.

5 Determine the results of the closec command.

If the "closec" command	Do
returns a filename	step 8
does not return a filename	step 6

6 List the primary file (closedNotSent directory):

listfile <stream_name>

where

<stream_name> is the name of the stream

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

8 Send the primary file (closedNotSent directory):

sendfile <stream_name>

where

<stream_name> is the name of the stream.

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

9 Go to the previous level:

quit

10 Determine the results of the sendfile command.

If the "sendfile" command is	Do
successful	you have completed this procedure
not successful	step 11

Observe the SDMB logs on the CM in logutil to determine why the **sendfile** command is not successful prior to continuing with step 11.

11 Access the schedule level:

```
schedule
```

12 List the parameters of the schedule tuple:

```
list
```

If the parameters are	Do
correct, but you are receiving an alarm	contact your next level of support
incorrect	step 13

13 Reset the schedule tuple parameters:

```
change
```

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

15 Enter the file format.

16 Enter the destination name.

The destination name can be up to 15 alphanumeric characters.

17 Observe the schedule tuple displayed.

18 Enter the corrected parameters.

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

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

20 Save the changed parameters:

```
save
```

If you have	Do
corrected the parameters in the schedule tuple	step 8
determined that the parameters are correct	step 21 (verify login and write permissions are correct for SFTP process

21 Exit the maintenance interface:

```
quit all
```

22 Login as root user.

23 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).

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

—End—

Verifying the secure file transfer protocol

Purpose

Use this procedure on the core manager to verify that the secure file transfer protocol (SFTPW) for password-based authentication is configured correctly to transfer files.

Prerequisites

You must be a user in a role group authorized to perform accounting-admin actions.

You must obtain non-restricted shell access.

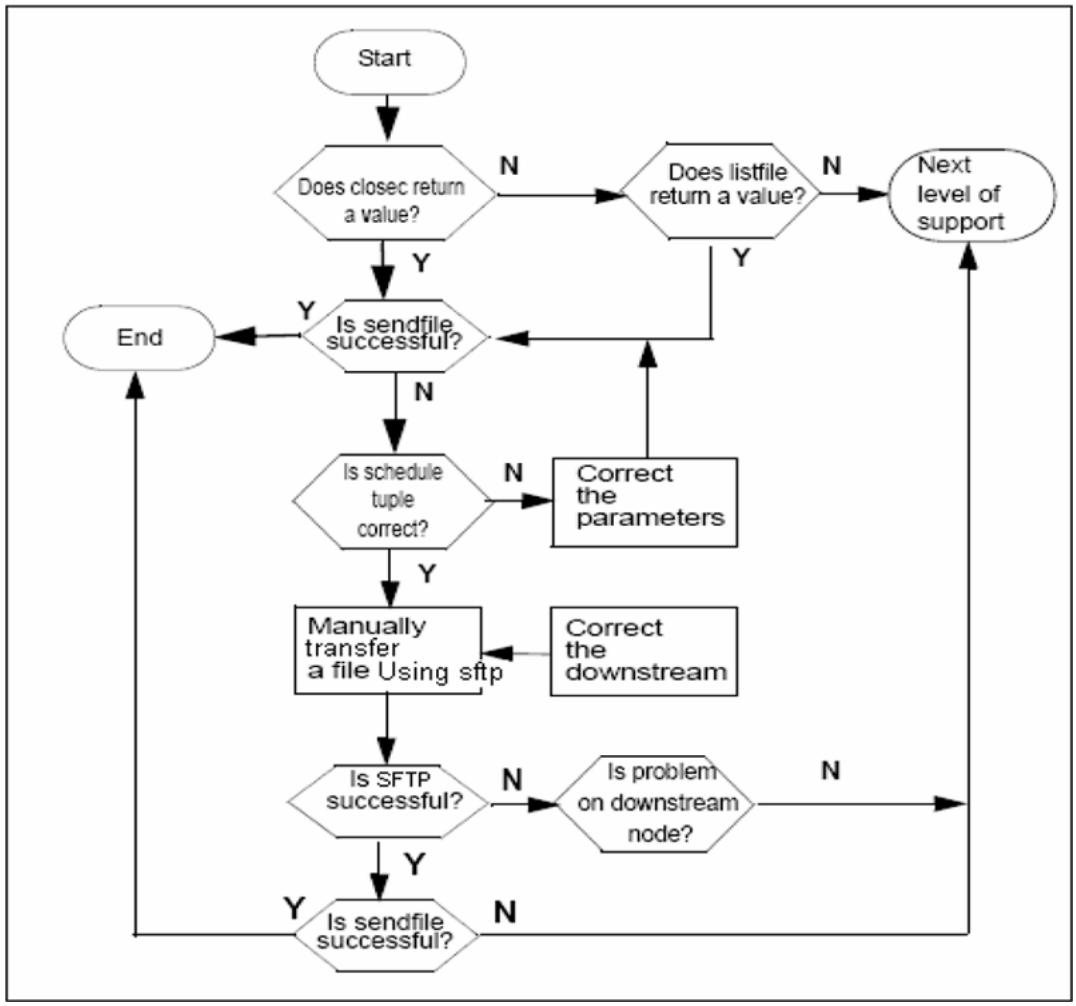
For more information on how to log in to the CBM as an authorized user, how to request a non-restricted shell access, or how to display actions a role group is authorized to perform, review the procedures in the following table.

Procedure	Document
Logging in to the CBM	*Core and Billing Manager 850 Security and Administration*, NN10358-611
Requesting non-restricted shell access	*Core and Billing Manager 850 Security and Administration*, NN10358-611
Displaying actions a role group is authorized to perform	*Core and Billing Manager 850 Security and Administration*, NN10358-611

Action

The following flowchart summarizes the steps outlined in the procedure.

SFTPW verification flowchart



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 file transfer using SFTP

Step	Action

At the core manager

1 Log in to the core manager as a user authorized to perform accounting-admin actions.

2 Access the bill maintenance level:

```
billmtc
```

3 Access the file system:

filesys

4 Close active billing files:

closec <stream_name>

where

<stream_name> is the name of the stream.

ATTENTION
You must close any active billing files prior to the FTP process.

5 Determine the results of the closec command.

If the "closec" command	Do
returns a filename	step 8
does not return a filename	step 6

6 List the primary file (closedNotSent directory):

listfile <stream_name>

where

<stream_name> is the name of the stream

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

8 Send the primary file (closedNotSent directory):

sendfile <stream_name>

where

<stream_name> is the name of the stream.

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

9 Go to the previous level:

quit

10 Determine the results of the sendfile command.

If the "sendfile" command is	Do
successful	you have completed this procedure
not successful	step 11

Observe the SDMB logs on the CM in logutil to determine why the **`sendfile`** command is not successful prior to continuing with step 11.

11 Access the schedule level:

```
schedule
```

12 List the parameters of the schedule tuple:

```
list
```

If the parameters are	Do
correct, but you are receiving an alarm	step 1
incorrect	step 13

13 Reset the schedule tuple parameters:

```
change
```

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

15 Enter the file format.

16 Enter the destination name.

The destination name can be up to 15 alphanumeric characters.

17 Observe the schedule tuple displayed.

18 Enter the corrected parameters.

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

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

20 Save the changed parameters:

```
save
```

If you have	Do
corrected the parameters in the schedule tuple	step 8
determined that the parameters are correct	• step 21 (verify login and write permissions are correct for SFTP process without testing a billing file), OR

- step 24 (verify login and write permissions are correct for SFTP process while testing an actual billing file)

21 Exit the maintenance interface:

```
quit all
```

22 Login as an authorized user.

23 Attempt to transfer any billing file to the destination used by the "sendfile" command using SFTP. This action verifies that SFTP is functioning properly for the node and directory.

You can use any billing file for step 23 because you are only verifying login and write ability on the downstream node.

24 Exit back to the command prompt:

```
quit all
```

25 Login as an authorized user.

26 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

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

27 Access the /tmp directory:

```
cd /tmp
```

28 FTP to the downstream node:

```
sftp <User> @ <address>
```

where

<user> is the SBA user id to login to the downstream destination node
<address> is the Primary_Destination IP address of the destination node

29 Log onto the node when prompted by the FTP (Remote_Login and Remote_Password defined in the schedule tuple):

If the login attempt is unsuccessful, obtain a valid login ID and password and update the schedule tuple with the valid values.

30 Change the directory to the one the schedule tuple is using:

```
sftp> cd <remote_directory>
```

where

<remote_directory> is the Remote_Storage_Directory defined in the schedule tuple.

31 If the "cd" command is unsuccessful, obtain a valid directory from the downstream node and update the schedule tuple with the valid values.

32 Attempt to write a file to the destination node directory used for billing:

```
sftp> put <file> <file.tmp>
```

where

<file> is the name of a billing file that is copied to the /tmp directory in step 26.
<file.tmp> is the name of the billing file with the .tmp extension appended.

33 Rename the <file.tmp> file:

```
sftp> rename <file.tmp> <file>
```

where

<file.tmp> is the name of the billing file with .tmp extension appended that you created in step 32.
<file> is the name of billing file to which the .tmp extension was appended in step 32.

34 Exit from the SFTP session:

```
sftp> quit
```

If the file transfer is	Do
successful	step 37
unsuccessful because of a permission error	step 35
unsuccessful for a reason other than permission error	step 37

35 Correct the directory permissions to allow write access.

36 Repeat steps 1 through 34.

37 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).

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

—End—

Verifying the FTP Schedule

Purpose

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

Prerequisites

You must be a user in a role group authorized to perform accounting-manage actions.

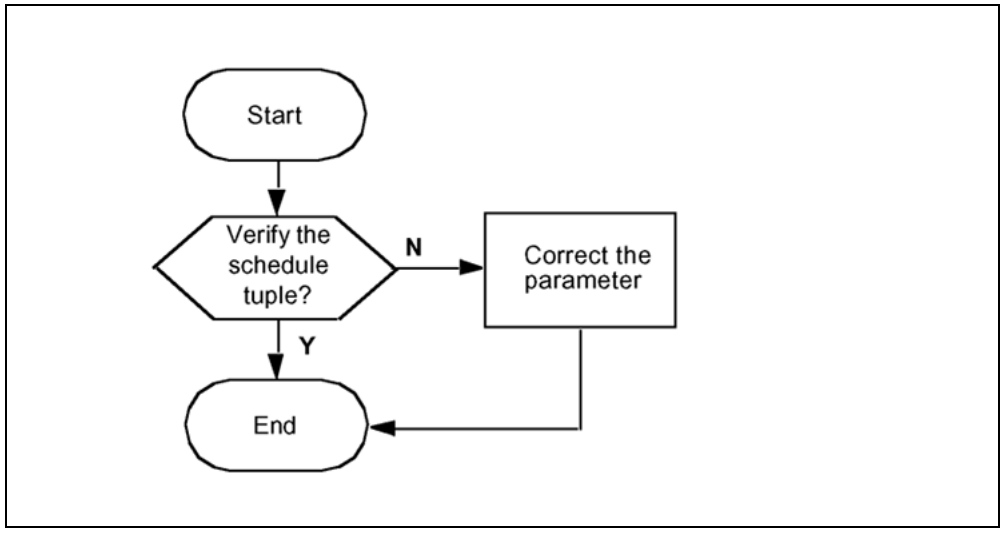
For information on how to log in to the CBM as an authorized user or how to display information about a user or role group, review the procedures in the following table.

Procedure	Document
Logging in to the CBM	*Core and Billing Manager 850 Security and Administration*, NN10358-611
Displaying actions a role group is authorized to perform	*Core and Billing Manager 850 Security and Administration*, NN10358-611

Action

The following flowchart summarizes the steps in the procedure.

Verifying the FTP schedule flowchart



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

Step	Action

At any workstation or console

1 Log in to the core manager.

2 Log in to the core manager as a user authorized to perform accounting-manage actions.

3 Access the bill maintenance level:

```
billmtc
```

4 Verify the schedule tuple:

```
schedule
```

5 List the parameters of the schedule tuple:

```
list
```

If the parameters are	Do
correct	contact your next level of support
incorrect	step 6

6 Reset the schedule tuple parameters:

```
change
```

7 Enter the stream name (billing file name).

8 Enter the file format.

9 Enter the destination name.

The destination name can be up to 15 alphanumeric characters.

10 Observe the schedule tuple displayed.

11 Enter the parameters that you need to correct.

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

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

13 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 14

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

15 You have completed the procedure.

—End—

Verifying the SFTPW/KSFTP Schedule

Purpose

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

Prerequisites

You must be a user in a role group authorized to perform accounting-manage actions.

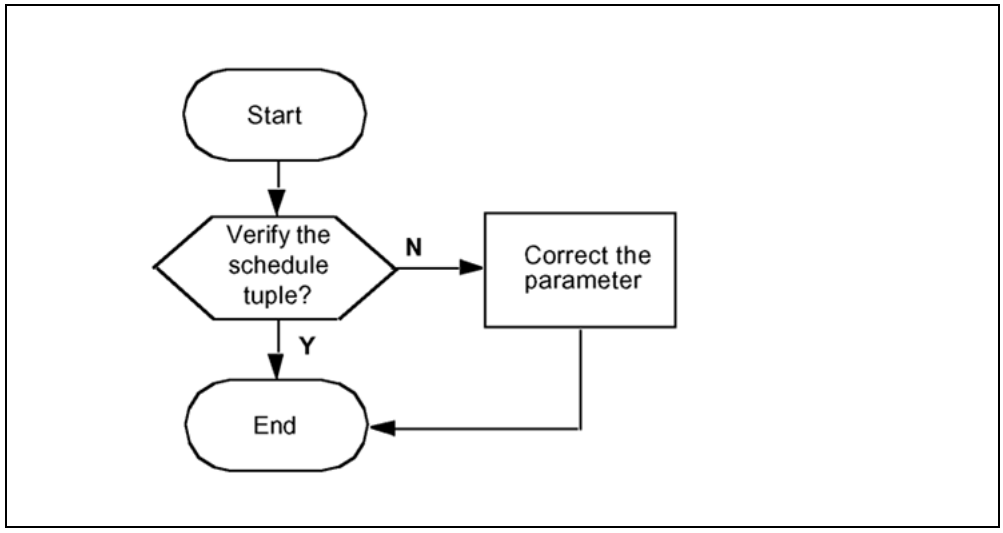
For information on how to log in to the CBM as an authorized user or how to display information about a user or role group, review the procedures in the following table.

Procedure	Document
Logging in to the CBM	*Core and Billing Manager 850 Security and Administration*, NN10358-611
Displaying actions a role group is authorized to perform	*Core and Billing Manager 850 Security and Administration*, NN10358-611

Action

The following flowchart summarizes the steps in the procedure.

Verifying the FTP schedule flowchart



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

Step	Action

At any workstation or console

1 Log in to the core manager as a user authorized to perform accounting-manage actions.

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.

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.

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.

—End—

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 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 reinserting 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 these links for a view of the disks on a Netra t1400 and Netra 240:

- "Netra t1400" (page 212)
- "Netra 240" (page 213)

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

ATTENTION

The steps contained within these procedures change depending on whether the SPFS platform has previously been upgraded. If you are working on an upgraded platform, be sure to pay special attention to the associated notes during the disk replacement procedures.

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

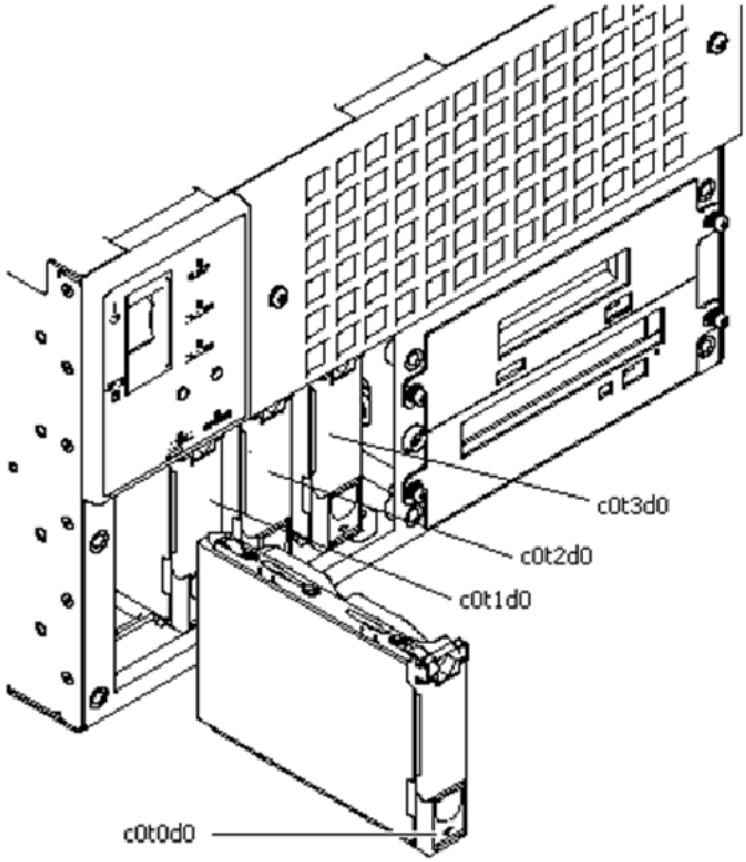
- Replacing failed disks on a Netra t1400
- Replacing failed disks on a Netra 240 simplex
- Replacing failed disks on a Netra 240 cluster (two-server)

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

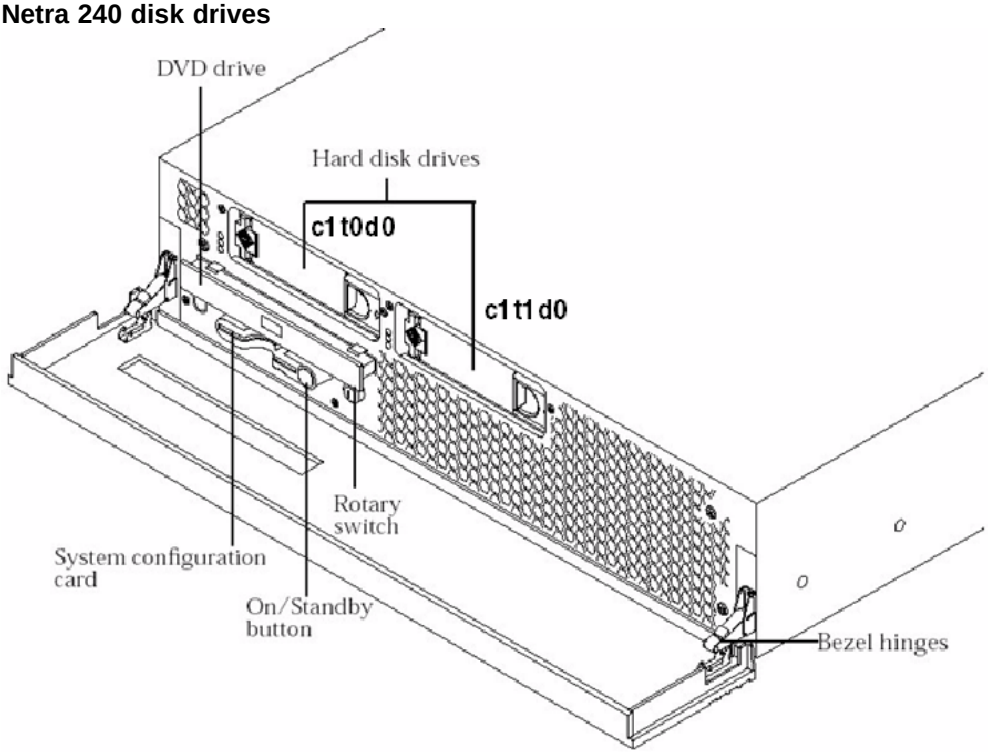


Netra 240

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

This procedure has the following prerequisites:

- The root user ID and password to log into the server.
- Physical access to the server.
- A replacement hard drive of the of the same size as the hard drive being replaced.
- No other maintenance procedure, such as upgrade, or patch application are currently being executed.
- A Phillips screwdriver, if the system is a Netra t1400/t1405.

Prerequisites for Core and Billing Manager 850

In order to perform this procedure, you must have the following authorization and access:

- You must be a user in a role group authorized to perform fault-admin actions.
- You must obtain non-restricted shell access.

For more information about how to log in to the CBM as an authorized user, how to request a non-restricted shell access, or how to display actions a role group is authorized to perform, review the procedures in the following table.

Related procedures

Procedure	Document
Logging in to the CBM	*Core and Billing Manager 850 Security and Administration*, NN10358-611
Requesting non-restricted shell access	*Core and Billing Manager 850 Security and Administration*, NN10358-611
Displaying actions a role group is authorized to perform	*Core and Billing Manager 850 Security and Administration*, NN10358-611

Action

Perform the following steps to complete this procedure.

Replacing failed disks on a Netra t1400

Step Action

At your workstation

1 Log in to the system that is reporting disk or disk mirroring errors as the root user using the system physical IP address.

2 Start the CLI tool by typing "cli" at the shell console.

```
# cli
```

and press the Enter key.

Example response

```
Command Line Interface
1 - View
2 - Configuration
3 - Other
X - exit
select -
```

3 Enter the number next to the "Configuration" option in the menu.

Example response

```
Configuration
1 - NTP Configuration
2 - Apache Proxy Configuration
3 - OAMP Application Configuration
...
14 - Disk Drive Upgrade
15 - Disk Drive Replacement
...
```

```
X - exit
select -
```

4 Enter the number next to the "Disk Drive Replacement" option in the menu.

Example response

```
Disk Drive Replacement
1 - disk_drive_replace (Perform Faulty Disk Drive
Replacement)
X - exit
select -
```

5 Select the number next to the "disk_drive_replace" option in the menu.

Example response

```
=== Executing "disk_drive_replace" ===
INFO: Once the disk replacement is complete, it could
take several hours until full disk redundancy is
restored since all file systems on the new drive must
resync.  Are you sure you want to continue [y,n]?:
```

6 Enter **y** if you want to continue with the disk replacement procedure.

The output provided by the disk replacement utility after specifying **y** will depend on the current status of the system's disks and their configuration which, in turn, depends on many factors. Therefore, the response will probably look different from the following example.

Example response

```
INFO: Initializing disk data:  Success.
INFO: Determining this system's disk configuration
variant:  Success.
INFO: Configuration status for disks:  Results:
- Status for "disk" on "c1t0d0", on "wcars2yh-unit0",
at level "INFO":  - Disk size = 73GB.
- Status for "disk" on "c1t1d0", on "wcars2yh-unit0",
at level "INFO":  - Disk size = 73GB.
- Status for "metadisk" on "c1t1d0", on "wcars2yh-un
it0", at level "WARNING":
- Missing metadb replicas on slice "c1t1d0s7".
- Slice "c1t1d0s5" of submirror "d102" of mirror "d100"
is in "Maintenance" state.
- Slice "c1t1d0s1" of submirror "d1" of mirror "d2" is
in "Maintenance" state.
- Slice "c1t1d0s3" of submirror "d7" of mirror "d8" is
in "Maintenance" state.
- Submirror "d4" is not attached to mirror "d5".
- Submirror "d10" is not attached to mirror "d11".
- Possible orphaned submirror "d10".
```

```
Which disk would you like to replace ("c1t0d0",
"c1t1d0",  "exit"):
```

7 If you would like to abort the disk replacement procedure, enter **exit** otherwise, enter the disk you would like to replace.

Example response

```
Analyzing system state to determine if disk replacement
can proceed:
INFO: Disk replacement can proceed.
Details:
Warnings exist, but they are recoverable.
Do you want to continue with the disk replacement
procedure [y,n]?:
```

8 If the disk analysis detects:

a. A situation that prevents the disk replacement from proceeding, then it will automatically abort this procedure. Call second level support.

b. That disk replacement can continue, then confirm that you would like to continue by entering **y** and pressing the Enter key. The disk replacement utility will take a couple minutes to finish this step.

Example response

```
INFO: Ensuring the mate disk configuration is sane.
Results:
- Status for "metadisk" on "c1t0d0", on "wcars2yh-unit0
", at level "INFO":
- Configured the MetaDisk for target disk:  c1t0d0

INFO: Deconfiguring the target disk "c1t1d0".  Results:
- Status for "disk" on "c1t1d0", on "wcars2yh-unit0",
at level "INFO":
- Deconfigured disk "c1t1d0".
- Status for "metadisk" on "c1t1d0", on "wcars2yh-unit0
", at level "INFO":
- Removed metadb replicas from slice "c1t1d0s7", on
target disk:  "c1t1d0".
- Deleted the concatenation or stripe "d10" defined on
disk "c1t1d0".
- Deleted the concatenation or stripe "d1" defined on
disk "c1t1d0".
- Deleted the concatenation or stripe "d4" defined on
disk "c1t1d0".
- Deleted the concatenation or stripe "d102" defined
on disk "c1t1d0".
Deleted the concatenation or stripe "d7" defined on
disk "c1t1d0".
```

```
Go to the next step in the procedure "Replacing one or
more failed disk drives on an SSPFS-based server" in
the document "NN10408-900" for the necessary steps to
physically replace the faulty hard drive with the new
hard drive.

Enter "y" when you have completed physically
replacing the faulty hard drive to continue with the
configuration of the new hard drive:
```

Generally, if any status is provided at "ERROR" level, then there is a disk configuration or health issue that the disk replacement utility cannot resolve, and the disk replacement procedure must be halted.

If the "ERROR" is that a file system is currently in "Resync" state then you must wait until the file system has finished resynchronizing. This may take a couple hours and depends on the size of the file system being resynchronized as well as system load. You can retry this disk replacement procedure after the file systems are resynchronized.

If any status is provided at "WARNING" level, then there is a disk configuration or health issue but most likely the disk replacement utility can resolve the issue(s), depending on the combination of warnings that it has detected. This analysis step will let you know if the disk replacement can continue.

If there is one warning that states that a file system is in "Maintenance" state, and another warning that states that a file system is in "Last Erred" state, then the disk with the file system in "Maintenance" state must be replaced first and its file systems resynchronized before replacing the hard drive with the file system in "Last Erred" state.

If status is only provided at "INFO" level or if there is no status information, then both disk configuration and health are in good condition.

9 Physically replace the failed disk.

Messages similar to the following might be displayed at the console or in the system logs while replacing the hard drive:

Message 1.
Apr 21 11:39:47 wcars2yh unix: MAJOR ALARM is set
SC Alert: MAJOR ALARM is set

Message 2.
SC Alert: DISK @ HDD0 has been removed.
Apr 27 16:24:44 wcars2yh unix: DISK @ HDD0 has been inserted.
SC Alert: DISK @ HDD0 has been inserted.

Message 3.
Apr 21 11:39:47 wcars2yh root:
/opt/resmon/Hardware/disk_check.ksh: Disk or disk mirroring errors:
See system alarms for details

a. Procedure for Netra 240:

   1. Ensure that you are properly grounded before removing the drive.
   2. Open the front panel of the Netra 240 (refer to figure "Netra 240 disk drives" (page 214)).
   3. Unlatch the hard drive with the blue light lit to its left.
   4. Use the latch as a lever to start removing the hard drive.
   5. Pull the drive the rest of the way out of the SCSI bay.
   6. Ensure the latch on the replacement hard drive is open.
   7. Insert the replacement hard drive completely into the vacant SCSI bay as far as it will go.
   8. Close the latch on the replacement hard drive.
   9. Close the front panel of the Netra 240.

b. Procedure for Netra t1400/t1405:

   1. Ensure that you are properly grounded before removing the drive.
   2. Open the front panel of the Netra t1400/t1405. You will need a phillips screwdriver.
   3. Determine the correct hard drive to replace by referring to the figure "Netra t1400 disk drives" (page 213). While facing the front of the t1400, the hard drives are, from left to right: c0t0d0, c0t1d0, c0t2d0, and c0t3d0.
   4. Unlatch the hard drive identified in the previous step.
   5. Use the latch as a lever to start removing the hard drive.
   6. Pull the drive the rest of the way out of the SCSI bay.
   7. Ensure the latch on the replacement hard drive is open.
   8. Insert the replacement hard drive completely into the vacant SCSI bay as far as it will go.
   9. Close the latch on the replacement hard drive.
   10. Close the front panel of the Netra t1400/t1405. You will need a Phillips screwdriver.

10 Complete the configuration of the new drive by entering y at the prompt. It will take the disk replacement utility a couple minutes to complete this step.

```
INFO: Configuring new hard drive.
Results:
- Status for "disk" on "c1t1d0", on "wcars2yh-unit0",
at level "INFO":
Configured target disk "c1t1d0".
- Status for "metadisk" on "c1t1d0", on "wcars2yh-unit0
", at level "INFO":
- Created metadb replicas on target disk:  c1t1d0
- Configured concatenation or stripe "d102" defined on
target disk "c1t1d0".
- Configured mirror "d100".
- Configured concatenation or stripe "d1" defined on
target disk "c1t1d0".
- Configured mirror "d2".
- Configured concatenation or stripe "d7" defined on
target disk "c1t1d0".
- Configured mirror "d8".
- Configured concatenation or stripe "d4" defined on
target disk "c1t1d0".
- Configured mirror "d5".
- Configured concatenation or stripe "d10" defined on
target disk "c1t1d0".
- Configured mirror "d11".
- Configured the MetaDisk for target disk:  c1t1d0

INFO: The disk replacement procedure has completed
successfully.

=== "disk_drive_replace" completed successfully
```

11 Exit each menu level of the command line interface to eventually return to the command prompt, by typing

```
select - x
```

and pressing the Enter key.

It will take several hours for the file systems on the new hard drive to synchronize. The "SPFS310" alarm will clear in about a minute.

You have completed this procedure.

—End—

Restoring the oracle data on an SPFS-based server

Application

Use this procedure to restore the oracle data from a backup tape or DVD on a Server Platform Foundation Software (SPFS)-based server.Sun Netra t1400 or Sun Netra 240). Also use this procedure to restore the data that was automatically backed up to a file on the server by the backup restore manager.

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)

Restoring the oracle data is not applicable to the MG 9000 Manage or the CBM as they do not use an oracle database.

Prerequisites

You need the tape or DVD on which you backed up the oracle data. If the data was backed up by the backup restore manager, you need the name of the file located in directory /data/bkresmgr/backup.

Action

Perform the following steps to complete this procedure.

Step	Action
	At the server

1 Use the following table to determine how to start this procedure.

If	Start at step
restoring from tape or DVD	step 2
restoring from a file	step 3

2 Insert the tape or DVD on which you backed up the oracle data, into the drive. If restoring the data from a file, start at step 3.

At your workstation

3 Log in to the server.

```
> 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 data restore

4 When prompted, enter your user ID and password.

5 Change to the root user.

```
$ su -
```

and press the Enter key.

6 When prompted, enter the root password.

7 Verify the permissions on the restore log directory (bkslog).

```
# ls -alrt /var/opt/nortel
```

and press the Enter key.

Example response

```
total 22
lrwxrwxrwx   1 root     succssn       28 Dec 22  2003
gwc -> /net/47.141.126.131//swd/gwc
drwxrwxr-x   4 root     other        512 Dec 22  2003 .
drwxr-xr-x   7 root     sys          512
Sep 10 12:41 ..
drwxr-xr-x   2 oracle   oinstall     512
Dec  8 15:58 db
```

```
drwxrwxrwt   2 root     other       6656 Dec
15 19:56 bkslog
```

If the permissions of bkslog	Do
are drwxrwxrwt	step 9
are not drwxrwxrwt	step 8

8 Change the permissions of bkslog.

```
# chmod 1777 /var/opt/nortel/bkslog
```

and press the Enter key.

9 Determine if server applications have been stopped.

```
# servquery -status all
```

and press the Enter key.

10 If not already done, stop the server applications that run on the server.

For	Refer to
CS 2000 Management Tools server applications	Stopping the SESM server application Starting the SAM21 Manager server application Stopping the NPM server application ATM/IP Security and Administration, NN10402-600
MG 9000 Manager and mid-tier server applications	MG 9000 Security and Administration, NN10162-611, if required
IEMS server application	IEMS Security and Administration, NN10336-611, if required

11 Verify the permissions, owner and group of /data/oradata by typing:

```
#ls -l /data
```

and pressing the Enter key.

Example response:

```
drwxr-xr-x   7 oracle   oinstall     512 Oct
16 18:13 oradata
```

12 Use the following table to determine the next step:

If	Go to
permission is "drwxr-xr-x" owner is "oracle" and group is "oinstall" as shown in the example in the previous step	step 14
values do not match the example in the previous step	step 13

13 Change the permission, owner and group of /data/oradata by typing:

`#chmod 755 /data/oradata`

and pressing the Enter key

`#chown oracle /data/oradata`

and pressing the Enter key

`#chgrp oinstall /data/oradata`

and pressing the Enter key

14 Verify the permissions, owner and group of /data/oradata/arch by typing:

`#ls -l /data/oradata`

and pressing the Enter key.

Example response:

```
drwxr-xr-x   4 oracle   oinstall     512
Oct 16 18:36 arch
```

15 Use the following table to determine the next step:

If	Go to
permission is "drwxr-xr-x" owner is "oracle" and group is "oinstall" as shown in the example in the previous step	step 17
values do not match the example in the previous step	step 16

16 Change the permission, owner and group of /data/oradata/arch by typing:

`#chmod 755 /data/oradata/arch`

and pressing the Enter key

`#chown oracle /data/oradata/arch`

and pressing the Enter key

```
#chgrp oinstall /data/oradata/arch
```

and pressing the Enter key

17 Use the following table to determine your next step.

If	Do
restoring from tape or DVD	step 18
restoring from a file	step 20

18 Restore the database from backup tape or DVD.

```
$ /opt/nortel/SPFS/bks/rsdata
```

and press the Enter key.

19 Remove the tape from the drive, or eject the DVD from the drive as follows:

a. Ensure you are at the root directory level.

```
# cd /
```

and press the Enter key.

b. Eject the DVD.

```
# eject cdrom
```

and press the enter key.

If the DVD drive tray does 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
```

Press the eject button located on the front of the DVD drive.

c. Remove the DVD from the drive.

Proceed to step 21.

20 Restore the database from the backup file.

```
$ /opt/nortel/SPFS/bks/rsdata -f /data/bkresmgr/backup
/<filename>
```

and press the Enter key.

Variable	Value
<filename>	is the name of the backup file created by the backup restore manager

21 Verify that the database restored properly.

```
# queryAllFaults
```

and press the Enter key.

If an alarm appears like the following, the database was not restored properly:

```
*** SPFS330 Import of Oracle data caused corruption
ORA-22337:  Error importing Oracle data cs2kaps=rtp6ba
ckupsesm;NODE=rtp6backupsesm;CLASS=SW;SWTYPE=Database
Fri Jun 10 15:48:59 2005
```

22 Use the information in the following table to determine the next step.

If	Do
no alarm appears	step 23
alarm appears	contact Nortel
the database did not restore properly	contact Nortel

23 Use the following table to determine your next step.

If	Do
WebPKProxy is configured	step 24
WebPKProxy is not configured	step 27

24 Restore the WebPKProxy.

```
# ls /data/pkclient/certificates
```

and press the Enter key.

25 Use the following table to determine your next step.

If	Do
the following files are associated with this machine: • CA1_Cert.pem • CA2_Cert.pem • TRUSTED_Cert.pem	step 26
the above files do not exist	step 27

26 Reconfigure WebPKProxy as follows:

a. From the CLI, select Configuration ---> Security Services Configuration ---> Certificate Manager Certificate Installation ---> install_certs.

Wait for the script to complete. Verify that no errors displayed.

b. From the CLI, select Configuration ---> Security Services Configuration ---> WebPKProxy/PKClient---> register_pkclient.

c. Enter the host name of the Certificate Manager.

The Certificate Manager box must be fully functional for this step to succeed.

Wait for the script to complete. Verify that no errors displayed.

27 Start the server applications that run on the server.

For	Refer to
CS 2000 Management Tools server applications	Stopping the SESM server application Starting the SAM21 Manager server application Stopping the NPM server application ATM/IP Security and Administration, NN10402-600
MG 9000 Manager and mid-tier server applications	the MG 9000 Security and Administration document, NN10162-611, if required
IEMS server application	the IEMS Security and Administration document, NN10336-611, if required

If one or more applications do not start, contact Nortel for assistance.

You have completed tis procedure.

—End—

Changing a user password on an SPFS-based server

Application

Use this procedure to change a user password on a Server Platform Foundation Software (SPFS)-based server.

ATTENTION

User accounts and passwords are automatically propagated from the active server to the inactive server in a high-availability (two-server) configuration to allow users to log in to either server. However, user files are not propagated to the other server.

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.

Step	Action
	At your workstation
1	Log in to the Active server by typing `> telnet <server>` and pressing the Enter key. where **`server`** is the IP address or host name of the SPFS-based server In a two-server configuration, log in to the active server using its physical IP address.
2	When prompted, enter your user ID and password.
3	Change to the root user by typing
4	When prompted, enter the root password.
5	Change the password for a specific user by typing `# passwd -r files <userid>` and pressing the Enter key. where

`userid` is a variable for the user's login identification

6 When prompted, enter a password of at least three characters.

It is not recommended to set a password with an empty value. Use a minimum of three characters.

7 When prompted, enter the password again for verification.

You have completed this procedure.

—End—

Logging in to the CBM

Purpose

Use this procedure to log in to the CBM.

Prerequisites

You must have a valid userID to log in to the CBM. Your userID can be either defined locally on the CBM, or in a centralized security server if the CBM is configured to authenticate with a centralized security server.

For more information on how to log in to the CBM as an authorized user, how to request a non-restricted shell access, or how to display actions a role group is authorized to perform, review the procedures in the following table.

Procedures related to this procedure

Procedure
Requesting non-restricted shell access
Adding, changing, or removing a user to or from a role group
Displaying actions a role group is authorized to perform
Displaying users of a role group or all role groups
Displaying information for a user or all users

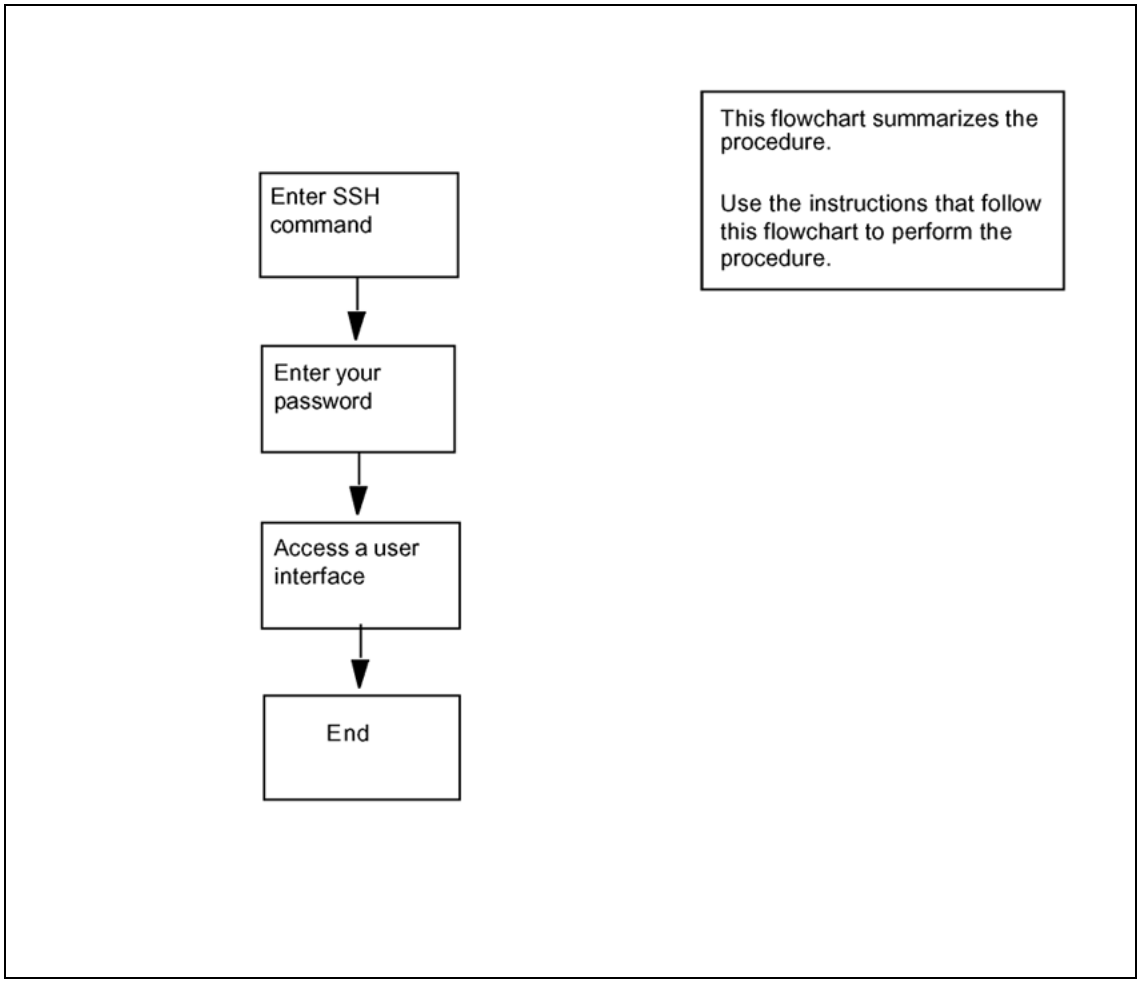
Application

It is recommended that you log in to the CBM through SSH (secure shell) using a password.

Procedure

The following flowchart provides an overview of the procedure. Use the instructions in the step-action procedure that follows the flowchart to perform the task.

Summary of Logging in to the CBM



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.

Logging in to the CBM

Step	Action

At the remote shell

1 Log in to the core manager using one of the following commands for SSH access:

```
> ssh <userID> @ <IPaddress | hostname>
```

or

```
> ssh -l <userID> <IPaddress | hostname>
```

where

<userID> is your userID
<IPaddress> is the IP address of the CBM
<hostname> is the host name for the CBM

Example response:

```
Don_secu's Password:
```

2 Enter your password.

3 Access a user interface, for example, access the maintenance interface:

```
cbmmtc
```

4 Exit the maintenance interface:

```
quit all
```

5 You have completed this procedure.

—End—

Shutting down an SPFS-based server

Application

Use this procedure to shut down a 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)

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 preceding components, therefore, ensure it is acceptable to shut down the server.

Prerequisites

You must have root user privileges.

Perform this procedure from a console only.

Prerequisites for Core and Billing Manager 850

In order to perform this procedure, you must have the following authorization and access:

- You must be a user in a role group authorized to perform fault-admin actions. Therefore, Step 3 and Step 9 are not required.
- You must obtain non-restricted shell access.

For more information about how to log in to the CBM as an authorized user, how to request a non-restricted shell access, or how to display actions a role group is authorized to perform, review the procedures in the following table.

Related procedures

Procedure	Document
Logging in to the CBM	*Core and Billing Manager 850 Security and Administration*, NN10358-611
Requesting non-restricted shell access	*Core and Billing Manager 850 Security and Administration*, NN10358-611
Displaying actions a role group is authorized to perform	*Core and Billing Manager 850 Security and Administration*, NN10358-611

Action

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

- "One-server configuration" (page 235)
- "Two-server (cluster) configuration" (page 236)

One-server configuration

Step	Action

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.

—End—

Two-server (cluster) configuration

Step	Action

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.

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.

ATTENTION
Only perform the remaining steps if you want to perform a full power down, which involves powering down both servers in the cluster.

7 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.

—End—

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 DVD-RW to use it again.

Prerequisites for Core and Billing Manager 850

All users with non-restricted shell access are authorized to perform this procedure.

You require root-user access, or must be a user in a role group authorized to perform config-admin actions, if an error occurs when ejecting a DVD.

For more information about how to log in to the CBM as an authorized user, how to request non-restricted shell access, or how to display actions a role group is authorized to perform, review the procedures in the following table.

Related procedures

Procedure	Document
Logging in to the CBM	*Core and Billing Manager 850 Security and Administration*, NN10358-611
Requesting non-restricted shell access	*Core and Billing Manager 850 Security and Administration*, NN10358-611
Displaying actions a role group is authorized to perform	*Core and Billing Manager 850 Security and Administration*, NN10358-611

Action

Perform the following steps to complete this procedure.

Step	Action
	At the server
1	Insert the DVD into the drive. 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 -l
```

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

ATTENTION

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 -l
```

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.

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, re-try the "eject cdrom" command.

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.

—End—

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 Server Platform Foundation Software (SPFS)-based server:

- "Simplex configuration (one server)" (page 243)
- "High-availability configuration (two servers)" (page 246)

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

The 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 following table lists the file systems that cannot be increased, and lists examples of those that can be increased.

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 procedures "Performing a backup of oracle data on an SPFS-based server" (page 258) and "Performing a backup of file systems on an SPFS-based server" (page 253) if required.

Action

Perform the following steps to complete this procedure.

Simplex configuration (one server)

Step	Action

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. You may log on as root or emsadm.

3 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 - SPFS_soft (Display Software
      Installation Level Of SPFS)
  2 - chk_SPFS (Check SPFS 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_uti’" option in the menu.

Example response

```
Filesystem             size   used  avail capacity  Mounted on
/dev/md/dsk/d2         3.9G   1.6G   2.3G    42%    /
/proc                    0K     0K     0K     0%    /proc
mnttab                   0K     0K     0K     0%    /etc/mnttab
fd                       0K     0K     0K     0%    /dev/fd
/dev/md/dsk/d8         2.0G    86M   1.8G     5%    /var
swap                   2.5G   160K   2.5G     1%    /var/run
swap                   512M   3.8M   508M     1%    /tmp
/dev/md/dsk/d11        4.9G   1.5G   3.4G    32%    /opt
/dev/md/dsk/d21        2.9G   111M   2.8G     4%    /opt/nortel
/dev/md/dsk/d22        5.9G   145M   5.7G     3%    /var/mysql/data
/backup                3.9G   4.0M   3.9G     1%    /backup
/data                  2.9G   5.9M   2.9G     1%    /data
/data/oradata          9.8G   2.5G   7.3G    26%    /data/oradata
/data/oradata/arch     963M    12M   893M     2%    /data/oradata/arch
/data/qca              9.8G    10M   9.7G     1%    /data/qca
```

The ‘capacity’ column indicates the percentage of disk utilization by the file system, which is specified in the ‘Mounted on’ column.

4 Note the file system you want to increase, as well as its current size (under column ’size’).

5 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.

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.

6 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 “data/oradata” file system, subtract its current size, 10337 MB from the desired size, for example, 15000 MB. You would increase the size of the “data/oradata” file system by 4662786 KB, or 4663 MB.

7 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 free_space
```

and pressing the Enter key.

Divide the resulting number by 2048 to determine 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 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 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 9 a (amount of free disk space you can allocate to file systems)	step 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.

8 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
```

The preceding example increases the '/data' file system by 512 megabytes (MB).

You have completed this procedure.

—End—

ATTENTION
During this procedure, the cluster will be running without a standby node. The duration is estimated at approximately one hour.

High-availability configuration (two servers)

Step Action

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

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.

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

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 8
ClusterIndicatorACT	step 2

8 Verify the status of file systems on this server by typing

```
# udstat
```

and pressing the Enter key.

If the file systems are	Do
STANDBY normal UP clean	step 9
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 - SPFS_soft (Display Software
      Installation Level Of SPFS)
  2 - chk_SPFS (Check SPFS 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

```
Filesystem             size   used  avail capacity  Mounted on
/dev/md/dsk/d2         3.9G   1.6G   2.3G    42%    /
/proc                    0K     0K     0K     0%    /proc
mnttab                   0K     0K     0K     0%    /etc/mnttab
fd                       0K     0K     0K     0%    /dev/fd
/dev/md/dsk/d8         2.0G    86M   1.8G     5%    /var
swap                   2.5G   160K   2.5G     1%    /var/run
swap                   512M   3.8M   508M     1%    /tmp
/dev/md/dsk/d11        4.9G   1.5G   3.4G    32%    /opt
/dev/md/dsk/d21        2.9G   111M   2.8G     4%    /opt/nortel
/dev/md/dsk/d22        5.9G   145M   5.7G     3%    /var/mysql/data
/backup                3.9G   4.0M   3.9G     1%    /backup
/data                  2.9G   5.9M   2.9G     1%    /data
/data/oradata          9.8G   2.5G   7.3G    26%    /data/oradata
/data/oradata/arch     968M    12M   893M     2%    /data/oradata/arch
/data/qca              9.8G    10M   9.7G     1%    /data/qca
```

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 ’size’).

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.

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.

12 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, 123 MB from the desired size, for example, 256 MB. You would increase the size of the ‘qca’ file system by 133153 KB, or 133 MB.

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

# /opt/nortel/sspfs/fs/meta.pl free_space
/ 5000 - p | dc
```

and pressing the Enter key.

Divide the resulting number by 2048 to determine 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 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 12 (size by which to increase the file system) is greater than the value you obtained in step 13 a (amount of free disk space you can allocate to file systems)	contact Nortel for assistance
the value you determined in step 12 (size by which to increase the file system) is less than the value you obtained in step 13 a (amount of free disk space you can allocate to file systems)	step 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.

14 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
```

The preceding example increases the '/data/qca' file system by 10 megabytes (MB).

15 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 16
otherwise	repeat step 15 until the file systems are "STANDBY normal UP clean".

16 Reboot the Inactive node by typing

```
# init 6
```

and pressing the Enter key.

Wait for the unit to recover before proceeding.

17 Perform a swact on the active unit by typing

```
# swact
```

and pressing the Enter key.

This action causes a cluster failover and makes the active node inactive, and the inactive node active.

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.

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 *ClusterIndicator*ACT, which indicates you are on the Active server.

22 Verify all applications are running on the active node by typing

```
# servquery -status all
```

and pressing the Enter key.

Verify all applications are running.

23 Verify all replicated file systems are "active up normal" by typing

```
# udstat
```

and press the Enter key.

Ensure all file systems are in the "active up normal" state.

24 Clone the other node using procedure "Cloning the image of one server in a cluster to the other server", ensuring you log into the active node.

You have completed this procedure.

—End—

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 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 (MG) 9000 Manager
- Network Patch Manager
- Core Billing Manager (CBM)

Prerequisites

This procedure has the following prerequisites:

- You must perform a data backup prior to performing this procedure. Refer to procedure "Performing a backup of oracle data on an SPFS-based server" (page 258) to complete this task.

  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 Sun Netra 240, use one or more blank CD-R, CD-RW, DVD-R or DVD-RW disks to store the data

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

  If you are using a new CD-RW or DVD-RW, or want to reuse a used CD-RW or 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.

Prerequisites for Core and Billing Manager 850

In order to perform this procedure, you must have the following authorization and access:

- You must be a user in a role group authorized to perform config-admin actions.

- You must obtain non-restricted shell access.

For CBM 850, root user ID and password are not required. Therefore, you are not required to change to the root user in steps 4 and 5 of this procedure.

For more information about how to log in to the CBM as an authorized user, how to request a non-restricted shell access, or how to display actions a role group is authorized to perform, review the procedures in the following table.

Procedure	Document
Logging in to the CBM	*Core and Billing Manager 850 Security and Administration*, NN10358-611
Requesting non-restricted shell access	*Core and Billing Manager 850 Security and Administration*, NN10358-611
Displaying actions a role group is authorized to perform	*Core and Billing Manager 850 Security and Administration*, NN10358-611

Action

ATTENTION
In a two-sever configuration, execute this procedure on the Active server.

Step	Action

At the server

1 Insert the blank tape or 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 7
a CD or DVD for backup	step 8

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
```

When using a 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 10
a CD or DVD for backup	step 12

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 content of the CD or DVD by typing

```
# gtar -tvMf /cdrom/*bkfullsys*/*.tar
```

and pressing the Enter key.

If you	Do
receive a prompt to prepare another volume	step 14
do not receive a prompt to prepare another volume	step 16

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, retry the eject cdrom command previously shown and press the Enter key.

18 Remove the DVD from the drive, label it, and store it in a safe place.

If the backup	Do
resides on multiple DVDs	Insert the next backup DVD in the disk drive and go to step 13
resides on a single DVD	step 19

19 You have completed this procedure. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

—End—

Performing a backup of oracle data on an SPFS-based server

Application

Use this procedure to perform a backup of oracle data on a 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 (MG) 9000 Manager

  An oracle data backup is not required when the SPFS-based server is hosting the MG 9000 Manager.
- Network Patch Manager (NPM)
- Core and Billing Manager (CBM)

An oracle data backup is not required when the SPFS-based server is hosting the CBM.

If the SPFS-based server is hosting the IEMS, it is highly recommended to purge the IEMS event and performance data prior to executing the data backup. This reduces the size of the oracle space used by the IEMS, and therefore, reduces the backup time, and possibility of a backup failure. The purge capability is only available in (I)SN07 onward.

If the SPFS-based server is hosting the IEMS, it is highly recommended to purge the IEMS event and performance data prior to executing the data backup. This reduces the size of the oracle space used by the IEMS, and therefore, reduces the backup time, and possibility of a backup failure. The purge capability is only available in (I)SN07 onward.

Refer to the procedure ‘Configuring dark office backups on an SPFS-based server’ in ATM/IP Solution-level Configuration Management, NN10409-500.

ATTENTION

It is recommended that provisioning activities be put on hold during the time of the data backup.

Prerequisites

This procedure has the following prerequisites:

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

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

  If you are using a new CD-RW or DVD-RW, or want to reuse an CD-RW or DVD-RW by erasing the contents, perform procedure 'Preparing a CD-RW or DVD-RW for use' in *ATM/IP Security and Administration document*, NN10402-600Packet MSC Security and Administration (NN20000-216).

ATTENTION

The database must be in sync with the Communication Server 2000 and the MG 9000 Manager (if present). Therefore, ensure you have the appropriate image of both before you proceed. Performing a restore from the Oracle database alone can cause data mismatches at the Communication Server 2000 and the MG 9000 Manager (if present).

Action

ATTENTION

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

Step	Action
	At the server
1	Insert the blank tape, CD or DVD into the drive. In a two-server configuration, insert the blank CD or DVD into the drive of 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 hostname of the SPFS-based server on which you want to perform 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.

6 If the server is hosting the IEMS, and you want to purge the event and performance data, do step step 7, otherwise proceed to step 10.

ATTENTION
This step stops the IEMS server. Ensure it is acceptable at this time to stop the IEMS server application.

7 Stop the IEMS server by typing:

```
# servstop IEMS
```

and pressing the Enter key.

8 Run the script to purge the data by typing

```
# /opt/nortel/iems/current/bin/purgeTempData.sh
```

and pressing the Enter key.

9 Start the IEMS server by typing

```
# servstart IEMS
```

and pressing the Enter key.

10 Use the following table to determine your next step.

If you are using	Do
a tape for backup	step 11
a CD or DVD for backup	step 12

11 Rewind the tape by typing

```
# mt -f /dev/rmt/0 rewind
```

and pressing the Enter key.

12 Back up the data by typing

$ /opt/nortel/SPFS/bks/bkdata

and pressing the Enter key.

Example response:

```
Backup Completes Successfully
```

13 Use the following table to determine your next step

If you are using	Do
a tape for backup	step 13
a CD or DVD for backup	step 16

14 List the content of the tape by typing

 # tar tvf /dev/rmt/0

and pressing the Enter key.

Example response:

```
-rw-rw-rw- 0/1 1874917 Mar 2 10:16 2005 opt/oracle.dmp
.gz
-rw-rw-rw- 0/1 1007616 Mar 2 10:16 2005 opt/critdata.c
pio
```

15 Remove the tape from the drive, label it, write-protect it, and store it in a safe place. Proceed to step 21

16 Reinsert the backup CD or DVD into the drive.

17 List the content of the CD or DVD by typing

 # tar tvf /cdrom/*bkdata*/*.tar

and pressing the Enter key.

Example response:

```
-rw-rw-rw- 0/1 1874917 Mar 2 10:17 2005 opt/oracle.dmp
.gz
-rw-rw-rw- 0/1 1007616 Mar 2 10:17 2005 opt/critdata.c
pio
```

When a DVD backup spans more than one disk, all the DVDs with the exception of the last one produce a file error during the verification process. This error message does not interfere with the backup process but can reappear several times as the backup spans multiple disks.

18 Ensure you are at the root directory level by typing

 # cd /

and pressing the Enter key.

19 Eject the CD by typing

```
# eject cdrom
```

and pressing the Enter key.

If the DVD drive tray does 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 in the order listed:

```
# /etc/init.d/volmgt stop
```

```
# /etc/init.d/volmgt start
```

Then press the eject button located on the front of the DVD drive.

20 Remove the CD or DVD from the drive, label it, and store it in a safe place.

21 You have completed this procedure. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

To restore the data from tape or CD/DVD, refer to procedure "Restoring the oracle data on an SPFS-based server" in *ATM/IP Security and Administration*, NN10402-600.

—End—

Verifying disk utilization on an SPFS-based server

Application

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

Prerequisites

You must have root user privileges.

Action

Perform the following steps to complete this procedure.

Step	Action
	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 - exits`
	`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 - SPFS_soft (Display Software
      Installation Level Of SPFS)
  2 - chk_SPFS (Check SPFS 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

```
Filesystem             size   used  avail capacity  Mounted on
/dev/md/dsk/d2         3.9G   1.6G   2.3G    42%    /
/proc                    0K     0K     0K     0%    /proc
mnttab                   0K     0K     0K     0%    /etc/mnttab
fd                       0K     0K     0K     0%    /dev/fd
/dev/md/dsk/d8         2.0G    86M   1.8G     5%    /var
swap                   2.5G   160K   2.5G     1%    /var/run
swap                   512M   3.8M   508M     1%    /tmp
/dev/md/dsk/d11        4.9G   1.5G   3.4G    32%    /opt
/dev/md/dsk/d21        2.9G   111M   2.8G     4%    /opt/nortel
/dev/md/dsk/d22        5.9G   145M   5.7G     3%    /var/mysql/data
/backup                3.9G   4.0M   3.9G     1%    /backup
/data                  2.9G   5.9M   2.9G     1%    /data
/data/oradata          9.8G   2.5G   7.3G    26%    /data/oradata
/data/oradata/arch     968M    12M   893M     2%    /data/oradata/arch
/data/qca              9.8G    10M   9.7G     1%    /data/qca
```

You have completed this procedure.

—End—

Replacing a DVD drive on an SPFS-based server

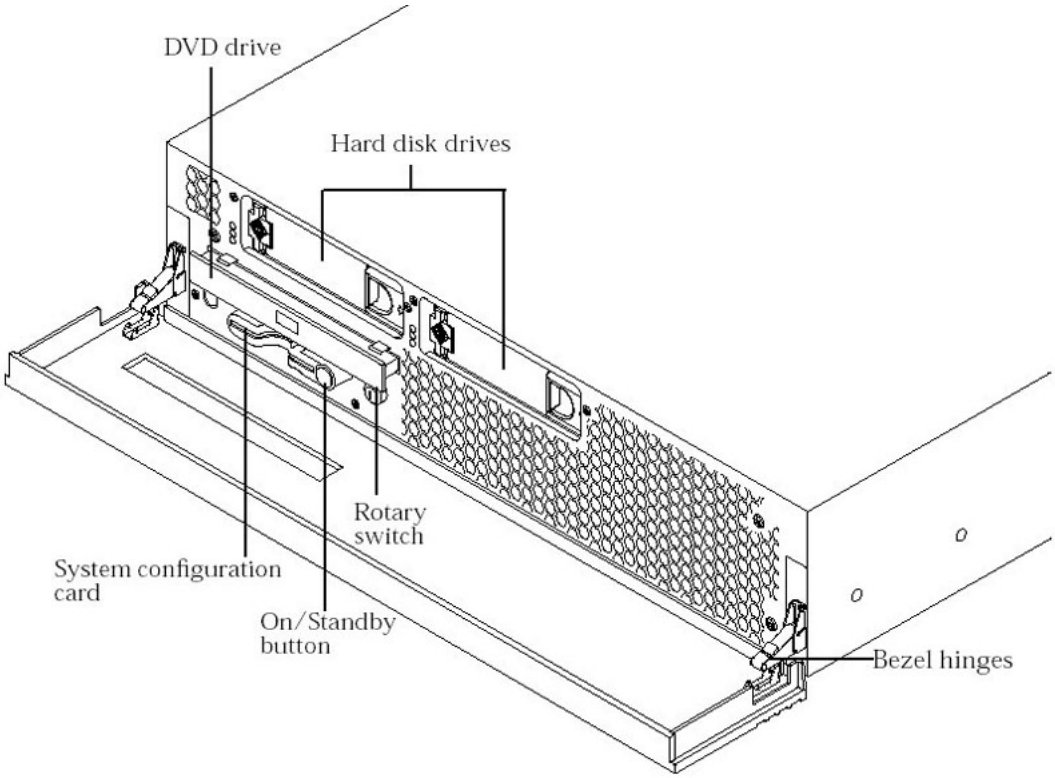
Application

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 following methods according to your office configuration:

- "Simplex configuration (one server)" (page 266)
- "High-availability configuration (two servers)" (page 266)

Prerequisites

None.

Action

Simplex configuration (one server)

Step	Action

At your workstation

1 Power down the server. Refer to procedure "Shutting down an SPFS-based server" (page 234) 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.

—End—

High-availability configuration (two servers)

Step	Action

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. Refer to procedure "Initiating a manual failover on a Sun Netra 240 server pair" (page 268) if required.

3 Once the active server acquires the status of standby (inactive), power down the server. Refer to procedure "Shutting down an SPFS-based server" (page 234) 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.

—End—

Initiating a manual failover on a Sun Netra 240 server pair

Application

Use this procedure to initiate a manual failover on a Sun Netra 240 server pair. Initiating a manual failover can be required in the following situations:

- general maintenance
- software update without a data schema or configuration change

The failover causes the standby (inactive) server to take over and start providing OAM&P services as the new active server.

ATTENTION
During an automatic or manual failover, the high-availability (HA) cluster takes approximately 5 minutes to failover and bring up the standby node to Active state.

Prerequisites

You must perform this procedure on the active node.

Action

Perform the following steps to complete this procedure.

ATTENTION
Perform the steps that follow on the Active server.

Step	Action
	At the active node console
1	Log in to the active node through the console (port A) using the root user ID and password. Ensure you are on the Active server by typing ubmstat. If *ClusterIndicatorSTBY* is displayed in the response, which indicates you are on the Inactive server, log out of that server and log in to the other server in the pair. The response must display *ClusterIndicatorACT*, which indicates you are on the Active server.
2	Initiate the manual failover by typing # **`swact`** and pressing the Enter key. *Example response*

```
Are you sure you want to initiate a cluster failover?
[Y/N]
```

3 If it is acceptable to initiate a manual failover, indicate you want the failover to occur by typing

y

and pressing the Enter key.

You have completed this procedure.

—End—

Viewing customer logs on an SPFS-based server

Application

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

- Succession Element and Sub-element Manager (SESM)
- Gateway Controller (GWC)
- Server Platform Foundation Software (SPFS)

Use this procedure to view customer logs for the CS 2000 Management Tool server.

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.

Step	Action
	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 tying `$ 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.

—End—

Canceling a running remote backup process

Application

Use this procedure to cancel an existing remote backup process.

Prerequisites

This procedure has no prerequisites.

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

Action

Perform the following steps to complete this procedure.

Step	Action
	At your workstation
1	Establish a connection to the server that is hosting the CS 2000 Management Tools through telnet or SSH, and log in using the root user ID and password. In a two-server configuration, log in to the active server using the physical IP address of the active server, and ensure you are on the active server using the `ubmstat` command. For detailed steps, refer to procedure "Logging in to an SPFS-based server".
2	Launch the command line interface tool by typing `# cli` and pressing the Enter key.
3	From the resulting menu, select the number against the “Configuration” menu option, and press the Enter key.

4 From the resulting menu, select the number against the “Remote Backup Configuration” menu option, and press the Enter key.

5 From the resulting menu, select the number against the “rbackup_cancel (Cancel Running Remote Backup)” menu option, and press the Enter key.

Example response

```
=== Executing "rbackup_cancel"
cleaning up files
unmounting /tmp/.snap/var /tmp/.snap/user_audio_files
/tmp/.snap/opt/nortel /tmp/.snap/opt /tmp/.snap/data/
qca
/tmp/.snap/data/oradata/arch /tmp/.snap/data/oradata
/tmp/.snap/data
/tmp/.snap/backup /tmp/.snap
removing scratch /tmp/.backing_store d99
=== "rbackup_cancel" execution completed
```

6 Exit each menu level of the command line interface tool by typing

```
select - x
```

and pressing the Enter key.

7 You have completed this procedure.

—End—

Logging in to an SPFS-based server

Application

Use this procedure to log into a Server Platform Foundation Software (SPFS) server. This procedures provides the steps to establish a login session using SSH, which is secure, or telnet, which is not secure.

Some tasks will require that you log in to the server through the console (port A) using the root user ID and password.

Prerequisites

This procedure requires the following information:

- the IP address or host name of the server

  In a two-server configuration, you need the physical IP address of the active or inactive server.
- a valid user id and password
- the root password if you need to perform a task on the server that requires root user privileges

Action

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

- Logging in using SSH
- Logging in using Telnet
- Logging in through the console

Logging in using SSH

Step	Action

At your workstation

1 Establish an SSH session.

If you have access to a workstation which supports the ssh command (Linux, for example) then proceed with step a.

Otherwise, connect to the server using an SSH client and proceed to step 2.

a. Establish an SSH session to the server by typing

```
> ssh -l <user_id> <server>
```

where

user_id is root or your user id
server is the IP address or host name of the SPFS-based server, or the physical IP address of the active or inactive server as required, in a two-server configuration

2 Use the following table to determine your next step.

If you receive	Do
a message indicating a host authentication issue and a request to continue the connection	step 3
a prompt for a password	step 4

ATTENTION
The prompt indicates SSH is verifying whether the server is a trusted host for the workstation. SSH performs the verification the first time SSH is run on a workstation.

3 Continue the connection by typing

```
y
```

and pressing the Enter key.

4 Enter the password for root or your user id and press the Enter key.

5 Use the following table to determine your next step.

If your server is a	Do
one-server configuration	step 9
two-server configuration	step 6

6 Ensure you are on the correct server by typing

```
# ubmstat
```

and pressing the Enter key.

7 Use the following table to determine your next step.

If you need to be on the	Do
active server and the response is ClusterIndicatorSTBY	step 8
inactive server and the response is ClusterIndicatorACT	step 8

If you need to be on the	Do
active server and the response is ClusterIndicatorACT	step 9
inactive server and the response is ClusterIndicatorSTBY	step 9

8 You are logged in to the wrong server. Return to step 1 to log in to the other server.

9 You have completed this procedure.

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

—End—

Logging in using Telnet

Step Action

At your workstation

1 Establish a telnet session 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, or the physical IP address of the active or inactive server in a two-server configuration

2 When prompted, enter your userid.

ATTENTION
You cannot log in using the root userid at this step.

3 When prompted, enter your password.

4 Use the following table to determine your next step.

If	Do
you need to log in as root	step 5
otherwise	step 7

5 Change to the root user by typing

```
$ su -
```

and pressing the Enter key.

6 When prompted, enter the root password.

7 Use the following table to determine your next step.

If your server is a	Do
one-server configuration	step 11
two-server configuration	step 8

8 Ensure you are on the correct server by typing

```
# ubmstat
```

and pressing the Enter key.

9 Use the following table to determine your next step.

If you need to be on the	Do
active server and the response is ClusterIndicatorSTBY	step 10
inactive server and the response is ClusterIndicatorACT	step 10
active server and the response is ClusterIndicatorACT	step 11
inactive server and the response is ClusterIndicatorSTBY	step 11

10 You are logged in to the wrong server. Log out of this server and return to step 1 to log in to the other server.

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

—End—

Logging in through the console

Step	Action

At the console connected to the server

1 Log in to the server through the console (port A) using the root user ID and password. In a two-server configuration, log in to the active or inactive server as required.

2 Use the following table to determine your next step.

If your server is a	Do
one-server configuration	step 6
two-server configuration	step 3

3 Ensure you are on the correct server by typing

```
# ubmstat
```

and pressing the Enter key.

4 Use the following table to determine your next step.

If you need to be on the	Do
active server and the response is ClusterIndicatorSTBY	step 5
inactive server and the response is ClusterIndicatorACT	step 5
active server and the response is ClusterIndicatorACT	step 6
inactive server and the response is ClusterIndicatorSTBY	step 6

5 You are logged in to the wrong server. Log out of this server and return to step 1 to log in to the other server.

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

—End—

Configuring Client/Server Ports on an SPFS-Based Server for Secure Firewall Communications

Use this procedure to configure the client-side and server-side ports.

Application

Use this procedure to configure the client-side and server-side ports on a Server Platform Foundation Software (SPFS) based server to facilitate secure firewall communication between client and server applications. You can also use this procedure to list the ports that are currently configured.

ATTENTION

The server-side port has a default value of 10080, and the client-side port has a default value of 10090. If the default value is acceptable, it is not necessary to configure the ports.

Prerequisites

The server-side port must have the same value across all offices in the network. If the ports do not have the same value, the client application GUIs will fail to launch.

Action

Perform the following steps to complete this procedure.

Configure the client- and server-side ports on an SPFS server

Step	Action

At your workstation:

1 Telnet 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.

Response

```
Command Line Interface
 1 - View
2 - Configuration
3 - Other
X - exit
select -
```

6 Enter the number next to the "Configuration" option in the menu.

Example response

```
Configuration
  1 - NTP Configuration
  2 - Apache Proxy Configuration
  3 - OAMP Application Configuration
  4 - CORBA Configuration
  5 - IP Configuration
  6 - DNS Configuration
  7 - Syslog Configuration
  8 - Remote Backup Configuration
  9 - Database Configuration
 10 - NFS Configuration
 11 - Bootp Configuration
 12 - Restricted Shell Configuration
 13 - Security Services Configuration
 14 - Disk Drive Upgrade
 15 - Login Session
 16 - Location Configuration
 17 - Cluster Configuration
 18 - Succession Element Configuration
 19 - snmp_poller (SNMP Poller Configuration)
 20 - backup_config (Backup Configuration)
X - exit
Select -
```

7 Enter the number next to the "Security Services Configuration" option in the menu.

Example response:

```
Security Services Configuration
1 - Socks Configuration
2 - IEMS Server Location Configuration
3 - PAM Configuration
X - exit
```

```
select -
```

8 Enter the number next to the "Socks Configuration" option in the menu.

Example response:

```
Socks Configuration
1 - config_socks (Modify Socks Security Service)
2 - list_socks (List Socks Security Service)
X - exit
select -
```

9 Enter the number next to the "list_socks" option in the menu to display the server-side and client-side Socks Proxy ports that are currently configured.

Example response:

```
The ports configured for use by socks are:
The Client side SOCKS Proxy will listen on port 10090
The Server side SOCKS Proxy will listen on port 10080
==="list_socks" completed successfully
```

10 Use the following table to determine how to proceed.

If you	Do
want to change the ports	Step 11
do not want to change the ports	you have completed this procedure

11 Enter the number next to the "config_socks" option in the menu.

Example response:

```
The changes of the server side port is a disruptive
action.  If the server side port is changed, the
SOCKS server and all dependent applications must be
restarted.
SOCKS ports in all offices must be configured to the
same port.  Misconfiguration will cause EMS clients to
not function.
Proceed with caution.
Enter the port the Server side SOCKS Proxy will listen
on.  Value must be within [1025 - 655351].  current
Value - 10080 [?, q]
```

12

ATTENTION

Changing the Socks server-side port requires a restart of the SOCKS server and all dependent applications.

Enter the server-side port, or press Enter to leave at the default value (10080).

Example response:

```
Leaving SERVER port at 10080
Enter the port the Client side SOCKS Proxy will listen
on.  Value must be within [1025 - 655351].  Current
value - 10090 [?, q]
```

13

ATTENTION

Changing the Socks client-side port requires that all client workstations already running the application GUIs, be restarted to use the new port.

Enter the client-side port, or press Enter to leave at default the value (10090).

Example response:

```
Leaving CLIENT port at 10090
Leaving both ports at configured values:
           Server side SOCKS Proxy port: 10080
           Client side SOCKS Proxy port: 10090
==="Config_socks" completed successfully
```

14 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.

15 Use the following table to determine how to proceed.

If you	Do
changed one or both ports	Step 16
did not change the port values	you have completed this procedure

16 Perform one or both of the following substeps depending on whether you changed the server-side or client-side port, or both.

a. After changing the server-side port, restart the Socks server and all dependent server applications (SESM, SAM21EM, and MG9KEM)

Refer to the*ATM/IP Solution-level Security and Administration* , NN10402-600 for the Socks server, SESM and SAM21 server applications. Refer to the *MG 9000 Security and Administration*,

NN10162-611 for the MG 9000 Manager serer application. Refer to*Packet MSC Administration and Security* , NN20000-216, for the Socks and dependent server applications.

b. After changing the client-side port, restart any client workstations already running the application GUIs.

—End—

Initiating a recovery back to the cluster

Prerequisites

It is expected that the primary server is in the shut-down mode.

If the server was previously a CBM and contains billing files not already sent to a down-stream billing server, using the cluster server, these files should be copied to a downstream server prior to performing "Installing the remote backup server" (page 290). Otherwise these files and the billing records will be lost. Contact next level of support for assistance

Target

When completed, this procedure will restore the HA cluster and backup server.

Action

Initiating a recovery back to the cluster

At your workstation

Initiating a recovery back to the cluster

Step	Action
1	Follow the "Installing the remote backup server" (page 290)procedure. In this case, the unit0 server of the cluster is used as a remote backup server. Use the same hostname and IP address that was used to configure the remote backup server in the first place.
2	Follow the "Scheduling automatic backups on the remote server" (page 296)procedure. Use only one automated schedule and make sure to select a time that will not be invoked shortly.
3	Follow the "Performing a manual backup of the target server" (page 294)procedure.
4	Bring down the machine currently active by following the procedure ‘Two-server (cluster) configuration’ in chapter ‘Shutting down an SPFS-based server’ of the document ATM/IP Solution-level Fault Management NN10408-900.
5	Follow the "Initiating a switch over to the remote backup server" (page 287)procedure to bring the services back to unit0 of the cluster.

6 Follow the ‘Cloning the image of one server in a cluster to the other server’ procedure of the document ATM/IP Solution-level Security and Administration NN10402-600.

7 If the server was previously a CBM and contains billing files not already sent to a down-stream billing server, using the remote backup server, these files MUST be copied to a downstream server prior to performing "Installing the remote backup server" (page 290)Otherwise these files and the billing records will be lost. Contact next level of support for assistance.

8 Reinstall the backup server following the "Installing the remote backup server" (page 290)procedure.

9 Reconfigure the backup server following the "Scheduling automatic backups on the remote server" (page 296)procedure.

10 The procedure is complete.

—End—

Initiating a switch over to the remote backup server

Prerequisites

Prior to starting this procedure, shut down the Cluster machine.

Refer to section *Two-server (cluster) configuration* in chapter *Shutting down an SPFS-based server* in NTP NN10408-900, *ATM/IP Solution-level Fault Management*.

The user must be logged in as the root user in order to initiate the switch command.

CAUTION

If configuration, provisioning, patching or other “write”-type operations occurred since the last remote backup, the remote backup system can be out of sync compared to the data in network elements and/or the primary OAM system.

Take actions before initiating the switchover to a remote backup OAM server (that is, response to a geographic or other prolonged outage of the primary OAM system) to halt or prevent “write”-type operations by OSSs and operations personnel until an in-sync status is achieved.

When initiating a switchover to a remote backup OAM server, do not execute configuration, provisioning, patching or other “write”-type operations through the remote backup OAM system until out-of-sync conditions are cleared.

Target

When completed, this procedure reboots the remote backup server as the unit0 of the cluster.

Action

Initiating a switch over to the remote backup server

At your workstation

Step	Action
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 remote backup server.

2 When prompted, enter your user ID and password.

3 Change to the root user.

```
su - root
```

4 When prompted, enter the root password.

5 Invoke the switch by typing:

```
$ /opt/sspfs/rbks/switch
```

6 When ready, indicate you want to proceed by typing:

```
OK
```

—End—

Installing the remote backup server

Target

Use this procedure to install the remote backup server for Geographic Survivability. Backing up the remote server provides a standby backup system which is ready to provide service if the primary system is unavailable for an extended period of time. The remote server can assume the identity of the primary server with data and files accurate to the last synchronization.

Prequisites

You must have the root user ID and password to perform this procedure.

Use the following table to ensure that you have the information ready for input during this procedure.

System Variable	Actual value
Hostname	
IP address (remote backup server)	
Netmask	
Router (default gateway IP)	
DNS (Yes, No)	
Unit 0 IP address (IP of primary cluster unit 0)	
Daily backup (up to four) in format:**HH:MM** where **HH = hours (00-23)** **MM = minute (00-59)**	
DNS domain	
IP address (DNS server[s])	
DNS search domain(s)	

DNS variables apply only when a DNS server has been configured.

Action

Installing the remote backup server on a Geographic Survivability standby server

At your workstation or the remote server console

Step **Action**

1 Determine how to log in to the Sun Netra 240 (N240) server that is installed as the remote backup server.

If you want to log in by means of	Do
ssh	Type ssh -1 root <server> and press the Enter key. Go to step 2
telnet	Type telnet <server> and press the Enter key. Go to step 2
the remote server console	step 2

where

`server` is the name of the N240 server.

2 Log in to the server through the console (port A) and when prompted, enter the root user ID and password.

3 Bring the system to the {0} OK prompt by typing:

```
# init 0
```

4 Enter the following command to verify that the auto-boot option is set to true.

```
{0} ok printenv auto-boot?
```

If it is set to false, enter the following command.

```
{0} ok setenv auto-boot?=true
```

5 Insert disk 1 of the SPFS0** (090) CD set into the DVD drive on the standby unit.

6 Install the remote backup server for Geographic Survivability.

```
{0} OK boot cdrom - rbackup
```

7 Type OK and press Enter to acknowledge restriction on your use of the software.

8 Select the rbackup server profile for the system.

9 Enter no to not select the default settings. The N240 server must be connected to the network and must have access to the default

gateway. This allows you to enter the server's settings for the installation.

10 Enter site-specific information in response to the following prompts. (Refer to the information entered in the table at the beginning of this procedure.)

```
Enter the hostname for this system.
Enter the IP address for the remote backup server.
Enter the subnet mask for this network.
Enter the IP address for this network's router.
Enter the timezone for this system.
```

The default timezone is US/Eastern. Enter ? for a list of supported time zones.

```
Will this system use DNS?
```

11 Enter yes or no. If you answer yes, you are prompted for the DNS domain name, name server IP addresses, and the search domains. You can enter several name servers and search domains. To stop entry, enter a blank line

12 Enter OK to accept current settings.

The installation of the first CD takes approximately 25 minutes. No action is required until the following system response displays:

```
Media:

1.  CD/DVD
2.  Network File System
3.  Skip
Media[1]:
```

13 Enter 1 and then press Enter to select CD/DVD as the Media type for the installation of Solaris 9.

The system ejects disk 1 CD automatically.

14 Remove SPFS disk 1 CD from the server.

15 Insert SPFS disk 2 CD (the second SPFS CD in the set of 3 disks) into the DVD drive and then press Enter.

This step takes approximately 15 minutes to complete.

16 Enter 2 to continue with the installation.

17 Press Enter to reboot the system.

The installation of the Solaris Patches starts after the system reboots.

18 The installation of the second CD takes approximately 20 minutes. No action is required until the system prompts you to enter the third CD.

```
Done Installing Solaris Patches...
Insert SSPFS Deadstart CD ROM Disk 3 in the Drive.
Type "ok" when Ready.
```

19 Remove SPFS disk 2 CD from the server.

20 Insert SPFS disk 3 CD (the third SPFS CD in the set of 3 disks) into the DVD drive.

21 Enter OK and then press Enter to start the installation of the third CD.

The installation of the third CD takes approximately 50 minutes. You could be required to press Enter to reprint the login prompt to the screen after the reboot.

```
<Hostname> console login:
```

22 Log in to the server using the root user ID and password.

23 Remove SPFS disk 3 CD from the server.

```
eject cdrom
```

24 Enter the command line interface (CLI) tool.

```
cli
```

25 Enter the number next to the Configuration option in the menu.

26 Enter the number next to the Succession Element Configuration option in the menu.

27 Enter the number next to the PSE Application Configuration option in the menu.

28 Enter the number next to the Configure PSE option in the menu.

29 Enter the primary/cluster IP address of CS 2000 Management Tools server. This is the address of the NPM server.

30 Enter Y to confirm the IP address.

Ignore the following error message if it displays.

```
Can't configure PSE on remote backup unit to enable NPM
```

31 Enter X to exit each level until you have exited from the cli tool.

32 Start the PSE server.

```
# pse start
```

33 Verify that the server has started. If the server does not start, contact your next level of support.

```
# pse status
```

34 If an SPFS MNCL CD is to be installed, refer to the documentation included with the CD for complete installation instructions.

35 Enter NPM on the CS 2000 Management Tools server and follow patching procedures to apply all relevant patches.

—End—

Performing a manual backup of the target server

Target

Use this procedure to perform a manual backup of the primary server. Backing up the primary server provides a standby backup system which is ready to provide service if the primary system is unavailable for an extended period of time. The remote server can assume the identity of the primary server with system configuration data and files accurate to the last synchronization.

ATTENTION
This procedure is for use with Geographic Survivability only.

Action

Performing a manual backup of the remote server

At your workstation or the remote server console

Step Action

1 Determine how to log in to the Sun Netra 240 (N240) server that is installed as the remote backup server.

If you want to log in by means of	Do
ssh	Type ssh -l root <server> and press the Enter key. Go to step 2
telnet	Type telnet <server> and press the Enter key. Go to step 2
the remote server console	step 2

where

`server` is the name of the N240 server.

2 When prompted, enter the root password.

3 Start the command line interface tool.

```
cli
```

The system responds by displaying a menu.

4 Select the Configuration menu.

The system displays the Configuration menu.

5 Select the Remote Backup option.

```
Remote Backup Configuration
1-rbackup_display (Display Remote Backup Configuration)
2-rbackup_config (Remote Backup Configuration)
3-rbackup_exec (Execute Remote Backup Now)
4 - rbackup_cancel (Cancel Running Remote Backup)
X-exit
```

6 Select

```
3-rbackup_exec (Execute Remote Backup Now)
```

7 An automatic backup is made.

Pressing 4 during execution of the backup halts the process and performs necessary clean-up operations.

8 Exit the Remote Backup Configuration level.

x

—End—

Scheduling automatic backups on the remote server

Target

Use this procedure to schedule automatic backups to the remote server. Backing up the primary server provides a standby backup system which is ready to provide service if the primary system is unavailable for an extended period of time. The remote server can assume the identity of the primary server with data and files accurate to the last synchronization.

ATTENTION
This procedure is for use with Geographic Survivability only.

Action

Scheduling automatic backups of the remote server

At your workstation or the remote server console

Step Action

1 Determine how to log in to the Sun Netra 240 (N240) server that is installed as the remote backup server.

If you want to log in by means of	Do
ssh	Type ssh -l <server> and press the Enter key. Go to step 2
telnet	Type telnet <server> and press the Enter key. Go to step 2
the remote server console	step 2

where

`server` is the name of the N240 server.

2 When prompted, enter the root password.

3 Start the command line interface tool by entering:

```
cli
```

4 Select the Configuration menu.

The system displays the Configuration menu.

5 Select the Remote Backup option.

Response:

```
Remote Backup Configuration
```

```
1 - rbackup_display (Display Remote Backup Configurati
on)
2-rbackup_config (Remote Backup Configuration)
3-rbackup_exec (Execute Remote Backup Now)
4 - rbackup_cancel (Cancel Running Remote Backup)
X-exit
```

6 Select:

```
2-rbackup_config (Remote Backup Configuration)
```

The system responds with the IP address of the primary server that is currently configured as the remote server, and the times that are currently configured for automatic backups.

7 Enter the unit 0 IP address of the primary server to be backed up.

```
<nnn.nnn.nnn.nnn> is alive
```

where

nnn.nnn.nnn.nnn is the IP address that you entered.

8 Use the following table to determine your next step.

If the system	Do
prompts you to accept the ssh key	Enter yes. Go to step 9
does not prompt you to accept the ssh key	Go to step 9

```
Enter a time for a daily backup to occur (HH:MM):
```

where

HH is hours. Valid values are 00 to 23.
MM are minutes. Valid values are 00 to 59.

9 Enter the first time for a daily backup to occur

You can configure up to four times for daily backup to occur.

Response:

```
Enter a second time for a daily backup to occur (HH:MM)
or enter "x" to stop provisioning backup times:
```

10 Use the following table to determine your next step

If you	Do
want to enter another time for a remote backup to occur	Enter a second time for a daily backup to occur. Go to step 11
do not want to enter another time for a remote backup to occur	Enter x. Go to step 13

11 Use the following table to determine your next step

If you	Do
want to enter another time for a remote backup to occur	Enter a third time for a daily backup to occur. Go to step 12
do not want to enter another time for a remote backup to occur	Enter x. Go to step 13

12 Use the following table to determine your next step

If you	Do
want to enter another time for a remote backup to occur	Enter a fourth time for a daily backup to occur. Go to step 13
do not want to enter another time for a remote backup to occur	Enter x. Go to step 13

13 Use the following table to determine your next step

If you want to	Do
commit changes	Go to step 14
exit	Enter quit. Go to step 15
re-enter settings	Enter anything other than ok or quit. Go to step 9

14 Enter

```
ok
```

```
=== "rbackup_config"completed successfully
```

15 Exit the Remote Backup Configuration level.

```
x
```

—End—

Viewing configuration information for remote server backups

Target

Use this procedure to view the current configuration information for remote server backups. The system displays the IP address of the target system and the times in which automatic backups of the target system will occur.

ATTENTION
This procedure is for use with Geographic Survivability only.

Action

Viewing configuration information for remote server backups

At your workstation or the remote server console

Step	Action
1	Determine how to log in to the Sun Netra 240 (N240) server that is installed as the remote backup server.

If you want to log in by means of	Do
ssh	Type ssh -l <server> and press the Enter key. Go to step 2
telnet	Type telnet <telnet> and press the Enter key. Go to step 2
the remote server console	step 2

where

`server` is the name of the N240 server.

2 Start the command line interface tool by entering:

```
cli
```

The system responds by displaying a menu.

3 Select the Configuration menu.

The system displays the Configuration menu.

4 Select the Remote Backup option.

Response:

```
Remote Backup Configuration
1-rbackup_display (Display Remote Backup Configuration)
```

```
2-rbackup_config (Remote Backup Configuration)
3-rbackup_exec (Execute Remote Backup Now)
4 - rbackup_cancel (Cancel Running Remote Backup)
X-exit
```

5 Select

```
1-rbackup_display (Display Remote Backup Configuration)
```

Response:

```
Current settings:
Target system is:  <nnn.nnn.nnn.nnn>
Back up times are:  <Time 1>...<Time n>
```

where

<nnn.nnn.nnn.nnn> is the IP address of the remote server

where

<Time 1>...<Time n> is the set of times at which automated backups occur.

6 Exit the Remote Backup Configuration level by typing:

x

—End—

Viewing logs from a remote backup

Target

Use this procedure to view logs associated with a backup of the remote server. Logs are created during automatic and manual backups of the remote server.

Action

Viewing logs from a remote backup

At your workstation or the remote server console

Step Action

1 Determine how to log in to the Sun Netra 240 (N240) server that is installed as the remote backup server.

If you want to log in by means of	Do
ssh	Type ssh -l <server> and press the Enter key. Go to step 2
telnet	Type telnet <server> and press the Enter key. Go to step 2
the remote server console	step 2

where

`server` is the name of the N240 server.

2 Enter:

```
less /var/adm/messages
```

The system responds by displaying the contents of the log file.

3 The procedure is complete.

—End—

Carrier VoIP

Core and Billing Manager 850 Fault Management

Publication: NN10351-911
Document status: Standard
Document version: 04.04
Document date: 20 October 2006

To provide feedback or report a problem in this document , go to **http://www.nortel.com/documentfeedback**

The information in this document is sourced in Canada, the United States of America, and the United Kingdom.