CBM Fault Management

Fault management strategy

The Core Billing Manager (CBM) fault management strategy includes the dual functions of Fault Delivery and Test and Diagnostic capabilities.

The core manager component handles many of the fault delivery features.

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.

Tools and utilities

The primary fault management tools and utilities are alarms and logs.

Logs

The Log Delivery application, included as part of the base software platform on the core manager, collects logs generated by the core manager, the computing module on the call server, and other network elements, and delivers them to operational support systems (OSS). For more information on the Log Delivery application and tools, refer to the Basics document.

Log Delivery procedures

The following table lists tasks and procedures associated with the Log Delivery system and tools. Use this table to determine which procedure to use to complete a specific log-related task.

Table 1 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
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 on page 66"

Table 1 Log Delivery procedures

If you want to	Use procedure
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 on page 66”
store logs in a file	“Retrieving and viewing log records on page 66”
troubleshoot log delivery problems	“Troubleshooting Log Delivery problems on a CBM on page 76”

SDM logs

Core manager events are recorded internally to the core manager in a series of log reports. Core manager log reports are local to the core manager. Most core manager log reports do not appear in the generic Core log utility stream, except log reports SDM550 and SDM650.

Note: Log reports SDM550 and SDM650 appear in the Core log stream.

Core manager log reports fall into three categories: trouble (TBL) logs, state change logs, and information (INFO) logs.

- Trouble logs provide an indication of some type of fault for which corrective action can be taken. These logs are generated for connectivity failures, system resource problems, and application software and hardware failures. Each of these trouble conditions corresponds to an alarm on the alarm banner of the core manager maintenance interface.
- State change logs provide information about core manager state changes to InSv (in service), Offl (offline), ManB (manual busy), ISTb (in-service trouble), and SysB (system busy). While state changes from InSv to ISTb or SysB require corrective action, the logs indicating these changes do not provide detailed information about the reason for the state change. Specific information is contained in the TBL logs.

When the core manager or the Log Delivery application is returned to service from a ManB state, some logs may be delivered with the CM_CLLI in the Office ID field of the log header, instead of the data filled LOG_OFFICE_ID. This occurs only for logs generated by core manager applications, and only occurs until at least one log has been delivered that originated from a CM-based application. The discrepancy corrects itself as soon as the first CM log is received on the core manager.

- Information logs provide information about events that do not normally require corrective action. These logs are generated for system restarts, non-service-affecting state changes, and for events that clear TBL logs.

SDM logs describe events general events related to the operations of the core manager. The following table lists SDM logs.

Table 2 Core manager logs

Log	Trigger	Action
SDM267	CBM custlog log to indicate a change in the condition of a CBM link.	None
SDM300	The connection from the core manager to the Core or the operating company LAN server(s) is down.	Contact your system administrator or Nortel Networks for assistance.
SDM301	A logical volume is not mirrored.	Check hardware faults as mirroring may be lost due to a hard disk failure on the core manager. ***Note:*** If a disk has just been replaced and brought back in-service, the system may take more than 15 minutes to restore mirroring.
SDM302	The use of a system resource has exceeded its threshold.	Isolate and clear the problem.

Table 2 Core manager 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 system administrator or Nortel Networks 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 in for more information: • "Configuring a CBM for log delivery" in the Configuration Management document • "Deleting a device using logroute" in the Configuration Management document If required, contact your system administrator or Nortel Networks for assistance.
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. ***Note:*** The software on the core manager must not be at a lower release level than the software on the Core.
SDM308	System image backup (S-tape) is required or has failed.	If a manual system image backup (S-tape) is required, refer to procedure "Creating system image backup tapes (S-tapes) manually" in the Security and Administration document. Ensure the backup tape is inserted. If required, contact your system administrator or Nortel Networks for assistance.

Table 2 Core manager logs

Log	Trigger	Action
SDM309	A hardware device is faulty or has been manually taken out of service.	Use the “querysdm” command from the MAP display. If required, replace the faulty module using the corresponding procedure in this document. Check the cabling to the module. If you cannot determine the reason for the fault, contact your next level of support.
SDM315	The Table Access Service application on the core manager has detected corruption in the Data Dictionary on the Core.	Contact your next level of support with the information provided in the log. The log information contains essential information for identifying the Data Dictionary type that is corrupt.
SDM317	The system has detected a Distributed Computing Environment (DCE) problem.	Contact your next level of support to help determine the cause of the failure.
SDM318	An operational measurements (OM) report was not generated. (The OM report failed to complete within one report interval.)	Contact Nortel Networks.
SDM321	A split mode upgrade has begun	Complete or abort the split mode upgrade.
SDM325	Indicates a lost connection to a Preside network management component.	None
SDM332	Indicates that the system audit completed with failures.	Refer to the procedure “Viewing the system audit report and taking corrective action” in the SDM Fault Management
SDM334	OC3 Card receive/transmit fault	Use the logs command from the hw level of the cbmmtc display to check for an OC3 card fault on the CBM. Check the cabling to the OC3 port listed in the log.

Table 2 Core manager logs

Log	Trigger	Action
SDM335	Bad incoming CRCs on link	Use the logs command from the hw level of the cbmmtc display to check for an OC3 link fault on the CBM. Use the "trnsl" command from the MAP display to check the link status. Perform link tests from the MS card level.
SDM336	No heartbeat response received	Use the logs command from the hw level of the cbmmtc display to check for OC3 link faults on the CBM. Check the cabling to the OC3 port listed in all logs. Use the "trnsl" command from the MAP display to check the link status. Perform link tests from the MS card level.
SDM500	Indicates the initial startup of the core manager. This log is included in the SDM Log Delivery log stream, but does not appear on the RMI.	None
SDM501	Indicates a core manager state change to in service (InSv). This log is included in the SDM Log Delivery log stream, but does not appear on the RMI.	None
SDM502	Indicates a core manager state change to manual busy (ManB). This log is included in the SDM Log Delivery log stream, but does not appear on the RMI.	None
SDM503	Indicates a core manager state change to system busy (SysB). This log is included in the SDM Log Delivery log stream, but does not appear on the RMI.	Refer to the procedure “Clearing a critical APPL alarm” in the SDM Fault Management document
SDM504	Indicates a core manager state change to in-service trouble (ISTb). This log is included in the SDM Log Delivery log stream, but does not appear on the RMI.	Refer to the procedure “Clearing a minor or major APPL alarm” in the SDM Fault Management document

Table 2 Core manager logs

Log	Trigger	Action
SDM505	Indicates a core manager state change to offline (OffL) state. This log is included in the SDM Log Delivery log stream, but does not appear on the RMI.	None
SDM550	Indicates a core manager node status change. One or more of the following can cause the status change: • core manager node state • hardware device • software component • application	Refer to the corresponding procedure in this document if required. ***Note:*** Log SDM550 is generated on the CM.
SDM600	The connection from the core manager to the Core or the operating company LAN server(s) has been reestablished. This log is generated only after a connectivity failure has been corrected, and not at system startup.	None
SDM601	Mirroring has been reestablished after a logical volume mirroring failure.	None
SDM602	A system software resource has returned below its alarm threshold.	None
SDM603	A fault on a core manager application or process has cleared.	None

Table 2 Core manager logs

Log	Trigger	Action
SDM604	The Log Delivery application generates this log when the Core does not have enough CPU time to format logs, and discards the logs.	Increase office parameter PER_OPC_LOGDEV_BUFFER_SIZE to its maximum size of 22,000. (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 Nortel Networks for assistance.
SDM608	A system image backup (S-tape) has been completed.	None
SDM609	A hardware device has been returned to the in-service state.	None
SDM615	The SDM Exception Reporting Application generates a warning report at 8:00 a.m. local time when the system generates thresholded logs within the preceding 24 h.	Use LOGUTIL to disable thresholding for logs indicated in the report.
SDM616	A log delivery connection attempt was rejected.	None
SDM617	A Distributed Computing Environment (DCE) problem is cleared.	None
SDM618	The system generates this log report when the /var logical volume reaches 95% full on the disk.	None
SDM619	The OM Access Server has detected a corrupt OM Group during an OM Schema download.	None

Table 2 Core manager logs

Log	Trigger	Action
SDM620	Reports SDM system performance data such as CPU usage, number of processes, swap space occupancy, and logical volume capacities.	None
SDM621	A split mode upgrade has finished.	None
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 Nortel Networks for help.
SDM625	Indicates a re-established connection to a Preside network management component.	None
SDM630	Indicates the start time and completion time of the REX test.	None
SDM632	Indicates one of the following: • the system audit completed successfully • the system audit completed with warnings • a user cleared the system audit status • the system audit execution time is disabled or enabled	If the response is “the system audit completed with warnings”, refer to the procedure ”Viewing the system audit report and taking corrective action” in the SDM Fault Management document
SDM633	Indicates an OC3 link condition change.	None
SDM634	OC3 Card fault cleared	None
SDM635	Bad incoming CRCs cleared	None
SDM636	Heartbeat alarm cleared	None

Table 2 Core manager logs

Log	Trigger	Action
SDM650	SDM link maintenance requests the logging of a failed link maintenance action. An example of a link maintenance action is the system testing of a link.	None ***Note:*** Log SDM650 is generated on the CM.
SDM700	Log report SDM700 reports a Warm, Cold, or Reload restart or a norestartswact on the core	None

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 SDMCS 2000 Core Manager. The following table lists SDMB logs.

Table 3 SDM Billing Application (SBA) logs

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

Table 3 SDM Billing Application (SBA) logs

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

Table 3 SDM Billing Application (SBA) logs

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.	• Check the disk space on the core manager. You may need to FTP files or may need to clean up the disk.
	• The Record Client/File Manager is unable to write to the disk.	• Check the disk space on the core manager. You may need to FTP files or may need to clean up the disk.
	• The disk use is above the critical threshold specified in the MIB in parameter. When this occurs, alarm LODSK is raised.	• Check to see if files are being sent FTP. If not, set the system up to FTP files or back up files to the DAT tape.
	• The disk use is above the major threshold specified in the MIB in parameter. When this occurs, alarm LODSK is raised.	• Check to see if files are being sent FTP. If not, set the system up to FTP files or back up files to the DAT tape.
	• The disk use is above the minor threshold specified in the MIB in parameter. When this occurs, alarm LODSK is raised.	• Check to see if files are being sent FTP. If not, set the system up to FTP files or back up files to the DAT tape.
	• Reached limit for disk space or for the number of files that can reside on the system for a particular stream.	• Check to see if files are being sent FTP. If not, set the system up to FTP files or back up files to the DAT tape.
	• The SBA cannot close or open a file.	• Check to see if files are being sent FTP. If not, set the system up to FTP files or back up files to the DAT tape. Also check file permission for the destination directories. • Contact your next level of support.
	• Flush file failed	
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.

Table 3 SDM Billing Application (SBA) logs

Log	Trigger	Action
SDMB365	A serious problem is preventing the creation of a particular stream. Generated when a new version of SBA does not support a stream format on an active stream that was present in a previous load.	Revert to the previous running version of the SBA. If you removed the support for the stream format in the new release, turn off the stream before installing the new version. If the new version is supposed to support all existing streams, contact Nortel Networks for the latest appropriate software.
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.

Table 3 SDM Billing Application (SBA) logs

Log	Trigger	Action
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: ***Note:*** The system may escalate these logs and minor alarms to critical status when the DPMS transmitter exhausts all possible retries. The MIB parameter SessionFtpMaxConsecRetries specifies the condition.	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 • 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.

Table 3 SDM Billing Application (SBA) logs

Log	Trigger	Action
SDMB390	A schedule-related problem has occurred. When this occurs, alarm SBAIF is raised.	Clear the alarm and any alarms related to failure.
SDMB400	This log is generated for every active stream every hour and lists all of the current active alarms.	Clear alarms immediately using the corresponding procedure in the Fault section.
SDMB530	A change in the configuration or status of a stream has occurred.	None
SDMB531	The configuration for backup volumes has been corrected.	None
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.
SDMB610	A communication-related problem with the SBA has been resolved.	None
SDMB615	A software-related condition has been resolved.	None
SDMB620	A backup-related problem with the SBA has been resolved.	None
SDMB621	A new backup file has been started.	None
SDMB625	Recovery has started on a backup file.	None
SDMB650	The SBA is restarting one or more of its processes.	None
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.	Contact your next level of support.

Table 3 SDM Billing Application (SBA) logs

Log	Trigger	Action
SDMB660	A problem related to communications with other SBA features was resolved.	None
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.	None
SDMB680	The file transfer mode has changed value.	None
SDMB820	Minimal backup space is available.	Increase the size of backup volumes.

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:

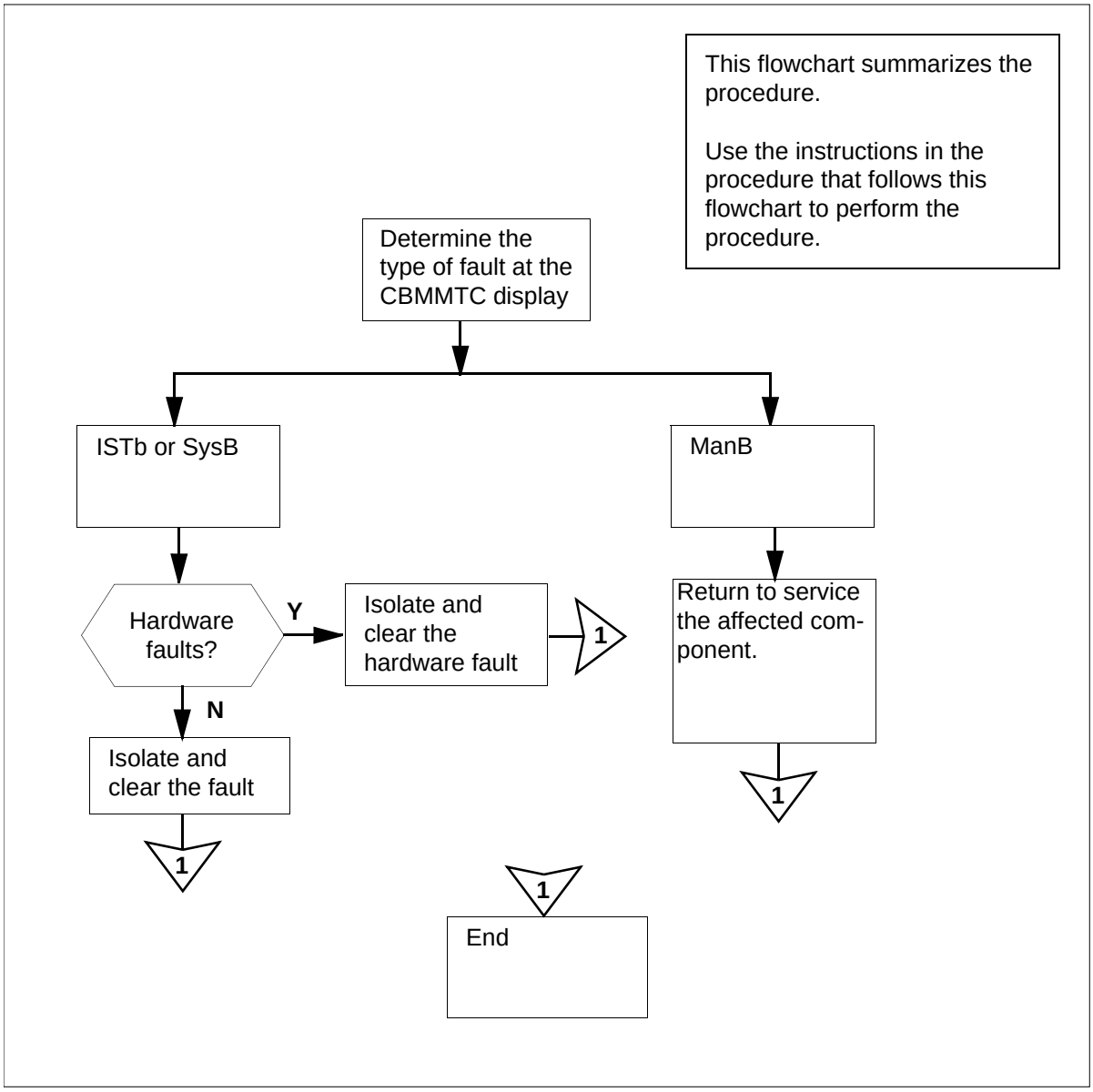
- One or more CBM applications have failed.
- CBM application is reporting an in-service trouble condition.
- A system software resource has exceeded its alarm threshold.
- A hardware device failure has been reported.
- Communication with the core has failed.

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

Action

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

Summary of clearing a minor or major or critical CBM alarm



Clearing a minor or major or critical CBM alarm

At the local or remote VT100 terminal

1 Log into the core manager as a maint class user, or root user, and obtain fault status information from the core manager by typing

> querycbm flt

and pressing the **Enter** key.

Example Response:

```
*** SPFS350 Current filesystem usage = 100 %
Filesystem  is filling up
cbm800=WCARY2QV;NODE=WCARY2QV;CLASS=SYS;SYSTYP
E=FSMon;FSMonName=FSUsage;FSName=/cbmdata/00/g
dd
Wed Jun 23 18:05:40 2004
 ** SPFS310 NOTICE: bge0: link down
Network Interface down
cbm850=hadry3;NODE=hadry3-unit0;CLASS=HW;HWTYP
E=NIC;NICNAME=bge0
Wed Jun 23 13:09:04 2004

 ** SDM336 Heartbeat alarm
No heartbeat response received.
cbm800=wcary2r1;NODE=wcary2r1;CLASS=NET;NETTYP
E=CORE
Tue Jun 22 01:59:29 2004

  * SDM610 Software Apply
SPF00O07 failed to apply.
cbm850=CBMDRY1;NODE=CBMDRY1;CLASS=SWIM;SWIMTYP
E=Patch;STATUS=Failed;ID=SPF00O07
Mon Jun 14 16:16:37 2004

  * SDM303 Trouble condition asserted.
Package: SDM_BASE.omsl
Process: omslomm
OMM-DDM Link Down.
cbm850=CBMDRY1;NODE=CBMDRY1;CLASS=APPL;APPLTYP
E=SDM_BASE.omsl:omslomm
Wed Jun 16 10:08:05 2004

 ** SPFS350 Mount Check failed
Filesystem /cbmdata/00/esa Not mounted
```

```
cbm850=HADRY2;NODE=HADRY2-unit0;CLASS=SYS;SYST
YPE=FSMon;FS
MonComp=MntChk;FSName=/cbmdata/00/esa
Thu Jun 24 05:15:59 2004

 ** SPFS340 MSH: Cluster nodes out of Sync
Cluster nodes out of Sync
cbm850=HADRY2;NODE=HADRY2-unit1;CLASS=NET;NETT
YPE=NODE
Thu Jun 24 05:13:45 2004

 ** SDM327 NTP alarm.
Synchronization started, may take up to 30
minutes.
cbm850=hadry3;NODE=hadry3-unit0;CLASS=NET;NETT
YPE=NTP
Wed Jun 23 14:49:00 2004

  * SDM330 Alarmd Data Collection from mate node
timed out
All Alarmd data collection requests timed out
cbm850=HADRY1;NODE=HADRY1-unit1
Fri Jun 25 18:12:47 2004

 ** SDM334 Major OC3 Card Fault: transmit fault
on link 0 (domain 0 port 0)
cbm800=TAK0_svr;NODE=TAK0_svr;CLASS=HW;HWTYPE=
OC3_FAULT_0
Thu Jun 24 14:17:36 2004
```

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

Fault type	log number	Description
Application	SDM303	Exceeded failure threshold Package: <package> Process: <process> Trouble condition asserted Package: <package> Process: <process> <reason>

Fault type	log number	Description
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)
	SDM336	Heartbeat alarm. No heartbeat response received.
Network Time Protocol	SDM327	NTP alarm. Synchronization started, may 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, SDM336)	Refer to Clearing a major or minor or critical APPL;SDM alarm on page 29
Network Time Protocol problem	have your system administrator isolate and clear the problem.
Application problem (SDM 303)	step 13

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

5

CAUTION

Potential service interruption

A logical volume on the CBM must never reach 100% disk full. The system enters into abnormal conditions 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.

If the GDD logical volume is exceeded, continue with step 6; otherwise, refer to the appropriate SSPFS 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. Proceed according to the choice.

If you decide to	Do
Increase the size of the GDD logical volume	proceed to the SSPFS procedure Increasing the size of a file system on a Sun server.
Decrease the number of days to retain logs	step 7

7 Access the Logroute commissioning tool by typing

```
# logroute
```

and pressing the Enter key.

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 by typing

> 4

and pressing the Enter key.

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 by typing

Enter Option ==> 1

and pressing the Enter key.

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

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

and pressing the Enter key.

11 Confirm to save the changes by typing "y"

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

and pressing the Enter key.

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
```

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

12 Go to step 22.

13 Log into the CBM as a maint class user, or root user, and access the maintenance interface by typing

 # cbmmtc

and pressing the Enter key.

14 Access the application (Appl) menu level of CBMMTC by typing:

```
> appl
```

and pressing the Enter key.

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
```

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

16 Proceed depending on the state of the application.

If the state is	Do
ManB	step 17
ISTb	step 18
SysB	step 19
Fail	step 20

17 Determine from office records or other personnel why the application was manually removed from service. When permissible, return the application software package to service by typing

```
> rts key
```

where

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

and pressing the Enter key.

Example response

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

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

```
RTS Application  Command complete.
```

If	Do
the application returns to service	step 23
the application does not return to service	step 16

18 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 min. 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 23
cannot resolve this problem	Contact your next level of support.

19 Use the reason given to resolve this problem

If you	Do
can resolve this problem	step 23
cannot resolve this problem	Contact your next level of support.

20 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 within10 min.

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

> bsy *key*

and pressing the **Enter** key.

where

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

Response:

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

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

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

21 Return the application to service by typing

`> rts key`

and pressing the **Enter** key.

where

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

Response:

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

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

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

22 Proceed depending on the state of the application.

If the application	Do
remains in a Fail state	refer to the configuration or installation information modules in the Configuration or Upgrades section, specific to that application
changes to InSv state	go to step 23

23 Obtain the fault status information from the CBM by typing

```
> querycbm flt
```

and pressing the Enter key.

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

Clearing a major or minor or critical APPL;SDM alarm

Application

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

Indication

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

Meaning

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

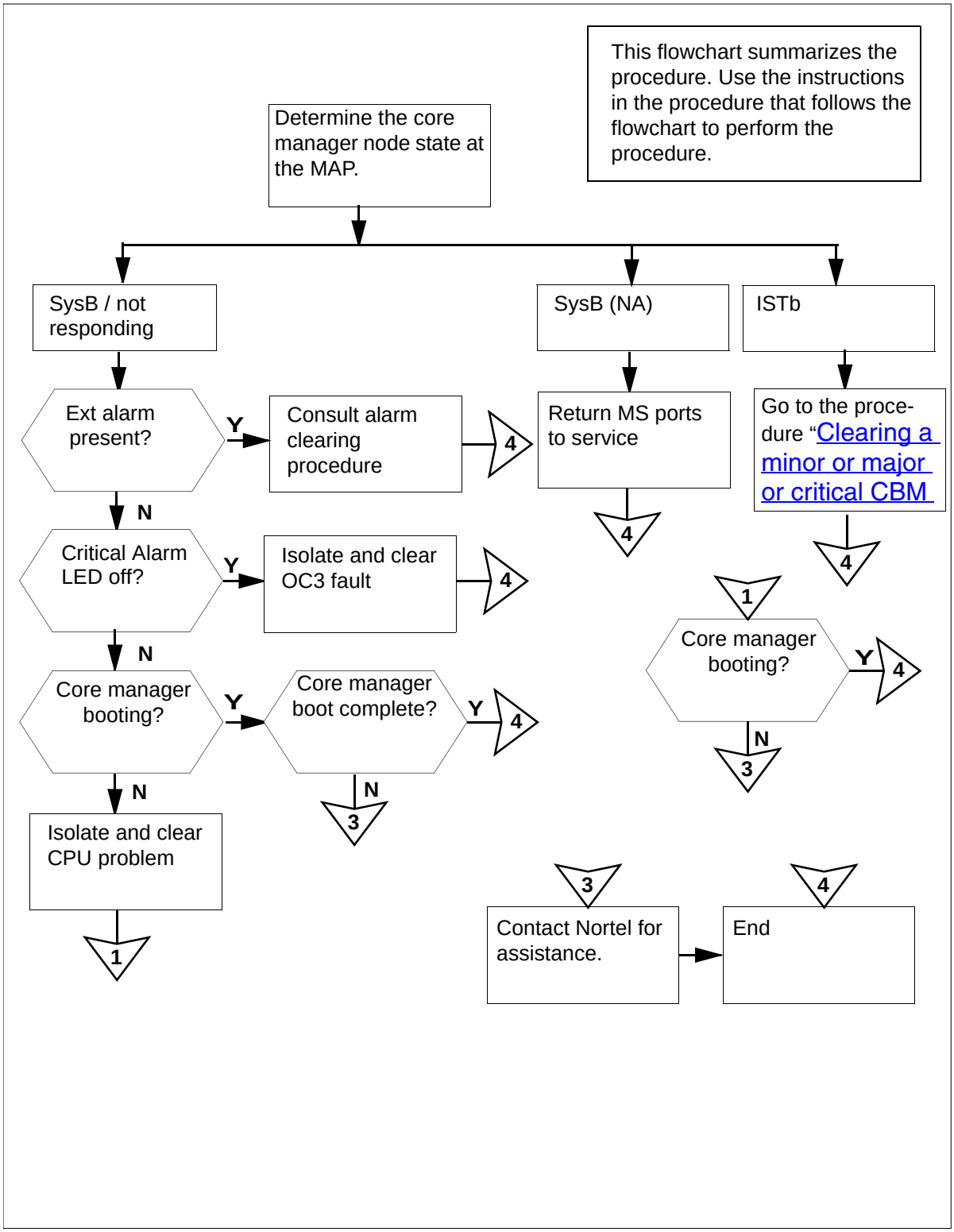
Impact

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

Action

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

Summary of clearing an APPL;SDM alarm



Clearing an APPL;SDM alarm

At the MAP display

1 Access the SDM level of the MAP display by typing

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

and pressing the **Enter** key.

Example response:

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

2 Determine the state of the core manager.

If the state is	Do
SysB/ (NA)	step 6
SysB/ is not responding	step 5
ISTb	the Clearing a minor or major or critical CBM alarm
ManB	step 3

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

```
> rts
```

and pressing the **Enter** key.

Example response:

```
SDM RTS initiated.
SDM RTS completed.
```

4 Determine

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

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

If	Do
not all of the links are out of service	contact your next level of support
all links are out of service	step 13

6 Determine the MS hardware that provides the OC3 links to the core manager by typing

```
> trnsl
```

and pressing the **Enter** key.

Note: The CM has designated the core manager as system busy (SysB) because all message switch (MS) ports that provide the OC3 links to the core manager are unavailable. The core manager may still be operational, but it is unable to communicate with the computing module (CM).

Example response

```
SDM 0 PORT 0 (MS 0:15:0) OK    ,C MsgCnd:Closed
SDM 0 PORT 1 (MS 1:15:0) ManB   MsgCnd:Closed
```

7 Record the MS port card number that is associated with the core manager OC3 links.

Note: In the example response shown in step 6, the port card number is 15.

8 Access the MS level of the MAP display by typing

```
> ms
```

and pressing the **Enter** key.

9 Access the shelf level by typing

```
> shelf 0
```

and pressing the **Enter** key.

10 Access the MS port card level that is associated with the core manager OC3 links by typing

```
> card <cardno>
```

and pressing the **Enter** key.

where

cardno
is the MS card number noted in step 7.

11 Note the status of the MS port card and its ports. Use the generic MS alarm clearing procedures provided with your DMS switching system to return the ports to service.

12 You have completed this procedure.

13 Access the EXT level of the MAP display by typing

```
> ext
```

and pressing the **Enter** key.

14 List all major EXT alarms by typing

```
> list maj
```

and pressing the **Enter** key.

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

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

If FSP alarm is	Do
present	step 16
not present	step 18

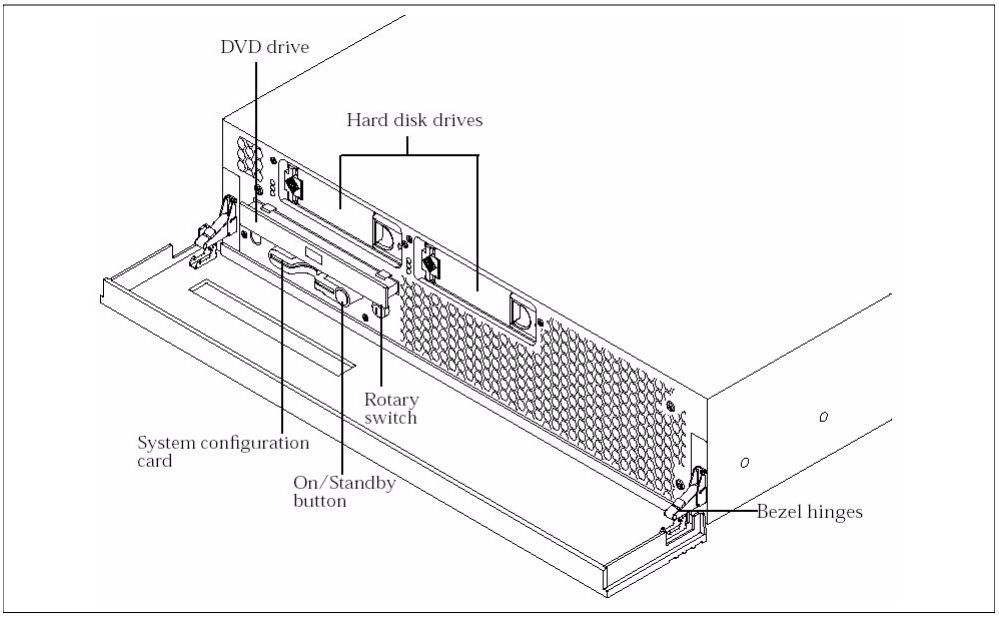
Note: An EXT FSP major alarm triggered by the core manager indicates that one or both -48V dc power inputs to the core manager have failed, or that the core manager has shut down because of thermal failure (overheating).

16 Clear the EXT FSP alarm using the procedure "Clearing an EXT FSP major alarm" in the SDM Fault Management document.

17 You have completed this procedure.

At the front of the core manager

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



Note: If the System in Service light is off, but power is available to the system and it has not shut down because of thermal failure (overheating), one or more of the following conditions is present or has occurred:

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

If the in-service light is	Do
on	step 31
off	step 19

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

If the system was	Do
manually shut down	step 22
not manually shut down	step 20

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

At the local VT100 console

21 Determine if the system is booting.

If the system is	Do
booting	step 23
not booting, or the boot has failed	step 22

At the front of the MSP

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

At the local VT100 console

23 Monitor the boot process. The boot process takes at least 5 min.

If the boot process	Do
does not start	step 24
starts, but does not complete (returns to the OK prompt)	step 26
completes normally, and the login prompt is displayed	step 31

At the front of the MSP

24 Cycle power to the core manager by turning the MSP breakers off and on. The MSP breakers supply power to the core manager. Turn top two breakers off and on.

At the local VT100 console

25 Monitor the boot process. The boot process takes at least 5 min.

If the boot process	Do
does not start	Contact your next level of support.
starts, but does not complete (returns to the OK prompt)	step 26
completes normally, and the login prompt is displayed	step 31

At the front of the MSP

26 Cycle power to the core manager by turning the MSP breakers off and on. The MSP breakers supply power to the core manager. Turn top two breakers off and on.

At the local VT100 console

27 Monitor the boot process at the local VT100 console.

If the boot process	Do
does not start	step 28
completes normally, and the login prompt is displayed	step 31

28 Perform a system software reinstall using the procedure Performing a full system restore on a Sun server (SN06.2 or greater) on page 220. Ensure that you reboot the system as indicated in that procedure.

29 Monitor the boot process.

If the boot process	Do
starts, but does not complete (returns to the OK prompt)	contact your next level of support
completes normally, and the login prompt is displayed	step 30

30 Complete the remainder of the procedure Performing a full system restore on a Sun server (SN06.2 or greater) on page 220.

At the local or remote VT100 console

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

32 Access the maintenance interface by typing

```
# cbmmtc
```

and pressing the **Enter** key.

33 Access the maintenance (Mtc) level by typing

```
> mtc
```

and pressing the **Enter** key.

34 Access the core level by typing

```
> core
```

and pressing the **Enter** key.

Example response

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

35 Continue according to state of the links.

If	Do
all links are open	step 44
any of the links are closed	step 36

36 Note the number of each closed link.

At the back of the core manager

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

If the fibre links	Do
require reconnecting or replacement	step 38
appear undamaged, and are correctly connected	step 40

38

CAUTION

Transmit and receive cables

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

Reconnect or replace the fibers on the OC3 card by pressing the fiber cable in.

At the local VT100 console

39 Monitor the link status at the core level.

If	Do
any of the links are closed	step 40
all links are open	you have completed this procedure

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

At the MAP display

40 At the MAP display, determine the MS hardware that provides the OC3 links to the core manager by typing

```
> trnsl
```

and pressing the **Enter** key.

Example response:

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

41 Record the MS port card number associated with the system-busy links identified in step 39.

Note: In the example response shown in step 40, the port card number is 15.

At the local VT100 console

42 Access the hardware (Hw) menu level of the CBM maintenance interface by typing

```
>hw
```

and pressing the **Enter** key.

43 Check for Alarm Logs for the OC3 links by typing

```
>logs
```

and pressing the **Enter** key.

```
CBM MATE NET APPL SYS HW CLLI: CTAT1
ISTb -   .  .   . ISTb Host: TAK0_svr
M M Active
Hw C
0 Quit R
2 O
3 S
```

4 Logs S
5 _
6 I
7
8
9
10
11
12 The Log Information retrieved for HW are
13 ** SDM314 Major Crossed Link: link 0 (domain 0 port 0) crossed
14 QueryCBM with link 1 (domain 0 port 1)
15 Crossed Link
16
cbm800=TAK0_svr;NODE=TAK0_svr;CLASS=HW;HWTYPE=CROSS_LINK_0
17 Help Thu Jun 24 09:19:26 2004
18 Refresh
maint

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

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

Clearing OC3 link faults

Application

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

Indication

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

Meaning

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

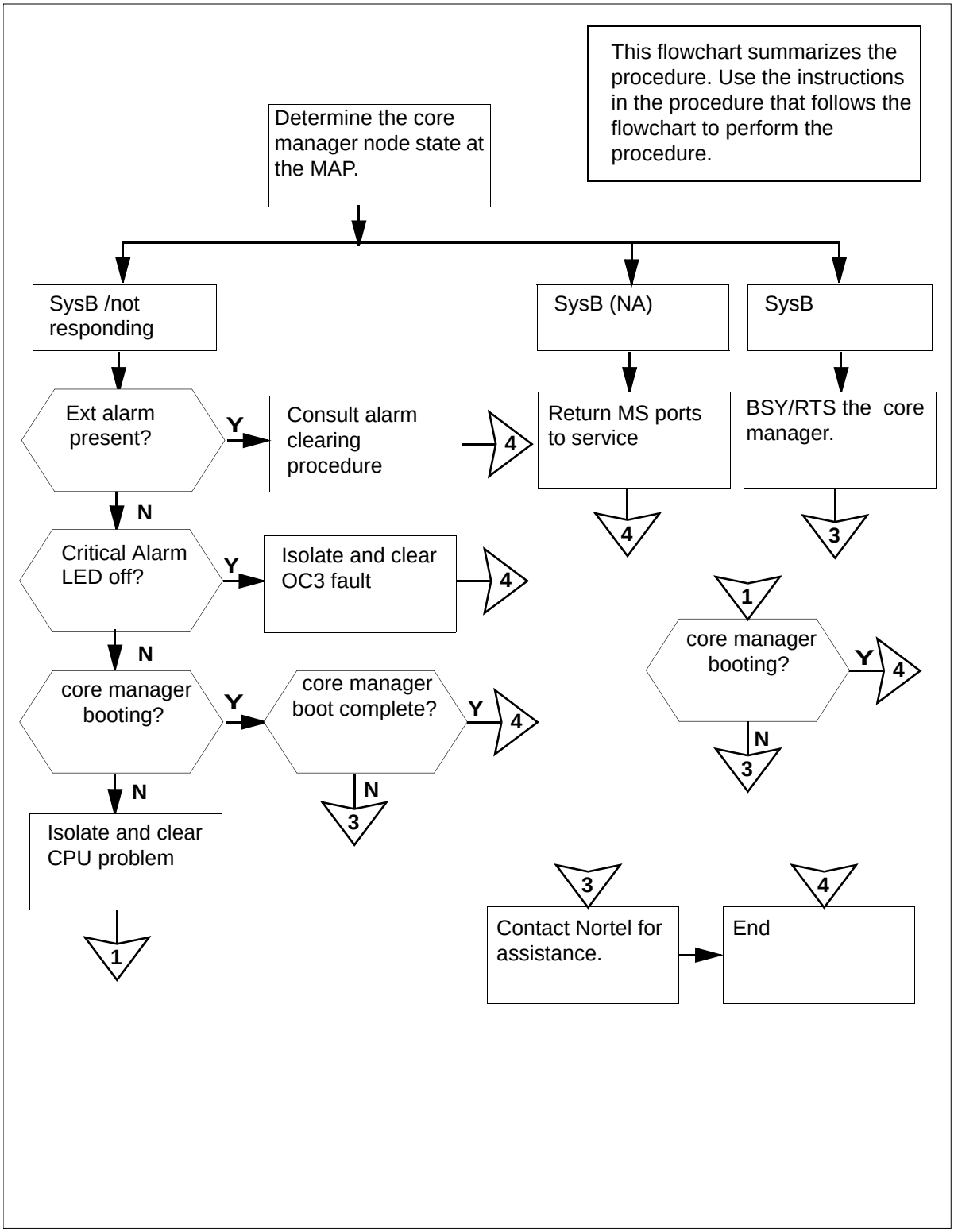
Impact

If the CM is unable to communicate with the core manager, the local state and operating condition of the core manager are unknown to the CM. MAP commands requesting state changes to the core manager are not sent to the core manager, and MAP requests for information from the core manager cannot be completed. The core manager maintenance interface can be used to obtain information about the core manager, when the CM-core manager link is not functioning. When communications are restored, the core manager local state aligns itself to the CM view of its state.

Action

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

Summary of clearing a critical APPL alarm



Clearing critical APPL alarm

At the local VT100 console

1 Access the hardware (Hw) menu level of the CBM maintenance interface by typing

```
>hw
```

and pressing the **Enter** key.

2 Check for Alarm Logs for the OC3 links by typing

```
>logs
```

and pressing the **Enter** key.

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


CBM   MATE   NET   APPL   SYS   HW   CLLI: CTAT1
ISTb   -     .    ISTb    .     .    Host: TAK0_svr
                                      Active
Hw
0  Quit
2
```

3
4 Logs
5
6
7
8
9
10
11
12 The Log Information retrieved for HW are
13 ** SDM334 Major OC3 Card Fault: receive fault on link 0 (domain 0
14 QueryCBM port 0)
15
16
cbm800=TAK0_svr;NODE=TAK0_svr;CLASS=HW;HWTYPE=OC3_FAULT_0
17 Help Wed Jun 23 11:07:29 2004
18 Refresh
root

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

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

Replacing a failed power supply

Application

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

Action

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

Replacing a power supply on a CBM server

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

Collecting DEBUG information using the CBMGATHER command

Purpose

The procedures that follow provide instructions on how to collect DEBUG information from the core manager while the device is in non-split mode or in split mode.

Application

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

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

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

Collecting DEBUG information in non-split mode

Use the following procedure to collect DEBUG information in non-split mode. This procedure can be used during a non-split mode upgrade or during normal operation of the core manager.

At the core manager command line (UNIX prompt)

1 Run the utility to collect the output:

```
# cbmgather
```

2 Run the utility to collect the output:

```
# FXgather
```

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

```
# cd /var/adm
# tar cvf varadm.tar [cdrs]*
# compress varadm.tar
```

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

Use the following table to determine your next step.

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

- /var/adm/cbmgather_<machine_name>_<date_and_time>.tar.Z

  Example
  /var/adm/cbmgather_wcary2p2_20020528091133.tar.Z

- /var/adm/varadm.tar.Z

5 Remove the output of the varadm.tar.Z file from the system:

```
# rm /var/adm/varadm.tar.Z
```

You have completed this procedure.

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

- /var/adm/ras/gather.<date_and_time>/gather.out

  Example
  /var/adm/ras/gather.020528090819/gather.out

- /var/adm/ras/gather.<date_and_time>/gather.cpio.Z

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

- /var/adm/varadm.tar.Z

7 Remove the output of the varadm.tar.Z file from the system:

```
# rm /var/adm/varadm.tar.Z
```

You have completed this procedure.

Collecting DEBUG information in split mode

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

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

domain (domain 0)

1 Run the utility to collect the output:

```
# cbmgather
```

If the platgather command	Do
executes	step 3
is not available	step 2

2 Run the utility to collect the output:

```
# FXgather
```

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

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

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

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

4 Run the utility to collect the output:

```
# cbmgather
```

If the platgather command	Do
executes	step 6
not available	step 5

5 Run the utility to collect the output:

```
# FXgather
```

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

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

Example response:

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

If you used the	Do
cbmgather command	steps 7 through 9
FXgather command	step 10 through 12

From the active domain (domain 0)

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

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

where

<source file>
is each of the following files:

- /var/adm/platgather_<machine_name>_<sys_old_or_new>_<date_and_time>.tar.Z

  Example
  /var/adm/platgather_wcary2p2_sysnew_20020523223351.tar.Z

- /var/adm/varadm_sysnew.tar.Z

Example command sequence

```
# smft -g /var/adm/platgather_wcary2p2_sysnew
_20020523223351.tar.Z
/var/adm/platgather_wcary2p2_sysnew
_20020523223351.tar.Z

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

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

- /var/adm/platgather_<machine_name>_sysold _<date_and_time>.tar.Z.

  Example
  /var/adm/platgather_wcary2p2_sysold _20020523223351.tar/Z

- /var/adm/platgather_<machine_name>_sysnew _<date_and_time>.tar.Z

  Example
  /var/adm/platgather_wcary2p2_sysnew_200205232233 51.tar.Z

- /var/adm/varadm_sysold.tar.Z
- /var/adm/varadm_sysnew.tar.Z

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

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

From the active domain (domain 0)

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

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

where

<source file>
is each of the following files:

- /var/adm/ras/gather.<date_and_time>/gather.out

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

- /var/adm/ras/gather.<date_and_time>/gather.cpio.z

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

- /var/adm/varadm_sysnew.tar.Z

Example command sequence

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

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

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

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

- /var/adm/ras/gather.<date_and_time>/gather.out

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

- /var/adm/ras/gather.<date_and_time>/gather.cpio.Z

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

- /var/adm/gather_sysnew.out
- /var/adm/gather_sysnew.cpio.Z
- /var/adm/varadm_sysold.tar.Z
- /var/adm/varadm_sysnew.tar.Z

12 Remove the following gathered output/files from the system:

```
# rm/var/adm/gather_sysnew.out
```

```
# rm/var/adm/gather_sysnew.cpio.Z
```

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

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

13 You have completed this procedure.

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

Purpose

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

Application

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

Procedures for which remote access to log devices can be used

Log device	Procedure	Applies to
TCP	Accessing a TCP device from a remote location	"Configuring a CBM for log delivery" in the Configuration Management document "Displaying or storing log records using logreceiver" in this document
TCP-IN	Accessing a TCP-IN device from a remote location	"Configuring CBM for log delivery" in the Configuration Management document "Deleting a device using logroute" in the Configuration Management document

Procedure

Accessing a TCP device from a remote location

At the remote workstation

1 Start the logreceiver tool:

```
> logreceiver <port_number>
```

where:

<port_number>
is the port number used for the TCP device on the core manager

2 Continue with the desired procedure listed in the table Procedures for which remote access to log devices can be used on page 51.

3 You have completed this procedure.

Accessing a TCP-IN device from a remote location

At the remote workstation

1 Use telnet to access the core manager:

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

where:

<ip_address>
is the address of the core manager

<port_number>
is the number of the port of the device on the core manager

2 Log into the core manager either as maint or admin.

3 Start the logroute tool:

```
# logroute
```

4 Continue with the desired procedure from the table Procedures for which remote access to log devices can be used on page 51.

5 You have completed this procedure.

SBA alarm troubleshooting

Purpose

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

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

Application

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

- 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. If there is an accompanying log, look at the whole picture.

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

Insufficient amount of storage

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

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

- Verifying the file transfer protocol on page 152
- Verifying the FTP Schedule on page 158

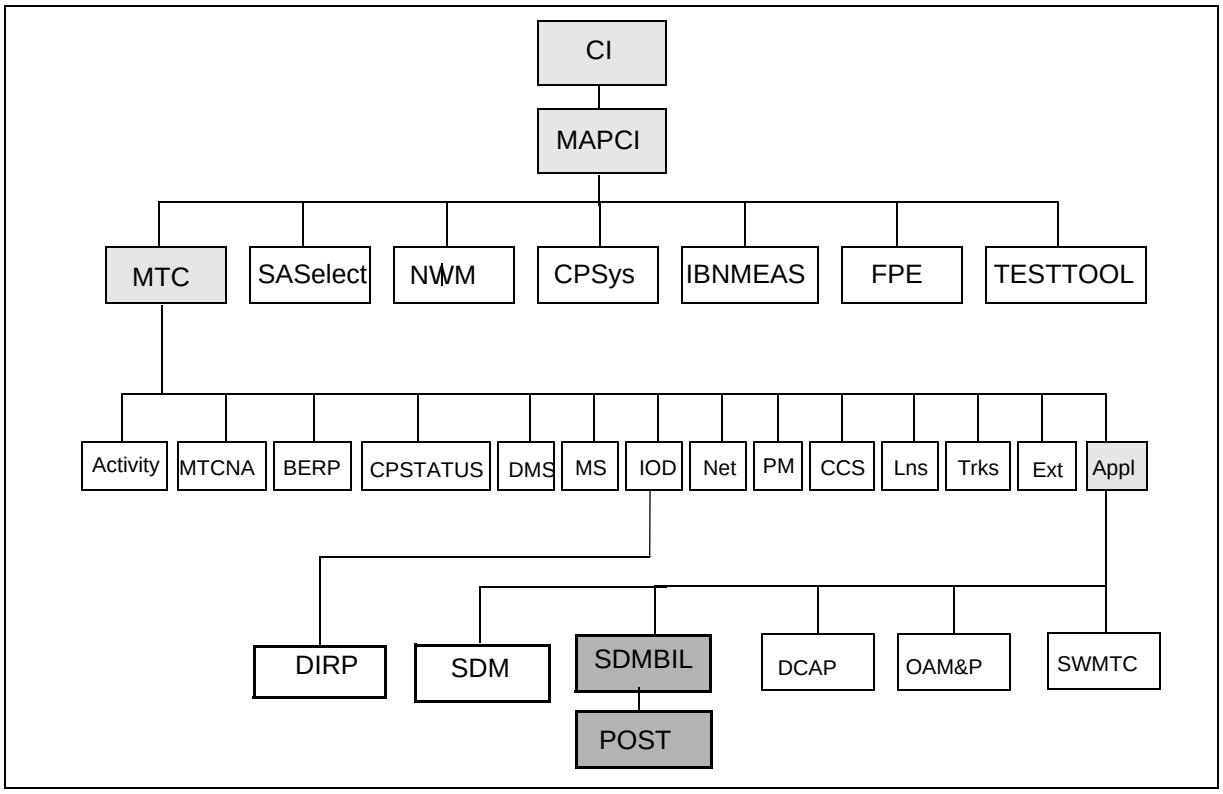
Use the following procedures to clear alarms based on communication problems between the core and the core manager:

- Clearing a DSKWR alarm on a CBM on page 102
- Clearing a NOCOM alarm on page 121
- Clearing a major SBACP alarm on page 143
- Clearing a minor SBACP alarm on page 147

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 on page 54 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 some 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 some communications or internal software error; data is being written to backup files
- Backup (Bkup):
  the stream is writing data to backup files due to a performance problem
- Recovery (Rcvy):
  the stream is in service and also sending backup files previously created to the core manager
- In-service (InSv):
  the stream is in a normal working state
- In-service trouble (ISTb):
  the core manager communication is in service trouble due to being in a split-mode state

Common procedures

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

- Verifying the file transfer protocol on page 152 helps you determine that the FTP process is configured correctly and is able to transfer files
- Verifying the FTP Schedule on page 158 helps you determine that the system is able to send FTP files on a regular basis
- “Configuring SBA backup volumes on the core” in the core manager Accounting document is used to create and activate alternative backup volumes for a stream

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

- Clearing a BAK50 alarm on page 82
- Clearing a BAK70 alarm on page 86
- Clearing a BAK90 alarm on page 90
- Clearing a BAKUP alarm on page 94
- Clearing a NOBAK alarm on page 116
- Clearing a NOREC alarm on page 128
- Clearing a NOSTOR alarm on page 130
- Clearing a NOVOL alarm on page 134

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

None

Action

Displaying SBA logs

At any workstation or console

1 Log into the core manager using the root user ID and password.

2 Access the billing maintenance interface:

```
# billmtc
```

3 Display the logs:

```
> displogs
```

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

4 You have completed this procedure.

Displaying SBA alarms

Purpose

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

Application

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

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

Prerequisites

None

Action

Displaying SBA alarms

At any workstation or console

1 Log into the core manager using the root user ID and password.

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.

Controlling the SDM Billing Application

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

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

At any workstation or console

1 Log in to the CBM.

2 Access the Application level by typing

```
# cbmmtc appl
```

and pressing the Enter key.

The system displays a list of applications.

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

If you want to	Do
busy the SBA	step 3
return the SBA to service	step 5

3

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 SDM Billing Application by typing

```
> bsy <x>
```

and pressing the Enter key.

Where:

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

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 by typing

`> y`

and pressing the Enter key.

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 8
did not busy successfully	contact your next level of support

5 Return the CBM Billing Application to service by typing

`> rts <x>`

and pressing the Enter key.

Where:

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

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

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

If the SBA	Do
returned to service successfully	step 6
did not return to service successfully	contact your next level of support

6 Use the following table to determine your next step.

If the system	Do
generates log SDMB375	step 7
does not generate log SDM375	you have completed this procedure

7 Perform the following steps to return the RTB streams to service:

a Exit the Application level by typing

```
> quit all
```

and pressing the Enter key.

b Access the billing maintenance level by typing

```
# billmtc
```

and pressing the Enter key.

c Access the schedule level by typing

```
> schedule
```

and pressing the Enter key.

d Access the real-time billing level by typing

```
> rtb
```

and pressing the Enter key.

e Busy the stream by typing

```
> bsy <stream name>
```

and pressing the Enter key.

Where:

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

f Return the stream to service by typing

```
> rts <stream name>
```

and pressing the Enter key.

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 8
does not return to service successfully	contact your next level of support

8 Quit the billing maintenance level by typing

```
> quit all
```

and pressing the Enter key.

9 You have completed this procedure

Displaying or storing log records using logreceiver

Purpose

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

Application

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

```
Failed to listen for connection request on port xxx,
exiting
```

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

Storage file

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

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

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

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

Action

Checking the port numbers in use on a workstation

At the client workstation

1 Check the port numbers in use:

```
more/etc/services
```

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

Storing logs in a file

At the client workstation

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

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

where

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

<filename> is the name of the file

Displaying log records on a workstation

At the client workstation

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

```
logreceiver <port>
```

where

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

2 You have completed this procedure.

Retrieving and viewing log records

Purpose

This procedure provides instructions on how to retrieve and view CM and core manager log records using the core manager log query tool.

Application

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

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

Action

Retrieving and viewing logs

At a terminal or terminal session connected to the core manager

1 Log into the core manager.

2 Start the log query tool using the default settings:

```
# logquery
```

Example response:

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

RTEC02CR   * BOOT201 MAR12 14:58:44 7364 INFO Bootp log report
Mac Address : 006038381f87
          MAC addr to node_id lookup failure : 13
          INM 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 your selected command, and press the Enter key.

5 When you are finished, exit the log query tool:

```
> quit
```

6 You have completed this procedure.

Troubleshooting AFT alarms

Purpose

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

Application

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

Indication

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

Meaning

An AFT alarm is generate under the conditions listed in the table AFT alarms.

AFT alarms

Alarm	Occurs when:
Critical (*C*)	• an AFT session network connection has been disrupted during file transfer • the retry count has been exceeded on a file • the message transfer protocol (MTP) timer has expired
Major (M)	an AFT session has been stopped using the AFT level Stop command

Impact

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

Action

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

Clearing critical alarms

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

- delete the tuple from the automaticFileTransferTable
- manually clear the alarm through the Alarm command at the AFT level of the BILLMTC remote maintenance interface (RMI)

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

Clearing major alarms

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

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

Procedure

Use the following procedure to clear an AFT alarm manually.

Clearing an AFT alarm

At the core manager

1 Access the BILLMTC level:

```
> billmtc
```

2 Access the Application (APPL) level:

```
> appl
```

3 Access the Automatic File Transfer (AFT) level:

```
> aft
```

4 Clear the alarm:

```
> alarm cancel <session_name>
```

where:

<session_name> is the unique name of the network connection for which you want to clear the alarm

Example response:

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

5 To cancel the alarms, enter:

```
> yes
```

Example response:

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

6 You have completed this procedure.

Deleting a tuple from automaticFileTransferTable

CAUTION

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

At the core manager

1 Access the BILLMTC level:

```
> billmtc
```

2 Access the APPL level:

```
> appl
```

3 Access the AFT level:

```
> aft
```

4 Access the AFTCONFIG level:

```
> aftconfg
```

5 Delete the tuple from the automaticFileTransferTable:

```
> delete <session_name>
```

where:

<session_name> is the unique name of the network connection that generated the alarm

Example response:

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

6 To delete the table entry (tuple), enter:

```
> yes
```

Example response:

```
Deleted table entry for AFT session:
<session_name>
```

7 You have completed this procedure.

Restarting an AFT session

At the core manager

1 Access the BILLMTC level:

```
> billmtc
```

2 Access the APPL level:

```
> appl
```

3 Access the AFT level:

```
> aft
```

4 Restart the AFT session that generated the alarm:

```
> start <session_name>
```

where:

<session_name> is the unique name of the network connection that generated the alarm

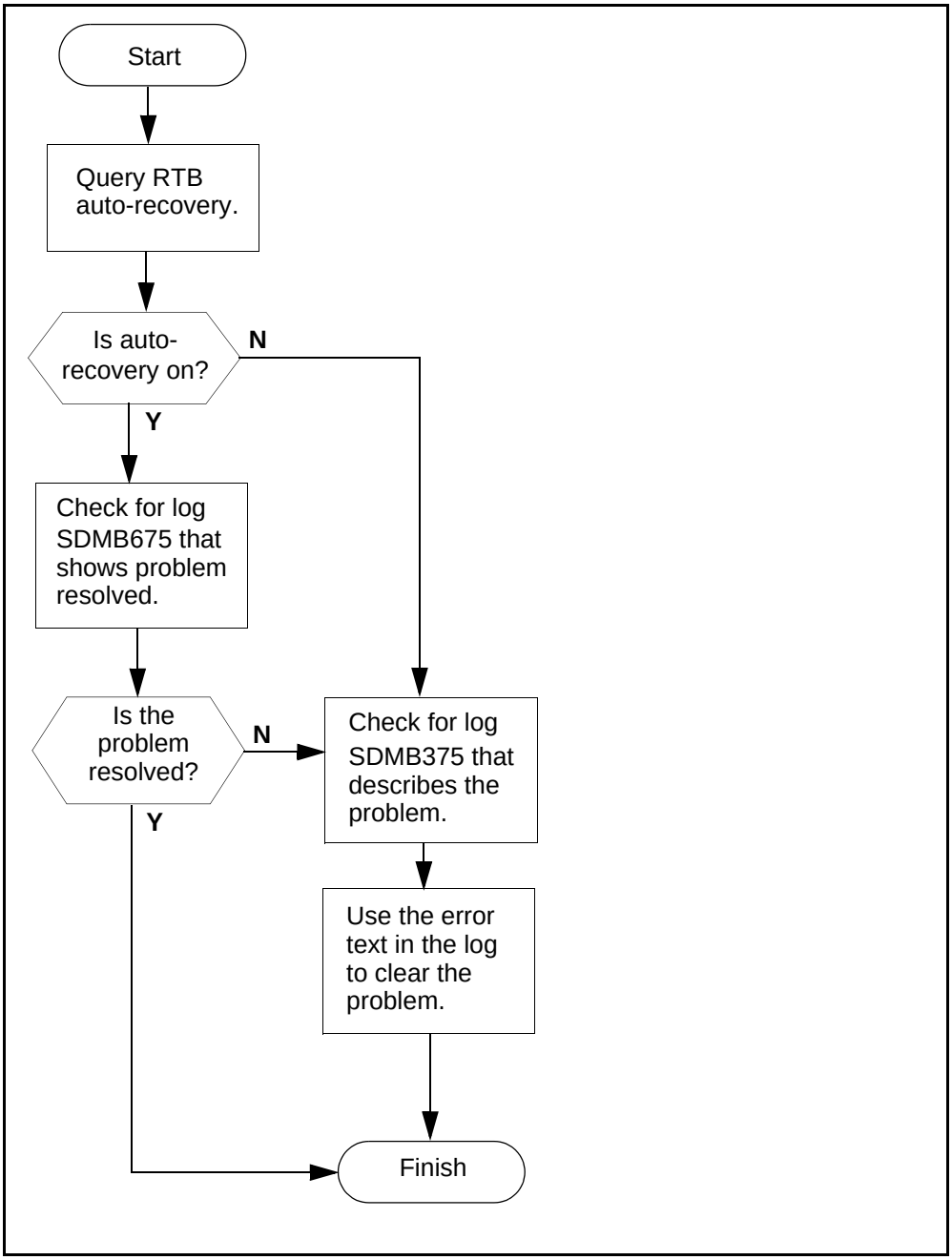
Example response:

```
*** WARNING: Started AFT session:
<session_name>
```

5 You have completed this procedure.

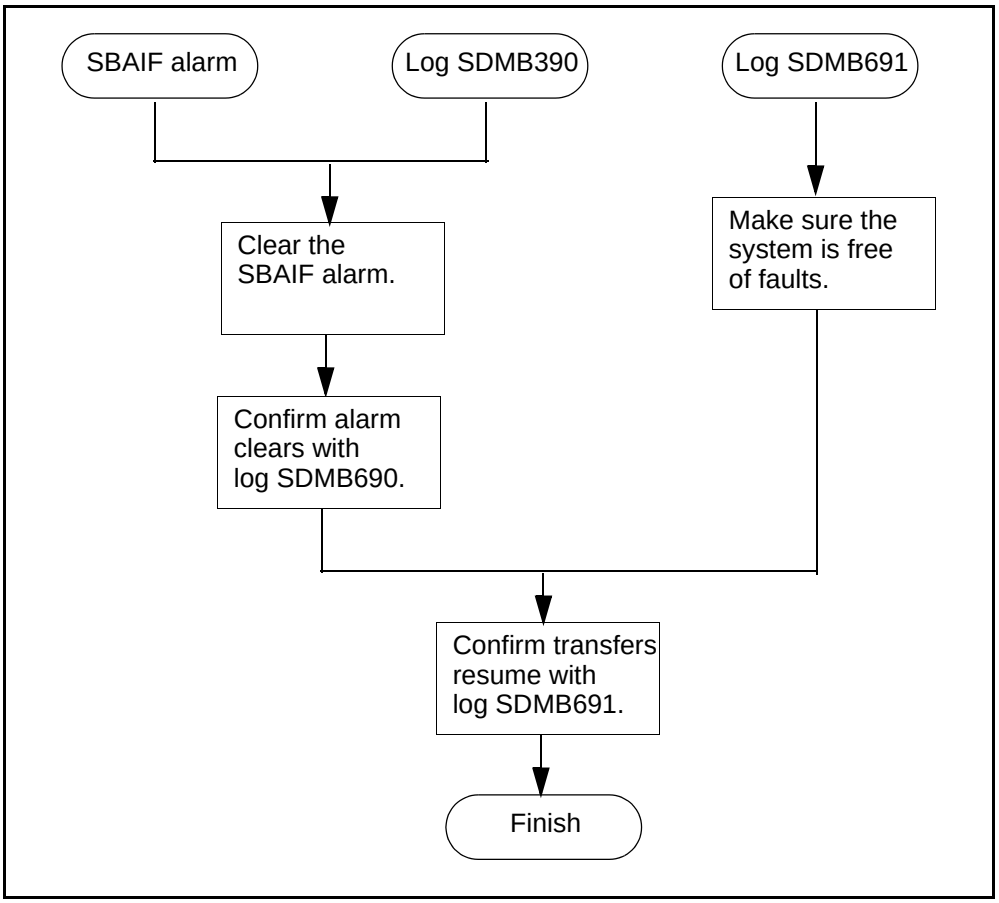
Troubleshooting RTB problems

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



Troubleshooting problems with scheduled billing file transfers

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



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

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

Troubleshooting Log Delivery problems on a CBM

Purpose

Use the procedure to

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

Fault conditions affecting Log Delivery

Lost logs

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

To clear the problem:

- access the Log Delivery commissioning tool
- select the Global Parameters menu, and
- increase the buffer size

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

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 “Configuring log delivery destinations” in the CBM Configuration Management NTP.

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 “Configuring log delivery destinations” in the CBM Configuration Management NTP.

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 unlikely event that all the log devices on the CM are full, the Log Delivery application generates an alarm. The application changes to ISTb and generates an SDM303 log at the RMI.

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

Interval

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

Procedure

Troubleshooting the log delivery application when its state is ISTb

At the local or remote VT100 console

1 Log into the CBM as the root user.

2 Access the maintenance interface:

```
# cbmmtc
```

3 Access the application level (Appl):

```
> appl
```

If GDD is	Do
Offl	step 4
ManB	step 5
InSv	step 6

4 Busy the GDD application:

```
> bsy <fileset_number>
```

where

<fileset_number>
is the number next to the GDD application

5 Return the GDD application to service:

```
> rts <fileset_number>
```

where

<fileset_number>
is the number next to the GDD application on the screen

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

If the Log Delivery application	Do
remains ISTb	step 6
goes InSv	you have completed this procedure

6 Check the CBM for any faults:

```
> querycbm flt
```

If	Do
a fault report indicates “log file is circulating (losing logs)”	step 7
no fault report indicates “log file is circulating (losing logs)”	contact your next level of support
a fault report indicates “no available CM log devices”	step 20

7 Exit the maintenance interface:

```
> quit all
```

8 Access the /gdd directory:

```
# cd /cbmdata/00/gdd
```

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

9 Check all log files:

```
# ls -l
```

10 Determine if there are any files present that are not log files.

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

If	Do
there are files present that do not start with LOGS.recorddata	step 11
all files start with LOGS.recorddata	step 17

11 Delete files that are not log files:

```
# rm <file>
```

where

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

Note: Once you remove the file, there is no way to restore it.

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 by typing

```
#  filesys grow -m /cbmdata/00/gdd -s
<size>{m,g}
```

Where

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

Note 1: Once you have increased the size of a file system, you cannot decrease it.

Note 2: 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

3Mb

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

20 Busy the Log Delivery application:

```
> bsy <fileset_number>
```

where

<fileset_number>
is the number next to the GDD application

21 Return the Log Delivery application to service:

```
> rts <fileset_number>
```

where

<fileset_number>
is the number next to the GDD application

22 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 23

23 You have completed this procedure.

Clearing a BAK50 alarm

Purpose

Use this procedure to clear a BAK50 alarm.

Indication

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

Meaning

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

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

ATTENTION

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

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

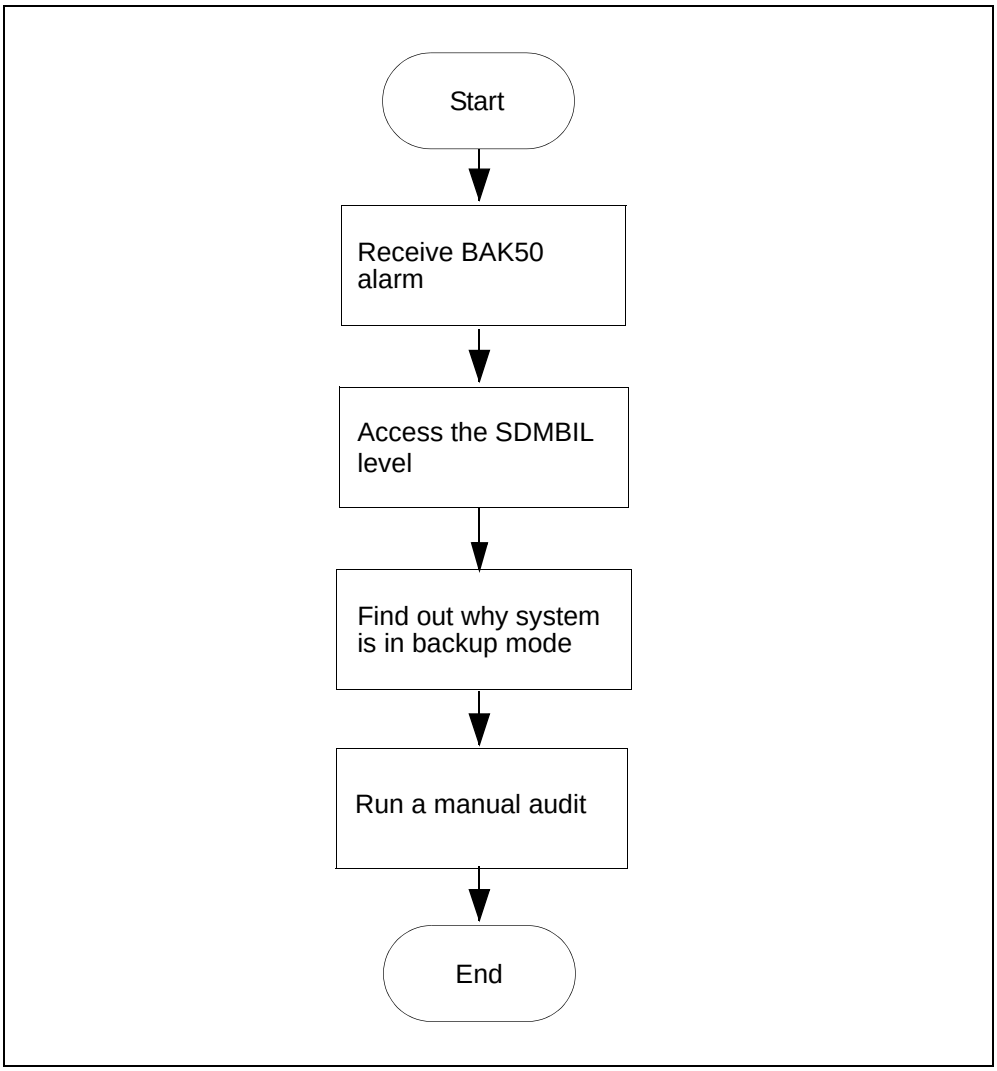
Impact

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

Procedure

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

BAK50 alarm clearing flowchart



Clearing a BAK50 alarm

At the MAP

1 Post the billing stream:

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

where

<stream_name> is the name of the billing stream.

2 Determine why the system is in backup mode.

3 Display all 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 that addresses the alarm or the condition that displays, and then return to step 5.
RBsy	refer to Clearing a major SBACP alarm on page 143, and then return to step 5.
ManB	Go to step 7
Bkup	Go to step 7

5 Use Audit to clear the alarm.

If the alarm	Do
cleared	step 6
did not clear	step 7

6 Ensure that the billing system is in recovery:

```
> post <streamname>
```

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

If the billing system	Do
is in recovery (Rcvy)	step 10
is not in recovery	contact your next level of support

7 Perform the procedure Adjusting disk space in response to SBA backup file system alarms on page 98

8 Use Audit to clear the alarm.

If the alarm	Do
cleared	step 9
did not clear	contact your next level of support

9 Ensure that the billing system is in recovery:

```
> post <streamname>
```

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

If the billing system	Do
is in recovery (Rcvy)	step 10
is not in recovery	contact your next level of support

10 You have completed this procedure.

Clearing a BAK70 alarm

Purpose

Use this procedure to clear a BAK70 alarm.

Indication

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

Meaning

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

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

ATTENTION

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

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

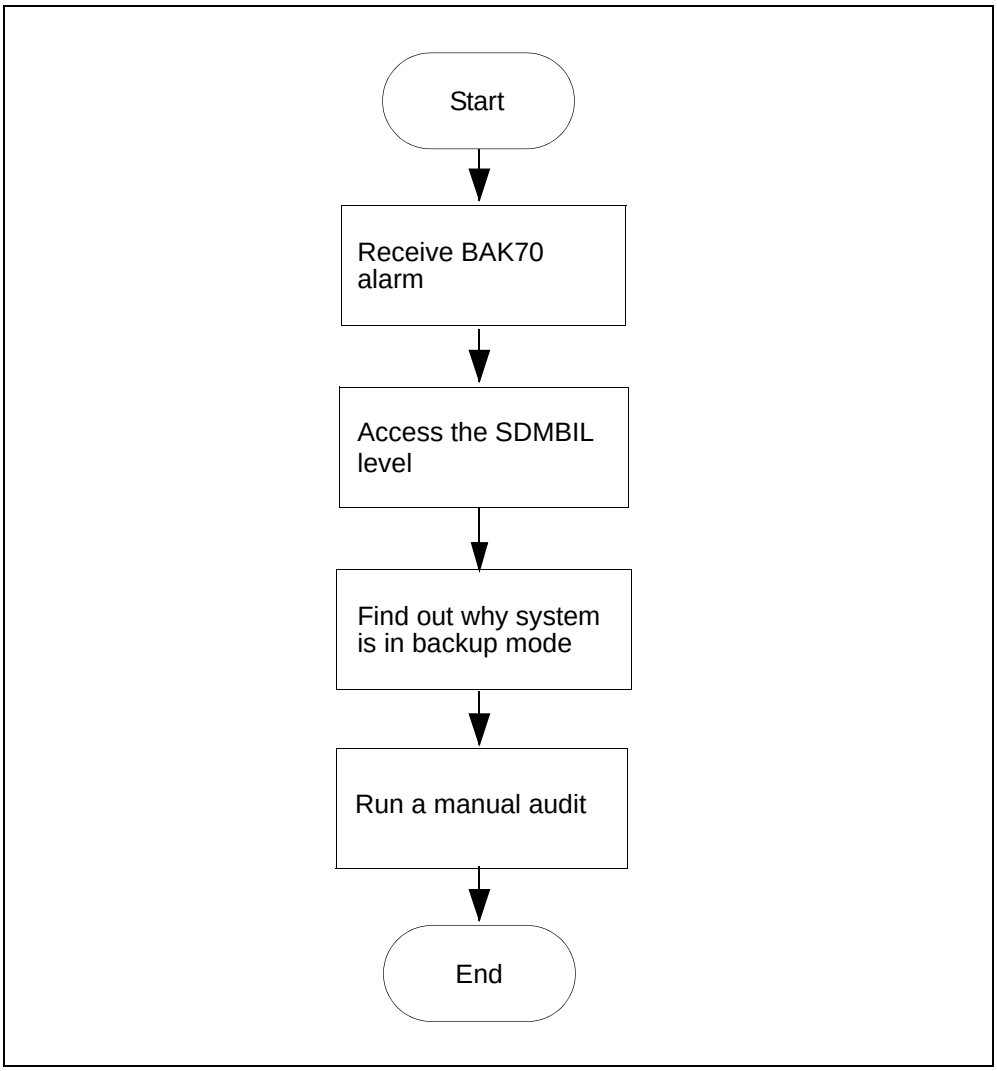
Impact

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

Procedure

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

BAK70 alarm clearing flowchart



Clearing a BAK70 alarm

At the MAP

1 Post the billing stream:

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

where

<billing_stream> is the name of the billing stream.

2 Determine why the system is in backup mode.

3 Display all of the alarms that have been raised:

```
> DispAL
```

4 Determine the state of the billing stream.

If the billing stream is	Perform the following steps
SysB	perform the procedure that addresses the alarm or the condition that displays, and then return to step 5.
RBsy	refer to Clearing a major SBACP alarm on page 143, and then return to step 5.
ManB	Go to step 7
Bkup	Go to step 7

5 Use Audit to clear the alarm.

If the alarm	Do
cleared	step 6
did not clear	step 7

6 Ensure that the billing system is in recovery:

```
> post <streamname>
```

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

If the billing system	Do
is in recovery (Rcvy)	step 10
is not in recovery	contact your next level of support

7 Perform the procedure Adjusting disk space in response to SBA backup file system alarms on page 98

8 Use Audit to clear the alarm.

If the alarm	Do
cleared	step 9
did not clear	contact your next level of support

9 Ensure that the billing system is in recovery:

```
> post <streamname>
```

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

If the billing system	Do
is in recovery (Rcvy)	step 10
is not in recovery	contact your next level of support

10 You have completed this procedure.

Clearing a BAK90 alarm

Purpose

Use this procedure to clear a BAK90 alarm.

Indication

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

Meaning

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

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

ATTENTION

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

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

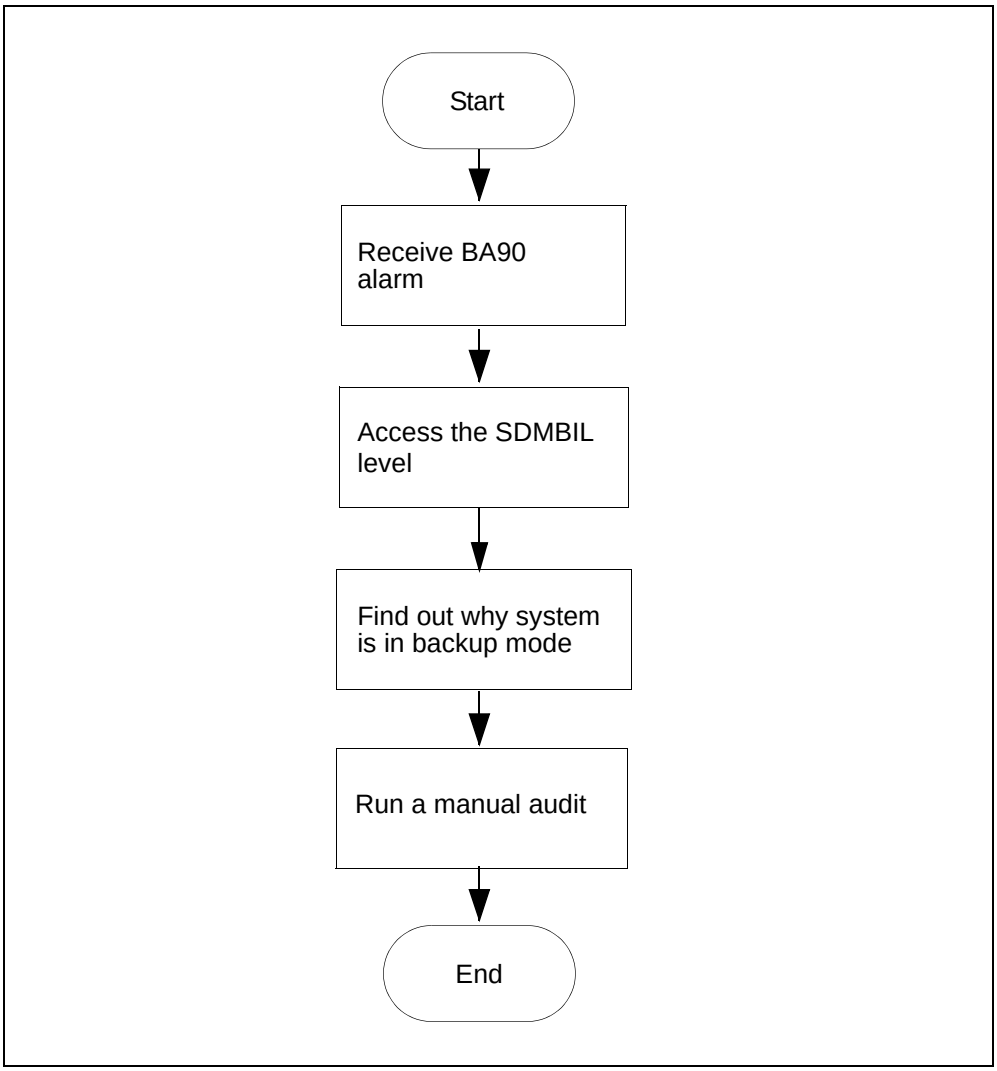
Impact

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

Procedure

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

BAK90 alarm clearing flowchart



Clearing a BAK90 alarm

At the MAP

1 Post the billing stream:

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

where

<billing_stream> is the name of the billing stream.

2 Determine why the system is in backup mode.

3 Display all alarms that have been raised:

```
> DispAL
```

4 Determine the state of the billing stream.

If the billing stream is	Perform the following steps
SysB	perform the procedure that addresses the alarm or the condition that displays, and then return to step 5.
RBsy	refer to Clearing a major SBACP alarm on page 143, and then return to step 5.
ManB	Go to step 7
Bkup	Go to step 7

5 Use Audit to clear the alarm.

If the alarm	Do
cleared	step 6
did not clear	step 7

6 Ensure that the billing system is in recovery:

```
> post <streamname>
```

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

If the billing system	Do
is in recovery (Rcvy)	step 10
is not in recovery	contact your next level of support

7 Perform the procedure Adjusting disk space in response to SBA backup file system alarms on page 98

8 Use Audit to clear the alarm.

If the alarm	Do
cleared	step 9
did not clear	contact your next level of support

9 Ensure that the billing system is in recovery:

```
> post <streamname>
```

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

If the billing system	Do
is in recovery (Rcvy)	step 10
is not in recovery	contact your next level of support

10 You have completed this procedure.

Clearing a BAKUP alarm

Purpose

Use this procedure to clear a BAKUP alarm.

Indication

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

Meaning

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

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

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

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

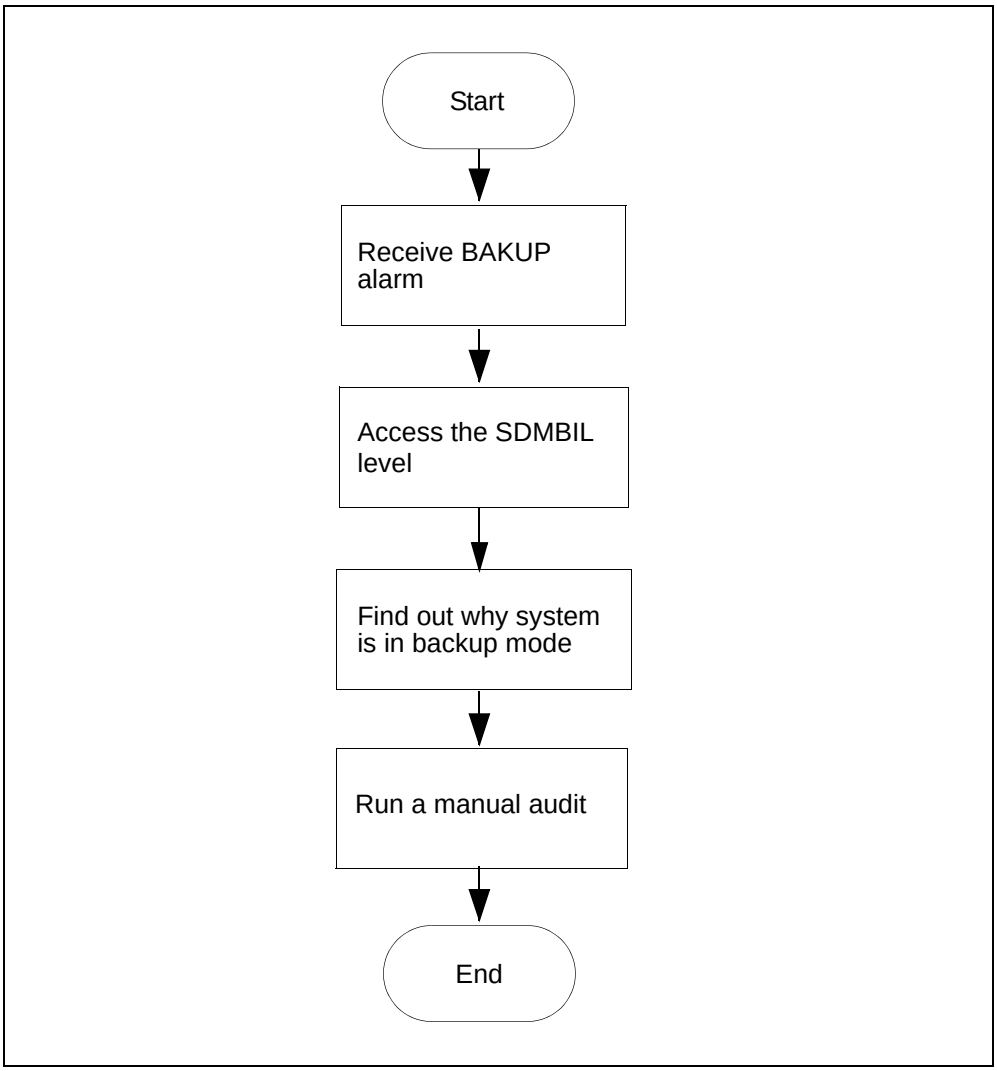
Impact

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

Procedure

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

BAKUP alarm clearing flowchart



Clearing a BAKUP alarm

At the MAP

1 Post the billing stream:

```
> mapci;mtc;appl;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 that addresses the alarm or the condition that displays, and then return to step 5.
RBsy	refer to Clearing a major SBACP alarm on page 143, and then return to step 5.
ManB	Go to step 7
Bkup	Go to step 7

5 Use Audit to clear the alarm.

If the alarm	Do
cleared	step 6
did not clear	step 7

6 Ensure that the billing system is in recovery:

```
> post <streamname>
```

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

If the billing system	Do
is in recovery (Rcvy)	step 10
is not in recovery	contact your next level of support

7 Perform the procedure Adjusting disk space in response to SBA backup file system alarms on page 98

8 Use Audit to clear the alarm.

If the alarm	Do
cleared	step 9
did not clear	contact your next level of support

9 Ensure that the billing system is in recovery:

```
> post <streamname>
```

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

If the billing system	Do
is in recovery (Rcvy)	step 10
is not in recovery	contact your next level of support

10 You have completed this procedure.

Adjusting disk space in response to SBA backup file system alarms

This procedure is used 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

At the MAP

1 Post the billing stream by typing

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

and pressing the Enter key.

Where

<x> is the name of the billing stream.

2 Display the names of the backup volumes configured for the stream by typing

`> conf view <x>`

and pressing the Enter key.

Where

<x> is the name of the billing stream.

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

If the backup volumes are located on	Do
DDU disks	step 4
IOP disks	step 5
SLM disks	step 5
3PC disks	step 5

4 Display and record the size of a volume and its number of free blocks by typing

`> dskut;sv <volume name>`

and pressing the Enter key.

Where

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

Repeat this step for each volume name that you recorded in step 2 and then proceed to step 6.

5 Display and record the size of a volume and its number of free blocks by typing

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

and pressing the Enter key.

Where

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

Repeat this step for each volume name that you recorded in step 2.

6 Refer to the following table to determine your next step.

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 NTP for your core manager.

7 You have completed this procedure.

Clearing a CDRT alarm

Purpose

Use this procedure to clear a CDRT alarm.

Indication

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

Meaning

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

At the MAP

1 You can determine the value of the active template ID on the DMS/CM:

```
> CTMPLT “template all”
```

2 You can 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.

Note 1: 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.

Note 2: If the alarm persists, refer to the contact your next level of support.

Clearing a DSKWR alarm on a CBM

Indication

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

Meaning

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

Impact

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

Action

Use the following procedure to clear DSKWR alarm.

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.

Clearing a DSKWR alarm

At the MAP interface on the CM

1 Access the SDMBIL level by typing

```
> mapci;mtc;appl;sdmbil
```

and pressing the Enter key.

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

```
> dispal
```

and pressing the Enter key.

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

If the NOBAK or NOSTOR alarm	Do
appears in the alarm banner	perform the procedure "Configuring SBA backup volumes on the core" in the NTP NN10363-811.
does not appear in the alarm banner	step 4

At your workstation

4 Check to see if any logs have been raised that indicate a problem with the system's disks, by performing the procedure, Displaying customer logs on a Sun server on page 229.

5 Determine whether the file system holding the billing files has adequate space by performing the procedure, Verifying disk space on a Sun server on page 231.

6 If you want to back up the billing files, perform the procedure "Copying files to DVD" in the NTP NN10363-811.

7 Using the information you obtained in step 5 determine whether the file system is full. The file system can be full if you have not sent the primary files downstream. If you feel that the capacity of the SBA file system requires adjustment, contact your next level of support.

If	Do
you want to send the billing files downstream	step 8
you feel that the capacity of the SBA file system requires adjustment	contact your next level of support

8 Access the BILLMTC interface by typing

```
> billmtc
```

and pressing the Enter key.

9 Access the FILESYS level by typing

```
> filesys
```

and pressing the Enter key.

10 Send the primary billing files to the downstream processor by typing

`> sendfile <x>`

and pressing the Enter key.

Where:

<x> is the name of the stream.

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

11 Refer to the following table to determine your next step.

If the SENDFILE command	Do
is not successful	refer to procedures Verifying the file transfer protocol and Verifying the FTP Schedule, then return to this procedure and repeat step 10
is successful	step 12
is not successful after you have performed the "Verifying the file transfer protocol" and "Verifying the FTP Schedule" procedures	contact your next level of support

12 Use Audit to clear the alarm

If the alarm	Do
cleared	step 20
did not clear	step 13

13 Quit the BILLMTC interface by typing

`> quit all`

and pressing the Enter key.

14 At the prompt, check for orphan files and for files someone else copied to the logical volume of your billing stream by typing

`> ls /<stream>/<x>/orphan`

and pressing the Enter key.

Where:

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

<x> is the name of the billing stream.

If	Do
your billing files are full because they have accumulated in orphan files and you are unclear as to how to clean up the billing directory	contact your next level of support
your billing files are full because they have accumulated in orphan files and you have cleaned up the billing directory and are still incurring a problem	step 15

15 Verify the write permission and ownership for the directories in the billing stream by typing:

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

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

<x> is the name of the billing stream.

16 Refer the following table to determine your next step.

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 r-x r-x	step 17
ownership for a directory is not maint	step 18
the alarm fails to clear	contact your next level of support

17 Change the permissions for a directory by typing

`> chmod 755 <directory>`

and pressing the Enter key.

Where:

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

18 Change the ownership of a directory by typing

`> chown maint:maint <directory>`

and pressing the Enter key.

Where:

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

19 Use Audit to clear the alarm

If the alarm	Do
cleared	step 20
did not clear	contact your next level of support

20 You have completed this procedure.

Clearing an FTP alarm

Purpose

Use this procedure to clear an FTP alarm.

Indication

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

Meaning

The FTP process failed. The SDMB logs provide details about the FTP problem. This alarm can be either critical or major.

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

Impact

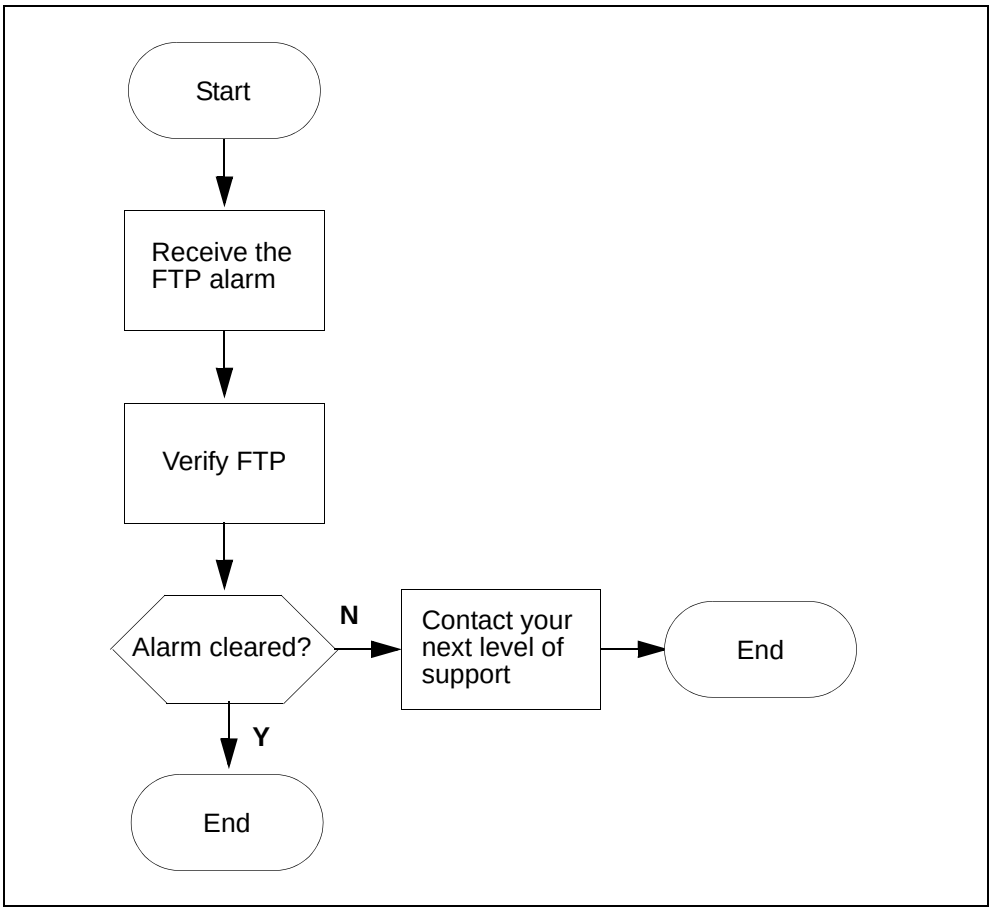
The core manager cannot FTP files to the downstream destination. It is possible that the core manager has reached its storage capacity limit, depending on the amount of storage and the volume of records.

As the core manager storage becomes full, alarms notify you of how much of its capacity is used. When this storage is full, the DMS/CM sends subsequent records to backup storage.

Action

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

FTP alarm clearing flowchart



Clearing an FTP alarm

At the MAP

1 Examine the SDMB logs for details about the FTP problem:

```
> logutil;open sdmb
```

Note: This command displays the most recent logs.

2 Verify that the FTP is working by performing Verifying the file transfer protocol on page 152 in this document.

3 If the alarm fails to clear, contact your next level of support.

4 You have completed the procedure.

Clearing an FTPW alarm

Purpose

Use this procedure to clear an FTPW alarm.

Indication

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

Meaning

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

Note: The FTPW alarm may be present on the CM for a non-existent schedule. For example, if an operator

- shut 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

the FTPW alarm is generated.

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

At the core manager

1 Complete procedure Verifying the file transfer protocol on page 152 in this document.

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

2 If you determine that the alarm was raised for a non-existent schedule, 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 CBM Accounting document, then return to this procedure.

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

4 You have completed the procedure.

Clearing an inbound file transfer alarm

Purpose

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

Indication

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

Meaning

The IFT alarm indicates the occurrence of an inbound file transfer. This alarm is raised if the link in the ftpdir directory of a stream cannot be managed or if access to a ftpdir directory is not capable. 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 attempts for the billing stream are not successful.

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:

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

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

Clearing an IFT alarm

At the MAP

1 Log in to the core manager as maint user.

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

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

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

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

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

5 Remove the <rcLogicalVolumeDirectory>/ftpdir directory:

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

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

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

6 You have completed the procedure.

Clearing an LODSK alarm

Purpose

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

Indication

CAUTION
Possible Loss of Service
If you receive a LODSK alarm, transfer (FTP) the billing files in the closedNotSent directory, or write to tape immediately. Refer to Verifying the file transfer protocol on page 152 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.

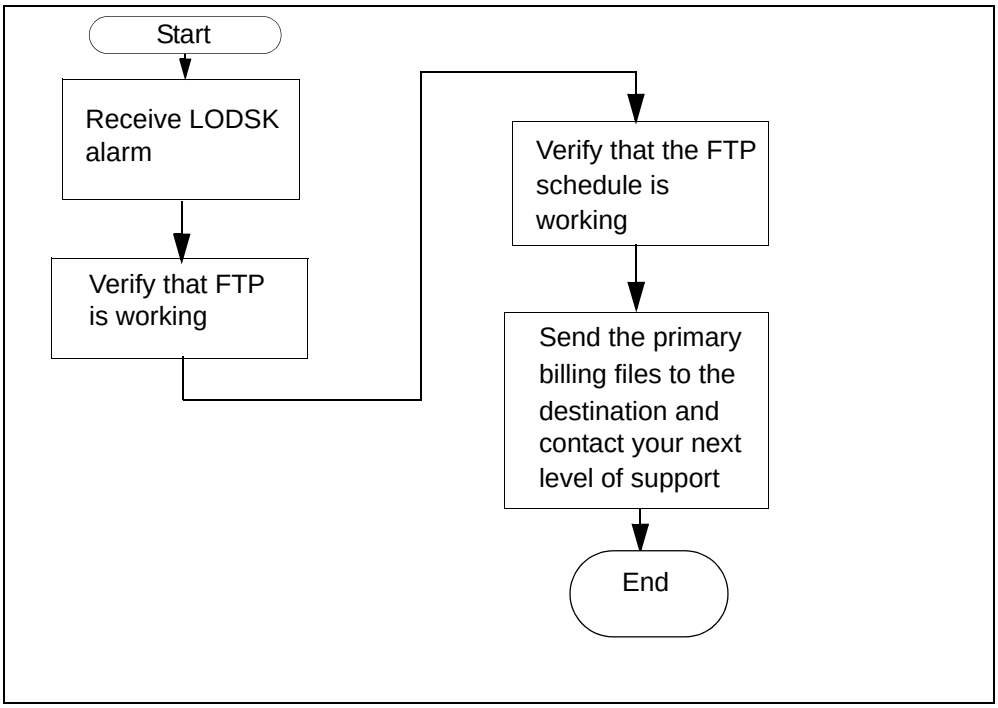
Impact

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 if the disks reach 100 percent capacity.

Action

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

LODSK alarm clearing flowchart



Clearing a LODSK alarm

At the MAP

1 Use the procedure Verifying the file transfer protocol on page 152 to determine if the FTP is working properly.

If the alarm	Do
clears	you have completed this procedure
does not clear	refer to procedure Verifying the FTP Schedule on page 158 in this document
does not clear after you have performed the procedure	contact your next level of support

Clearing a NOBAK alarm

Purpose

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

Indication

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

Meaning

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

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

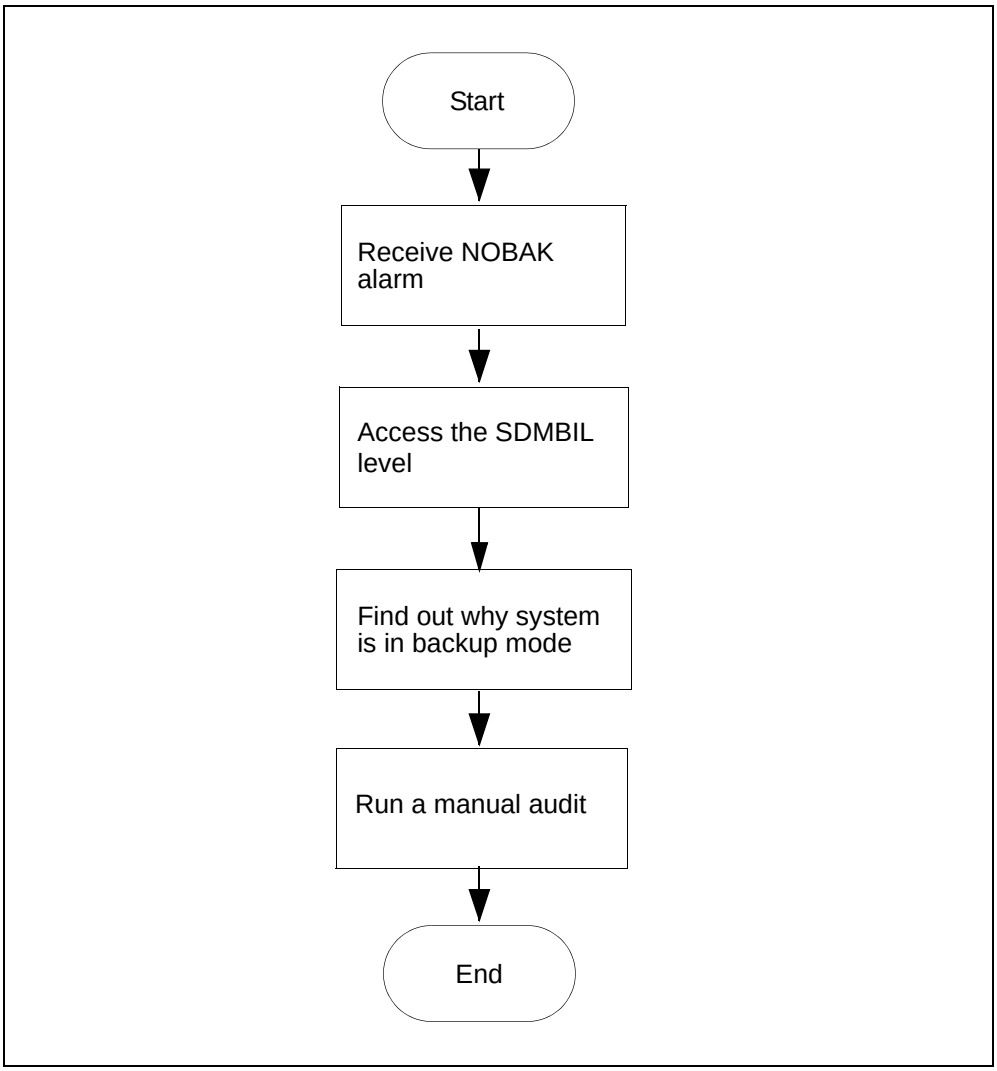
ATTENTION

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

Procedure

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

NOBAK alarm clearing flowchart



Clearing a NOBAK alarm

At the MAP

1 Post the billing stream:

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

where

<billing_stream> is the name of the billing stream

2 Determine why the system is in backup mode.

3 Display all alarms that have been raised:

```
> DispAL
```

4 Determine the state of the billing stream.

If the billing stream is	Perform the following steps
SysB	perform the procedure that addresses the alarm or the condition that displays, and then return to step 5.
RBsy	refer to Clearing a major SBACP alarm on page 143, and then return to step 5.
ManB	Go to step 7
Bkup	Go to step 7

5 Use Audit to clear the alarm.

If the alarm	Do
cleared	step 6
did not clear	step 7

6 Ensure that the billing system is in recovery:

```
> post <streamname>
```

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

If the billing system	Do
is in recovery (Rcvy)	step 10
is not in recovery	contact your next level of support

7 Perform the procedure Adjusting disk space in response to SBA backup file system alarms on page 98

8 Use Audit to clear the alarm.

If the alarm	Do
cleared	step 9
did not clear	contact your next level of support

9 Ensure that the billing system is in recovery:

```
> post <streamname>
```

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

If the billing system	Do
is in recovery (Rcvy)	step 10
is not in recovery	contact your next level of support

10 You have completed this procedure.

Clearing a NOCLNT alarm

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.

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

Impact

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

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

Action

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

Clearing a NOCOM alarm

Purpose

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

Indication

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

Meaning

Communications between the core and the core manager is disrupted.

The most likely causes of this alarm are

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

Impact

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

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

ATTENTION

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

Action

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

At the MAP

1 Access the APPL SDM Menu level:

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

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

2 Busy the core manager:

```
> bsy
```

3 Return the core manager to service:

```
> rts
```

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

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

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

4 Determine the status of the alarm.

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

At the core manager

5 Check for log SDMB375.

If the system	Do
generates log SDMB375	step 6
does not generate log SDM375	you have completed this procedure

6 Access the billing maintenance level:

```
# billmtc
```

7 Access the schedule level:

```
> schedule
```

8 Access the real-time billing level:

```
> rtb
```

9 Busy the stream:

```
> bsy <stream_name>
```

where:

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

10 Return the stream to service:

```
> rts <stream_name>
```

where:

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

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

Clearing a NOFL alarm

Purpose

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

Indication

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

Meaning

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

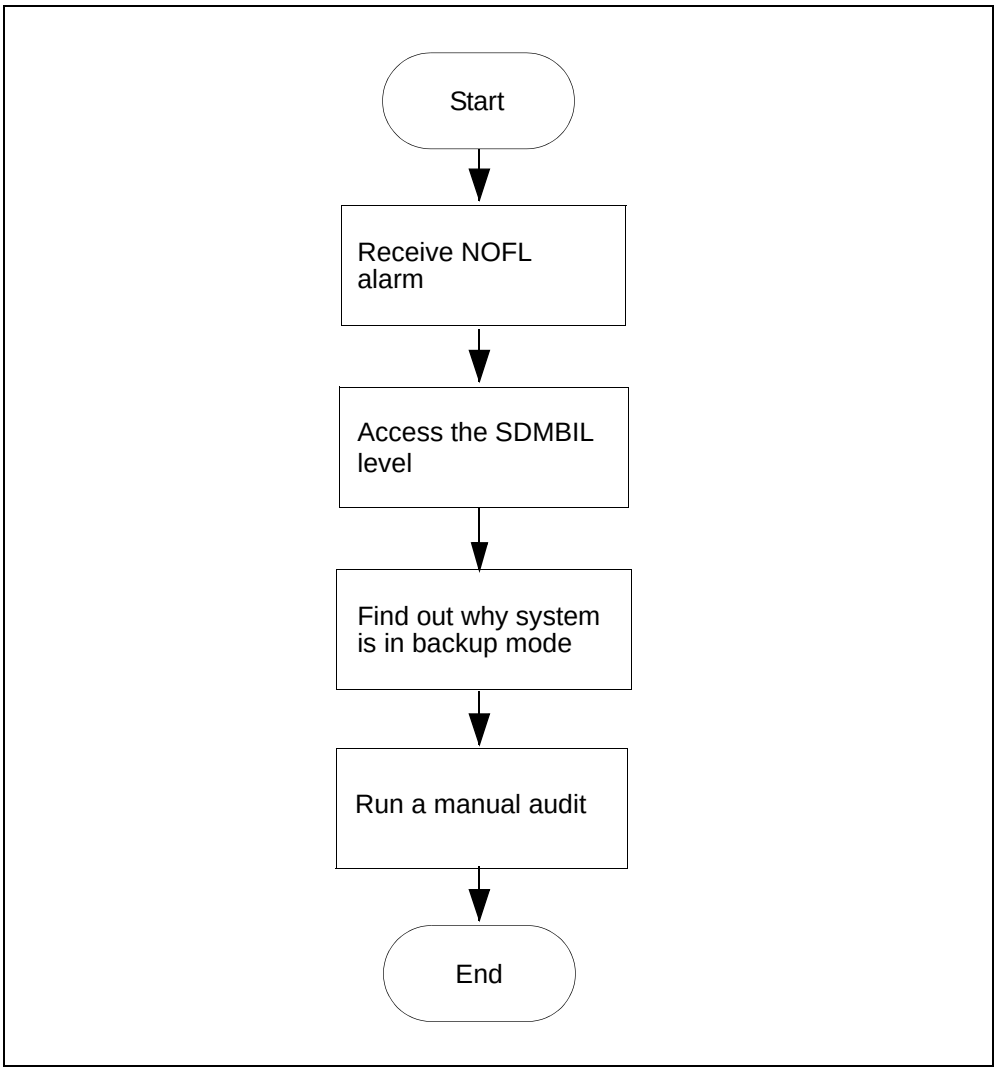
Impact

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

Procedure

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

NOFL alarm clearing flowchart



Clearing a NOFL alarm

At the MAP

1 Post the billing stream:

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

where

<stream_name> is the name of the billing stream.

2 Determine why the system is in backup mode.

3 Display all alarms that have been raised:

```
> DispAL
```

4 Determine the status of the billing stream.

If the billing stream is	Perform the following steps
SysB	perform the procedure that addresses the alarm or the condition that displays, and then return to step 5.
RBsy	refer to Clearing a major SBACP alarm on page 143, and then return to step 5.
ManB	Go to step 7
Bkup	Go to step 7

5 Use Audit to clear the alarm.

If the alarm	Do
cleared	step 6
did not clear	step 7

6 Ensure that the billing system is in recovery:

```
> post <streamname>
```

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

If the billing system	Do
is in recovery (Rcvy)	step 10
is not in recovery	contact your next level of support

7 Perform the procedure Adjusting disk space in response to SBA backup file system alarms on page 98

8 Use Audit to clear the alarm.

If the alarm	Do
cleared	step 9
did not clear	contact your next level of support

9 Ensure that the billing system is in recovery:

```
> post <streamname>
```

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

If the billing system	Do
is in recovery (Rcvy)	step 10
is not in recovery	contact your next level of support

10 You have completed this procedure.

Clearing a NOREC alarm

Indication

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

Meaning

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

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

If the stream is set to `on`, the alarm is major, and if the stream is set to `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.

Meaning

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

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

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

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

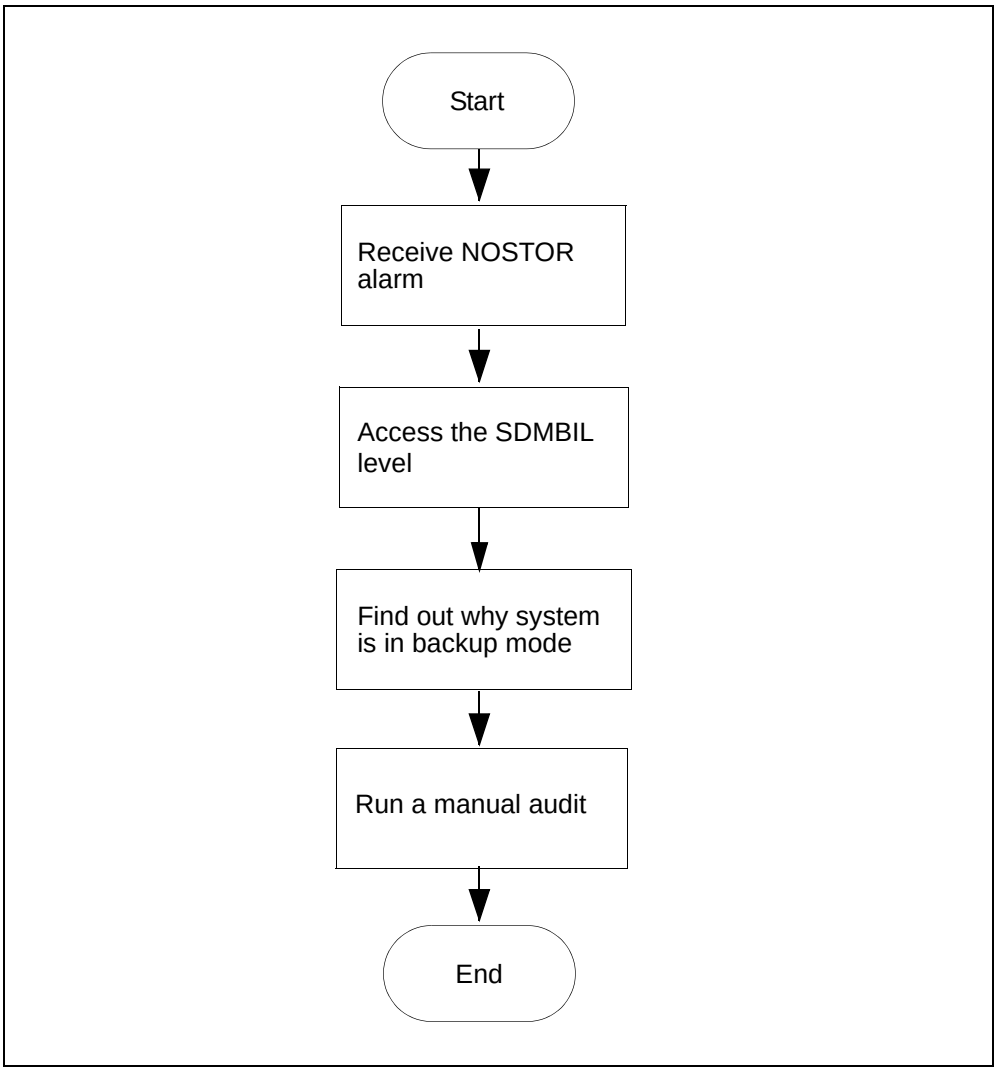
ATTENTION

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



Clearing a NOSTOR alarm

At the MAP

1 Post the billing stream:

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

where

<stream_name> is the name of the billing stream

2 Determine why the system is in backup mode.

3 Display all alarms that have been raised:

```
> DispAL
```

4 Determine the state of the billing stream.

If the billing stream is	Perform the following steps
SysB	perform the procedure that addresses the alarm or the condition that displays, and then return to step 5.
RBsy	refer to Clearing a major SBACP alarm on page 143, and then return to step 5.
ManB	Go to step 7
Bkup	Go to step 7

5 Use Audit to clear the alarm.

If the alarm	Do
cleared	step 6
did not clear	step 7

6 Ensure that the billing system is in recovery:

```
> post <streamname>
```

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

If the billing system	Do
is in recovery (Rcvy)	step 10
is not in recovery	contact your next level of support

7 Perform the procedure Adjusting disk space in response to SBA backup file system alarms on page 98

8 Use Audit to clear the alarm.

If the alarm	Do
cleared	step 9
did not clear	contact your next level of support

9 Ensure that the billing system is in recovery:

```
> post <streamname>
```

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

If the billing system	Do
is in recovery (Rcvy)	step 10
is not in recovery	contact your next level of support

10 You have completed this procedure.

Clearing a NOVOL alarm

Purpose

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

Indication

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

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.

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

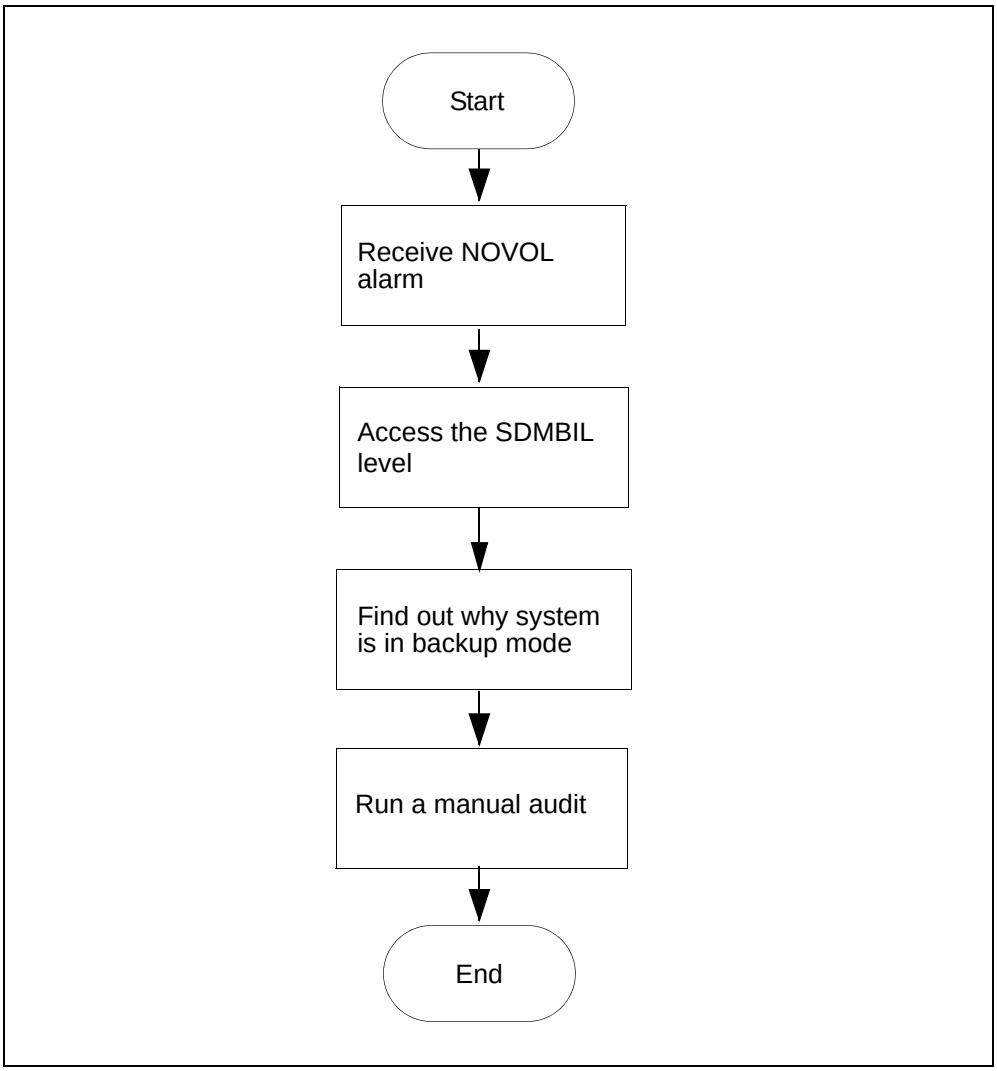
Impact

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



Clearing a NOVOL alarm

At the MAP

1 Post the billing stream:

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

where

<stream_name> is the name of the billing stream

2 Determine why the system is in backup mode.

3 Display all alarms that have been raised:

```
> DispAL
```

4 Determine the status of the billing stream.

If the billing stream is	Perform the following steps
SysB	perform the procedure that addresses the alarm or the condition that is displayed, and then return to step 5.
RBsy	refer to Clearing a major SBACP alarm on page 143, and then return to step 5.
ManB	Go to step 7
Bkup	Go to step 7

5 Use Audit to clear the alarm.

If the alarm	Do
cleared	step 6
did not clear	step 7

6 Ensure that the billing system is in recovery:

```
> post <streamname>
```

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

If the billing system	Do
is in recovery (Rcvy)	step 10
is not in recovery	contact your next level of support

7 Perform the procedure Adjusting disk space in response to SBA backup file system alarms on page 98

8 Use Audit to clear the alarm.

If the alarm	Do
cleared	step 9
did not clear	contact your next level of support

9 Ensure that the billing system is in recovery:

```
> post <streamname>
```

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

If the billing system	Do
is in recovery (Rcvy)	step 10
is not in recovery	contact your next level of support

10 You have completed this procedure.

Clearing an RTBCF alarm

Indication

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

Meaning

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

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.

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.

Action

At the MAP

1 Read the text in log SDMB375 for the cause of error.

2 Use the Logs reference documentation for SDMB375 to determine the actions to take to clear each type of error.

3 After you correct the error, return the RTB destination to service.

The system generates SDMB675 when the error is corrected and the alarm is cleared.

Clearing an RTBFM alarm

Purpose

Use this procedure to clear an RTBFM alarm.

Indication

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

Meaning

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

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.

Impact

RTB moves to the SysB state.

Action

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

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

The RTB stream will 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.

Meaning

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

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.

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.

Meaning

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

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.

Impact

RTB moves to the SysB state.

Action

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

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

If required, contact your next level of support.

Clearing a major SBACP alarm

Purpose

Use this procedure to clear an SBACP alarm.

Indication

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

Meaning

The SBA is shutting down because a user either

- busied the SBA or the core manager, or
- a process keeps dying and the SBA shut down

Impact

The SBA is out of service.

Action

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

At the MAP

1 Access the APPL SDM Menu level:

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

If the core manager is	Do
Offl or SysB	step 2
ManB	step 3
InSv or ISTb	step 6

2 Busy the core manager:

```
> bsy
```

3 Return the core manager to service:

```
> rts
```

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

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

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

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

At the core manager

4 Access the Appl level:

```
> appl
```

If the SBA application is	Do
ISTB, Offl, or SysB	step 5
ManB	step 6
InSv, and the alarm is no longer present	step 13
InSv, but the alarm is still present	contact your next level of support

5 Busy the SBA application:

```
> bsy <SBA_no>
```

where

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

6 Return the SBA application to service:

```
> rts <SBA_no>
```

where

<SBA_no> is the number of the SBA application.

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

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

If the SBA	Do
returned to service successfully and the alarm is no longer present	step 7
returned to service successfully and the alarm is still present	contact your next level of support
did not return to service successfully	contact your next level of support

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

```
> quit all
```

8 Access the billing maintenance level:

```
# billmtc
```

9 Access the schedule level:

```
> schedule
```

10 Access the real-time billing level:

```
> rtb
```

11 Busy the stream:

```
> bsy <stream name>
```

where:

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

12 Return the stream to service:

```
> rts <stream name>
```

where:

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

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

13 You have completed this procedure.

Clearing a minor SBACP alarm

Indication

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

Meaning

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

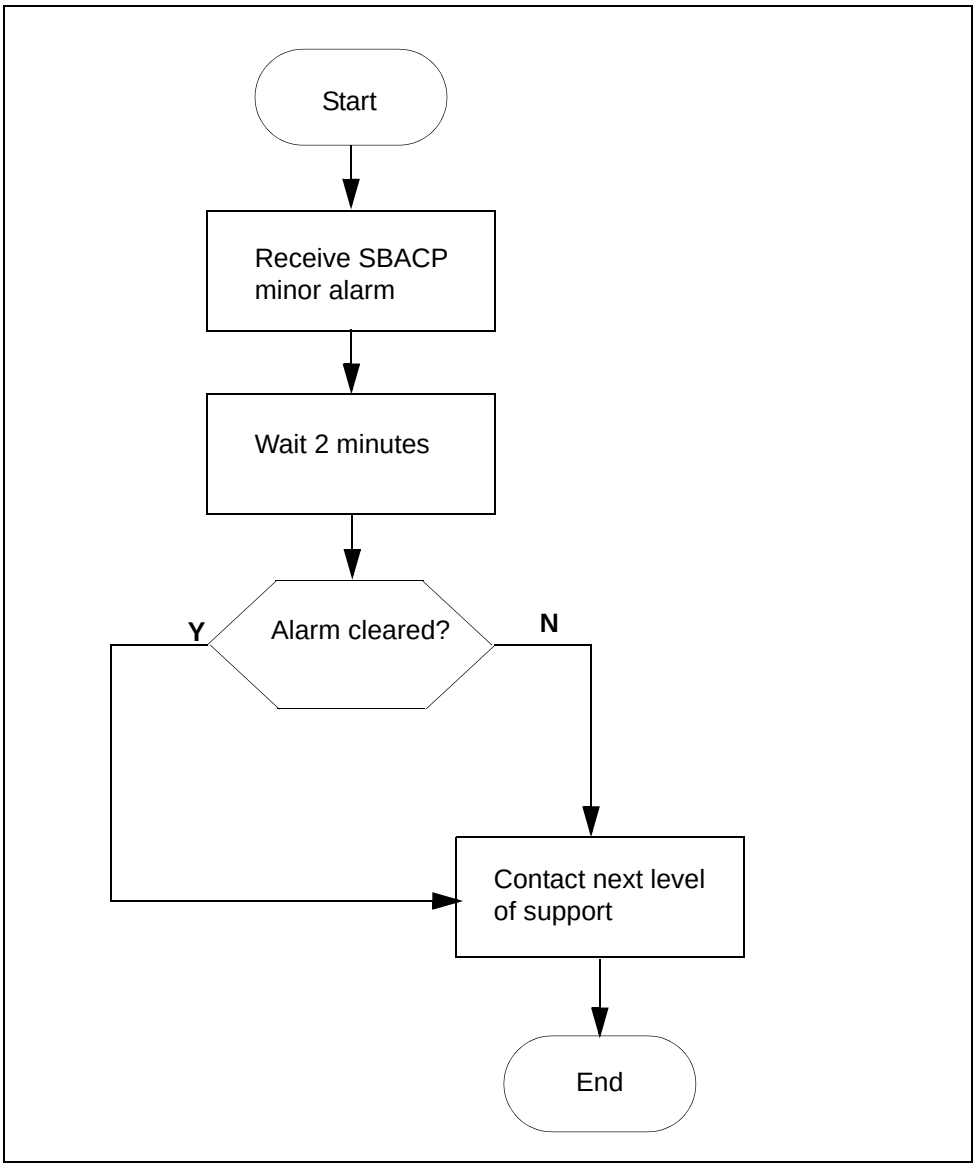
Impact

The SBA program ends but restarts within two minutes.

Action

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

SBACP (minor) alarm clearing flowchart



Clearing a minor SBACP alarm

At the MAP

1 Wait 2 minutes for the SBA to restart.

2 Contact your next level of support if the

- alarm does not clear, or
- SBA application fails three times within one minute

3 You have completed the procedure.

Clearing an SBAIF alarm

Purpose

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

Indication

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

Meaning

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

The system also generates an SDMB390 log.

Impact

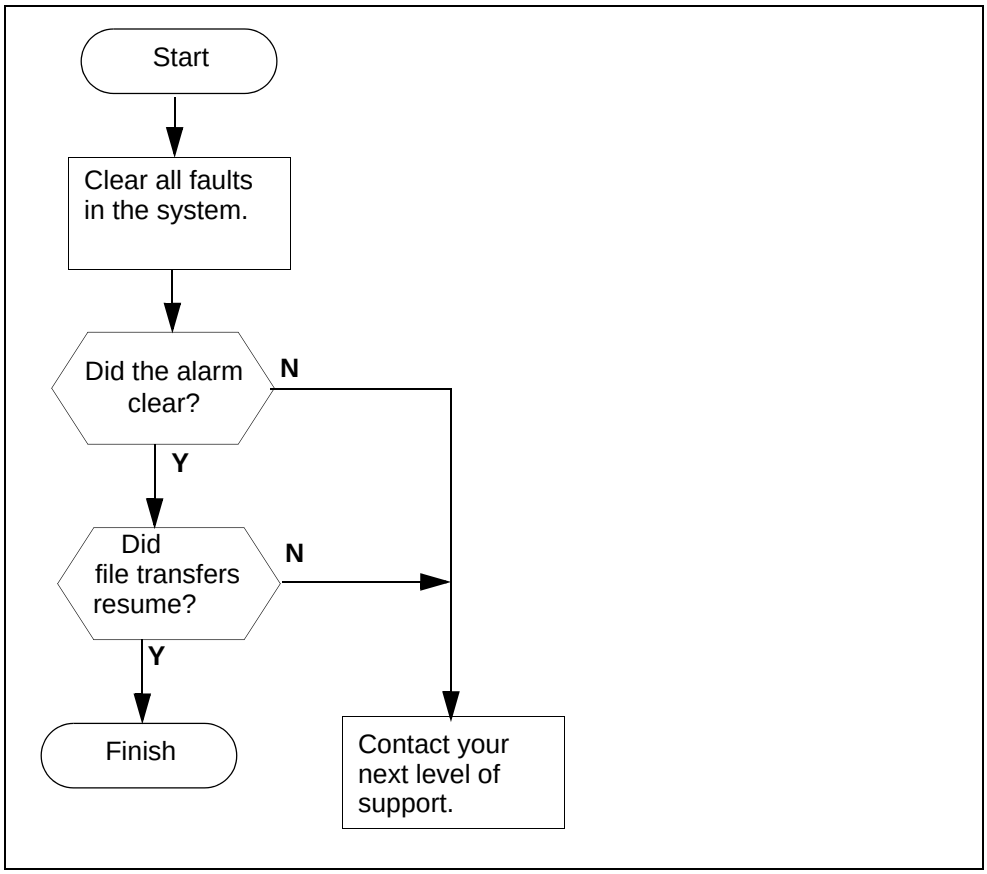
If the alarm does not clear, SBA is not able to transfer files to the downstream destination:

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

Action

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

SBAIF alarm clearing flowchart



Clearing an SBAIF alarm

At a workstation or console

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

The SBAIF alarm clears when the fault is corrected.

If the SBAIF alarm	Do
clears	step 2
does not clear	Contact your next level of support.

2 Access the core manager.

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

If log SDMB690	Do
is present	step 4
is not present	Contact your next level of support.

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

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

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

If	Do
log SDMB691 indicates the file transfer schedule is now working for the stream.	step 5
log SDMB691 indicates a new problem with the scheduled transfer of billing files	Contact your next level of support
any other log indicates problems with the scheduled transfer of billing files	Contact your next level of support

5 You have completed this procedure.

Verifying the file transfer protocol

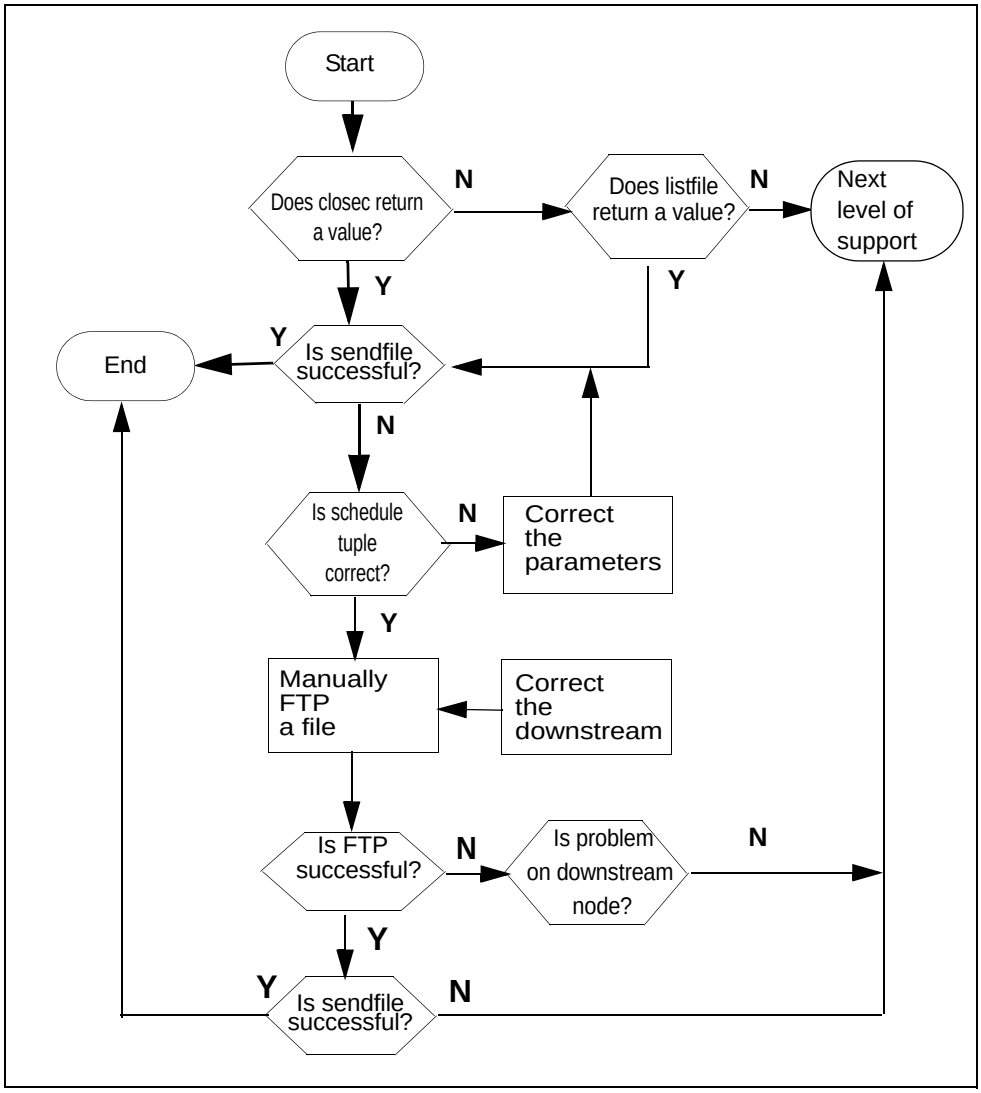
Purpose

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

Action

The following flowchart summarizes the steps outlined in the procedure.

FTP verification flowchart



Verify the FTP

At the core manager

1 Access the bill maintenance level:

```
# billmtc
```

2 Access the file system:

```
> filesys
```

3 Close active billing files:

```
> closec <stream_name>
```

where

<stream_name> is the name of the stream.

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

4 Determine the results of the closec command.

If the “closec” command	Do
returns a filename	step 6
does not returns a filename	step 5

5 List the primary file (closedNotSent directory):

```
> listfile <stream_name>
```

where

<stream_name> is the name of the stream

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

6 Send the primary file (closedNotSent directory):

```
> sendfile <stream_name>
```

where

<stream_name> is the name of the stream.

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

7 Go to the previous level:

```
> quit
```

8 Determine the results of the sendfile command.

If the “sendfile” command is	Do
successful	you have completed this procedure
not successful	step 9

Note: Observe the SDMB logs on the CM in logutil to determine why the `sendfile` command is not successful prior to continuing with step 9.

9 Access the schedule level:

```
> schedule
```

10 List the parameters of the schedule tuple:

```
> list
```

If the parameters are	Do
correct, but you are receiving an alarm	step 20
incorrect	step 11

11 Reset the schedule tuple parameters:

```
> change
```

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

13 Enter the file format.

14 Enter the destination name.

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

15 Observe the schedule tuple displayed.

16 Enter the corrected parameters.

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

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

18 Save the changed parameters:

```
> save
```

If you have	Do
corrected the parameters in the schedule tuple	step 6
determined that the parameters are correct	step 19 (verifies login and write permissions are correct for FTP process without testing a billing file)
determined that the parameters are correct	step 22 (verifies login and write permissions are correct for FTP process while testing an actual billing file)

19 Exit the maintenance interface:

```
> quit all
```

20 Login as root user.

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

Note: You can use any billing file for step 21 because you are only verifying login and write ability on the downstream node.

22 Exit back to the command prompt:

```
> quit all
```

23 Login as root user.

24 Copy a billing file from the closedNotSent directory to a temporary directory:

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

where

<logical_vol> is the logical volume for the stream that is in use

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

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

25 Access the /tmp directory:

```
# cd /tmp
```

26 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

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

Note: A successful login is confirmed by a “230 User <address> 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.

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

```
ftp> cd <remote_directory>
```

where

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

Note: A successful login is confirmed by a “250 CWD command successful” message returned by the FTP.

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

29 Set the file transfer mode to binary:

```
ftp> binary
```

Note: A successful command is confirmed by a “200 Type set to I” message returned by the FTP.

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

```
ftp> put <file>
```

Where

<file> is the name of a billing file that is copied to the /tmp directory in step 24.

31 Exit from the FTP session:

```
ftp> quit
```

If the file transfer is	Do
successful	step 34
unsuccessful because of a permission error	step 32
unsuccessful for a reason other than permission error	step 34

32 Correct the directory permissions to allow write access.

33 Repeat steps 20 through 31.

34 Send the primary files in the closedNotSent directory:

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

where

<billing_stream> is the name of the billing stream

<dest_name> is the name you choose to name the destination (for example, fraud detection).

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

If the "sendfile" command is	Do
successful	you have completed this procedure
unsuccessful	contact your next level of support

Verifying the FTP Schedule

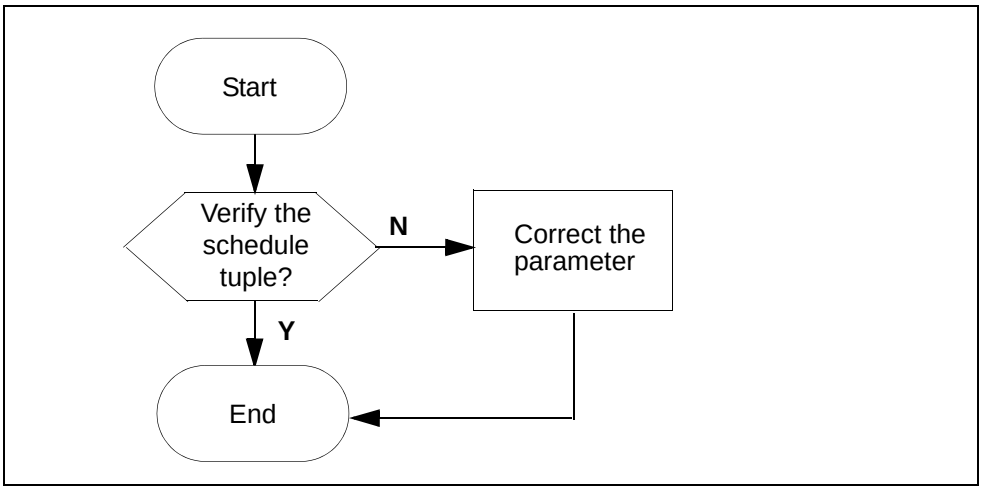
Purpose

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

Action

The following flowchart summarizes the steps in the procedure.

Verifying the FTP schedule flowchart



Verifying the FTP schedule

At any workstation or console

1 Log in to the core manager.

2 Access the bill maintenance level:

```
# billmtc
```

3 Verify the schedule tuple:

```
> schedule
```

4 List the parameters of the schedule tuple:

```
> list
```

If the parameters are	Do
correct	contact your next level of support
incorrect	step 5

5 Reset the schedule tuple parameters:

> change

6 Enter the stream name (billing file name).

7 Enter the file format.

8 Enter the destination name.

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

9 Observe the schedule tuple displayed.

10 Enter the parameters that you need to correct.

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

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

12 Save the changed parameters:

> save

If the parameters are	Do
correct, or if you have corrected the parameters, but are still receiving an alarm	contact your next level of support
correct and you are no longer receiving an alarm	step 13

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

14 You have completed the procedure.

Replacing a failed disk drive in-service

Application

Use this procedure to replace a disk drive in-service on the Netra t1400 or the Netra 240 server.

> **ATTENTION**
> This procedure replaces a disk drive in-service. Do not take the server down when performing this procedure.

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, an alarm light will be illuminated on the front panel, and a major alarm will be received if the office alarm cable is connected. Any failing disk should be replaced. After the disk is replaced, the alarm light will go off within a few minutes.

Systems installed with SSPFS use disk mirroring. With mirrored hot-swap disks, a single failed disk can be replaced without interrupting the applications running on the Netra server. Thus, a disk can be replaced while the system is in-service.

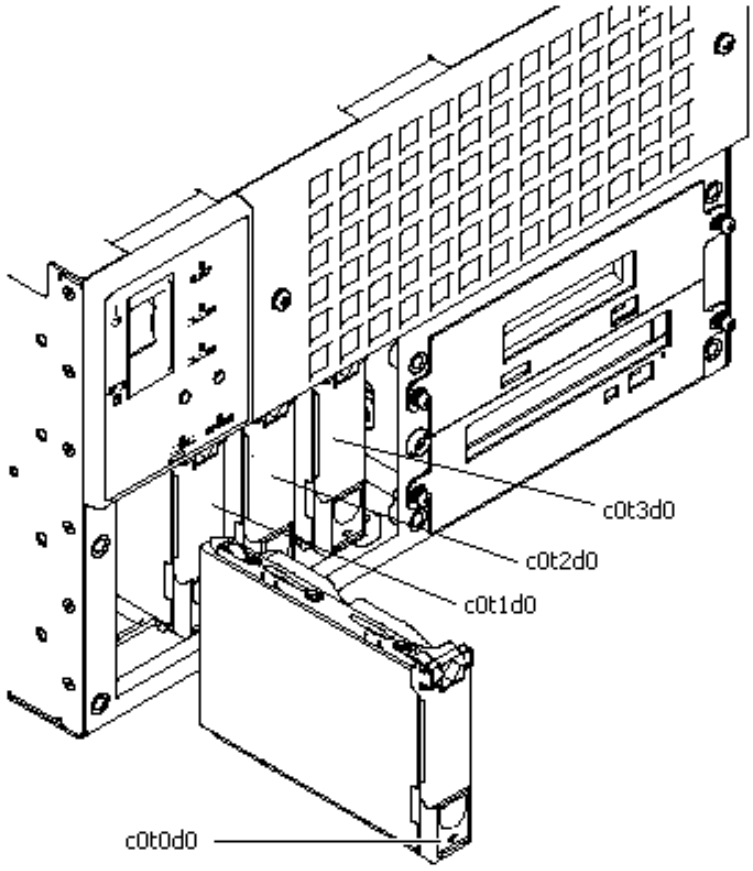
The steps to replace a failed drive are to identify the failed drive, replace it physically, remove it logically, and add the replacement drive into the disk mirror.

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 hard drives of the Netra t1400.

Netra t1400 hard drives

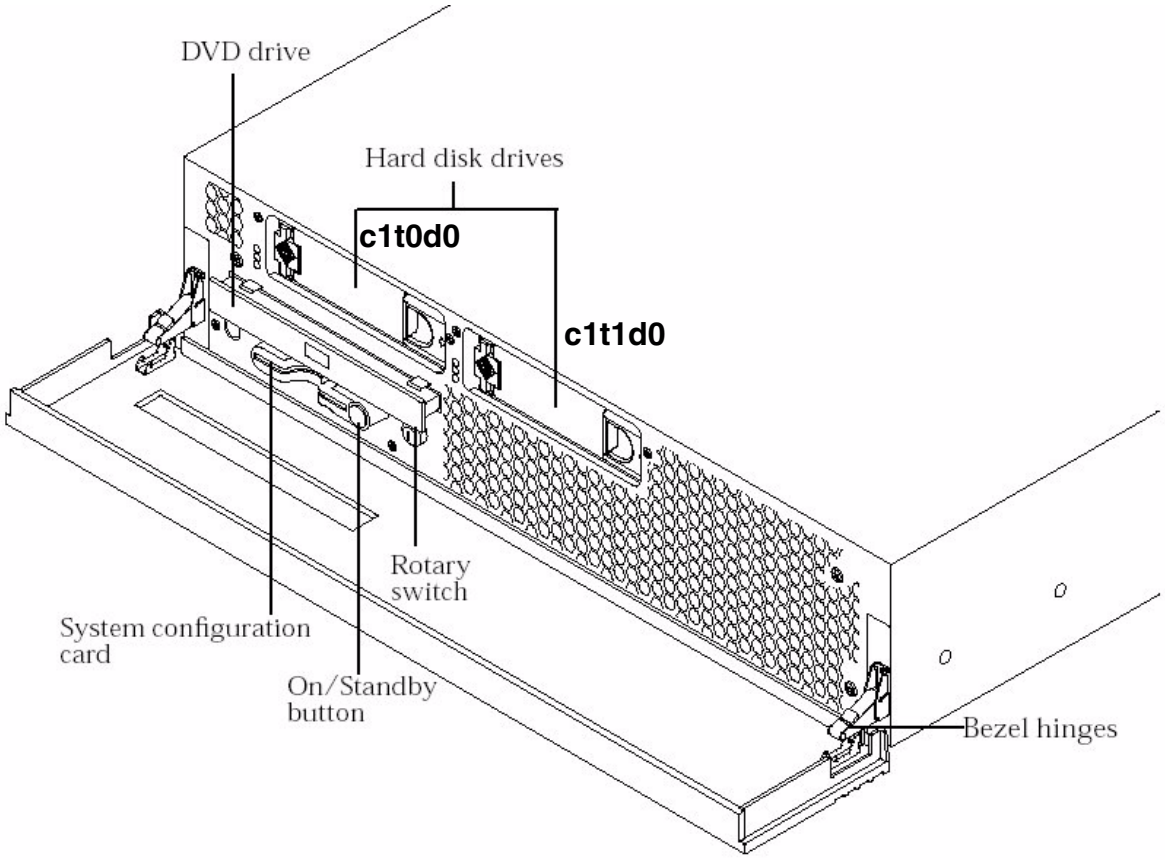


Netra 240

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

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

Netra 240 hard drives



Prerequisites

At least one of the hard drives must be functioning.

Action

Perform the following steps to complete this procedure.

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 Netra t1400 or Netra 240 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 Check the health of the system's disks by typing

```
# metastat
```

and pressing the Enter key.

Note: Information about each system disk will be displayed. The normal state is "Okay". The state "Resyncing" means the mirror was broken and is being re-created. The state "Needs Maintenance" or "Maintenance" means that the disk needs to be replaced.

6 Use the following table to determine your next step.

If you are replacing a disk drive on the	Do
Netra t1400	step 7
Netra 240	step 16

7 Determine the disk that needs to be replaced on the Netra t1400 by viewing the results from step 5.

If you are replacing	Do
c0t0d0	step 8
c0t1d0	step 10
c0t2d0	step 12
c0t3d0	step 14

8 Locate disk "c0t0d0" using the Netra t1400 hard drives on page 161 figure. Use the documentation for the Netra t1400 to physically replace the disk. When complete, return to this procedure, and do step 9.

9 Logically replace disk "c0t0d0" by entering the following sequence of commands:

```
# metadb -d c0t0d0s7
```

```
# prtvtoc -h /dev/rdsk/c0t1d0s2 | fmthard -s -
/dev/rdsk/c0t0d0s2
```

```
# metadb -a -c 2 c0t0d0s7
```

```
# metareplace -e d2 c0t0d0s1
# metareplace -e d5 c0t0d0s0
# metareplace -e d8 c0t0d0s3
# metareplace -e d11 c0t0d0s4
# metareplace -e d100 c0t0d0s5
```

10 Locate disk “c0t1d0” using the Netra t1400 hard drives on page 161 figure. Use the documentation for the Netra t1400 to physically replace the disk. When complete, return to this procedure, and do step 11.

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

```
# metadb -d c0t1d0s7
# prtvtoc -h /dev/rdsk/c0t0d0s2 | fmthard -s -
/dev/rdsk/c0t1d0s2
# metadb -a -c 2 c0t1d0s7
# metareplace -e d2 c0t1d0s1
# metareplace -e d5 c0t1d0s0
# metareplace -e d8 c0t1d0s3
# metareplace -e d11 c0t1d0s4
# metareplace -e d100 c0t1d0s5
```

12 Locate disk “c0t2d0” using the Netra t1400 hard drives on page 161 figure. Use the documentation for the Netra t1400 to physically replace the disk. When complete, return to this procedure, and do step 13.

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

```
# metadb -d c0t2d0s7
# prtvtoc -h /dev/rdsk/c0t3d0s2 | fmthard -s -
/dev/rdsk/c0t2d0s2
# metadb -a -c 2 cot2d0s7
# metareplace -e d100 c0t2d0s0
```

14 Locate disk “c0t3d0” using the Netra t1400 hard drives on page 161 figure. Use the documentation for the Netra t1400 to physically replace the disk. When complete, return to this procedure, and do step 15.

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

```
# metadb -d c0t3d0s7
# prtvtoc -h /dev/rdsk/c0t2d0s2 | fmthard -s -
/dev/rdsk/c0t3d0s2
# metadb -a -c 2 c0t3d0s7
# metareplace -e d100 c0t3d0s0
```

16 Determine the disk that needs to be replaced on the Netra 240 by viewing the results from step 5.

If you are replacing	Do
c1t0d0	step 17
c1t1d0	step 19

17 Locate disk “c1t0d0” using the Netra 240 hard drives on page 162 figure. Use the documentation for the Netra 240 to physically replace the disk. When complete, return to this procedure, and do step 18.

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

```
# metadb -d c1t0d0s7
# prtvtoc -h /dev/rdsk/c1t1d0s2 | fmthard -s -
/dev/rdsk/c1t0d0s2
# metadb -a -c 2 c1t0d0s7
# metareplace -e d2 c1t0d0s1
# metareplace -e d5 c1t0d0s0
# metareplace -e d8 c1t0d0s3
# metareplace -e d11 c1t0d0s4
# metareplace -e d100 c1t0d0s5
```

19 Locate disk “c1t1d0” using the Netra 240 hard drives on page 162 figure. Use the documentation for the Netra 240 to physically replace the disk. When complete, return to this procedure, and do step 20.

20 Logically replace disk “c1t1d0” by entering the following sequence of commands:

```
# metadb -d c1t1d0s7
```

```
# prtvtoc -h /dev/rdsk/c1t1d0s2 | fmthard -s -
/dev/rdsk/c1t1d0s2
# metadb -a -c 2 c1t1d0s7
# metareplace -e d2 c1t1d0s1
# metareplace -e d5 c1t1d0s0
# metareplace -e d8 c1t1d0s3
# metareplace -e d11 c1t1d0s4
# metareplace -e d100 c1t1d0s5
```

21 You have completed this procedure.

Erasing the contents of a CD/DVD on a Sun server

Application

Use this procedure to erase the contents of a CD/DVD on a Sun server (Netra 240), when you want to re-use the CD/DVD.

Prerequisites

None

Action

Perform the following steps to complete this procedure.

At the Sun server

1 Insert the CD/DVD you want to erase into the drive.

At your workstation

2 Telnet to the Sun server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or hostname of the Sun server

3 When prompted, enter your user ID and password.

4 Erase the contents of the CD/DVD by typing

```
$ cdrw -b all
```

and pressing the Enter key

Note: You can also use the “fast” and “session” arguments. For more details, refer to the man pages by typing **`man cdrw`**.

5 Remove the CD/DVD from the drive.

6 You have completed this procedure.

Increasing the size of a file system on a Sun server

Application

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

- Simplex configuration (one server) on page 169
- High-availability configuration (two servers) on page 172

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

The Succession Server Platform Foundation Software (SSPFS) creates file systems to best fit the needs of applications. However, it may be necessary to increase the size of a file system.

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

SSPFS file systems

Cannot be increased	Can be increased (examples)
/ (root)	/data
/var	/opt/nortel
/opt	/data/oradata
/tmp	/audio_files
	/PROV_data
	/user_audio_files
	/data/qca
	/data/mg9kem/logs

During the time file systems are being increased, writes to the file system are blocked, and the system activity increases. The more size that is added to the file system, the greater the impact on performance.

Prerequisites

Before you perform this procedure, verify that the file system is full or nearly full and that its content is valid application data. Remove any unneeded files or files generated in error that could be taking up disk space.

Action

Perform the following steps to complete this procedure.

Simplex configuration (one server)

At your workstation

1 Telnet to the Sun server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the Sun server that has the file system you want to increase

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

4 When prompted, enter the root password.

5 Access the command line interface by typing

```
# cli
```

and pressing the Enter key.

Example response

```
Command Line Interface
 1 - View
 2 - Configuration
 3 - Other

 X - exit

select -
```

6 Determine which file system to increase by checking the current disk capacity utilization as follows:

a Enter the number that corresponds to the “View” option in the menu.

Example response

```
View
  1 - sspfs_soft (Display Software
      Installation Level Of SSPFS)
  2 - chk_sspfs (Check SSPFS Processes)
  3 - sw_conf (The software configuration of
      the znc0s0jx)
  4 - cpu_util (Overall CPU utilization)
  5 - cpu_util_proc (CPU utilization by
      process)
  6 - port_util (I/O port utilization)
  7 - disk_util (Filesystem utilization)

  X - exit

select -
```

b Enter the number that corresponds to the “disk_util” option in the menu.

Example response

```
=== Executing "disk_util"

Filesystem             kbytes    used   avail capacity  Mounted on
/dev/md/dsk/d2       4129290 1892027 2195971    47%    /
/proc                      0       0       0     0%    /proc
fd                         0       0       0     0%    /dev/fd
mnttab                     0       0       0     0%    /etc/mnttab
/dev/md/dsk/d8       2053605  155600 1836397     8%    /var
swap                 3505488      40 3505448     1%    /var/run
swap                  524288     448  523840     1%    /tmp
/dev/md/dsk/d11      5161437 1428691 3681132    28%    /opt
/dev/md/dsk/d23      2031999   34313 1936727     2%    /PROV_data
/dev/md/dsk/d24      2031999  169042 1801998     9%    /audio_files
/dev/md/dsk/d20      3080022  294615 2723807    10%    /data
/dev/md/dsk/d25       949455  440344  452144    50%    /user_audio_files
/dev/md/dsk/d21      3080022  275962 2742460    10%    /opt/nortel
/dev/md/dsk/d22     12386331 10337214 1925254    85%    /data/oradata
/dev/md/dsk/d26       122847    1041  109522     1%    /data/qca

=== "disk_util" completed successfully
```

7 Determine the appropriate size for the file systems based on your specific needs.

8 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.

9

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

Increase the size of the file system by typing

`# filesys grow -m <mount_point> -s <size>{m,g}`

Where

mount_point
is the name associated with the file system

- /data
- /opt/nortel
- /data/oradata
- /PROV_data
- /audio_files
- /user_audio_files
- /data/qca
- /data/mg9kem/logs

size
is the size in megabytes (m) or gigabytes (g) you obtained in step 7

Example
`# filesys grow -m /data -s 512m`

Note: The example above increases the "/data" file system by 512 megabytes (MB).

10 You have completed this procedure.

High-availability configuration (two servers)

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

At your workstation

1 Telnet to the inactive node of the server cluster by typing

```
> telnet <server>
```

and pressing the Enter key.

where

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

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 Ensure the cluster is in a good state as follows:

a Run the udstat command by typing

```
# udstat
```

and pressing the Enter key.

If the system response contains “nodaemon”, “offline”, “down, “not mounted”, contact your next level of support. Otherwise, proceed to the next step.

b Run the ubmstat command by typing

```
# ubmstat
```

and pressing the Enter key.

If the system response is other than “ClusterIndicatorSTBY”. contact your next level of support. Otherwise, proceed to the next step.

c Run the CheckConfiguration command by typing

```
# CheckConfiguration
```

and pressing the Enter key.

If the system response is other than “Checking local cluster configuration against <other node>, contact your next level of support. Otherwise, proceed to the next step.

At the Inactive node

6

ATTENTION

Once you increase the size of a file system, you cannot decrease it.

Increase the size of the desired file system by typing

```
# GrowClusteredFileSystem.ksh <mount_point>
<size>{m,g}
```

Where

mount_point
is the name associated with the file system, for example

- /data
- /opt/nortel
- /data/oradata
- /PROV_data
- /audio_files
- /user_audio_files
- /data/qca
- /data/mg9kem/logs

size
is the size in megabytes (m) or gigabytes (g)

Example

```
# GrowClusteredFileSystem.ksh /data/qca 10m
```

Note: The example above increases the “/data/qca” file system by 10 megabytes (MB).

7 Reboot the Inactive node by typing

```
# init 6
```

and pressing the Enter key.

8 Wait for the Inactive node to reboot, then log in again using its physical IP address.

9 Telnet to the active node of the Sun server cluster by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the physical IP address of the active node in the Sun server cluster

10 When prompted, enter your user ID and password.

11 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

12 When prompted, enter the root password.

At the Active node

13 Stop the cluster by typing

```
# StopCluster
```

and press the Enter key.

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

At the newly Active node

14 Clone the other node using procedure Cloning the image of one node in a cluster to the other node on page 223 in this document.

15 You have completed this procedure.

Performing a full backup of Oracle data on a Sun server (pre-SN06.2)

Application

Use this procedure to perform a full backup of application data in the Oracle database on a Sun server (t1400) running the SN05 or SN06 release of the Succession Server Platform Foundation Software (SSPFS).

Note: For systems running the SN06.2 or greater release of the SSPFS, use procedure Performing a data backup on a Sun server (SN06.2 or greater) on page 212 in this document .

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

Prerequisites

This procedure has the following prerequisites:

- the Oracle database must be in-service
- you need a blank 4mm DDS-3 (Digital Data Storage) tape of 125m and 12GB to store the data

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

Action

Perform the following steps to complete this procedure.

At the Sun server

1 Insert the blank tape into the tape drive.

At your workstation

2 Telnet to the Sun server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or hostname of the Sun server on which you are performing a full backup of Oracle data

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.

6 Rewind the tape by typing

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

and pressing the Enter key.

7 Change to the Oracle user by typing

```
# su - oracle
```

and pressing the Enter key.

Note: You may be required to enter a password for the Oracle user.

8 Backup the Oracle data by typing

```
$ /opt/nortel/sspfs/bks/bkfullora
```

and pressing the Enter key.

9 Quit the Oracle user by typing

```
$ exit
```

and pressing the Enter key.

10 List the content of the tape to ensure the backup was successful by typing

```
# tar tvf /dev/rmt/0
```

and pressing the Enter key.

Example response:

```
-rw-r--r-100/100 8296448 Jun 11 18:08 2003
/var/tmp/bkexpora_2003061118_co.dmp
```

11 Remove the tape from the drive, label it, write-protect it, and store it in a safe place.

12 You have completed this procedure.

Creating or modifying the login greeting message on a Sun server

Application

Use this procedure to create or modify the login greeting message on a Sun server. This message is presented to the user who logs in to the Sun server through Telnet.

Prerequisites

None

Action

Perform the following steps to complete this procedure.

At your workstation

1 Telnet to the Sun server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the Sun server on which you are setting the CS 2000 IP address

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

4 When prompted, enter the root password.

5 Access the command line interface by typing

```
# cli
```

and pressing the Enter key.

Example response

```
Command Line Interface
 1 - View
 2 - Configuration
 3 - Other

 X - exit

select -
```

6 Enter the number that corresponds to the “Configuration” option in the menu.

Example response

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

 X - exit

Select -
```

7 Enter the number that corresponds to the “Login Session” option in the menu.

Example response

```
OAMP Application Configuration
 1 - login_session_timeout (Login Session
     Timeout Configuration)
 2 - login_session_server (Login Session Master
     Server Configuration)
 3 - telnet_greeting (Telnet Login Greeting)

 X - exit

select -
```

8 Enter the number that corresponds to the “telnet_greeting” option in the menu.

Example response

```
===Executing “telnet_greeting”

Telnet Login Greeting Message:
Authorized use only, activities logged.

Enter the Telnet Login Greeting Message.
Enter a blank line to end the message:
```

9 When prompted, enter the message. End the message with a blank line.

Example response

```
Enter “ok” to commit changes
Enter “quit” to exit
Enter anything else to re-enter settings
```

10 When prompted, commit the change by typing

ok

and pressing the Enter key.

Example response

```
===”telnet_greeting” completed successfully
```

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

`select - x`

and pressing the Enter key.

12 You have completed this procedure.

Performing a full backup of file systems (pre-SN06.2)

Application

Use this procedure to perform a full backup of the file systems on a Sun server (t1400) running the SN05 or SN06 release of the Succession Server Platform Foundation Software (SSPFS).

Note: For systems running the SN06.2 or greater release of the SSPFS, use procedure Performing a full backup of file systems (SN06.2 or greater) on page 215 in this document.

Prerequisites

This procedure has the following prerequisites:

- the Oracle database must be in-service
- you need a blank 4mm DDS-3 (Digital Data Storage) tape of 125m and 12GB to store the data

Action

At the Sun server

1 Insert a blank tape into the tape drive.

At your workstation

2 Telnet to the server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the server on which you are performing the backup

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.

6 Rewind the tape by typing

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

and pressing the Enter key.

7 Backup the file systems by typing

```
# /opt/nortel/sspfs/bks/bkfullsys
```

and pressing the Enter key.

8 List the content of the tape to ensure the backup was successful by typing

```
# ufsrestore tfs /dev/rmt/0 1 (for /)
# ufsrestore tfs /dev/rmt/0 2 (for /var)
# ufsrestore tfs /dev/rmt/0 3 (for /data)
# ufsrestore tfs /dev/rmt/0 4 (for /opt)
# ufsrestore tfs /dev/rmt/0 5 (for /opt/nortel)
```

and pressing the Enter key.

9 Remove the tape from the drive, label it, write-protect it, and store it in a safe place.

10 You have completed this procedure.

Restoring application data to the Oracle database (pre-SN06.2)

Application

Use this procedure to restore the application data to the Oracle database from a backup tape on a Sun server (t1400) running the SN05 or SN06 release of the Succession Server Platform Foundation Software (SSPFS).

Note: For system running the SN06.2 or greater release of the SSPFS, use Performing a data restore on a Sun server (SN06.2 or greater) on page 218 in this document.

Prerequisites

You need the tape on which the data was backed up.

Action

Perform the following steps to complete this procedure.

At the Sun server

1 Insert the backup tape into the drive.

At your workstation

2 Telnet to the Sun server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the Sun server on which you are performing the data restore

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.

6 Stop the server applications that run on the server.

For	Refer to
SESM, SAM21EM and NPM server applications	Enabling or disabling the socks security service on a Sun server on page 208 Creating or modifying the login greeting message on a Sun server on page 178 Deleting local user accounts from a Sun server on page 203
MG 9000 Manager and mid-tier server applications	the MG9000 Security and Administration document, NN10162-611, if required

7 Change to the Oracle user by typing

```
# su - oracle
```

and pressing the Enter key.

8 Perform the restore command by typing

```
$ /opt/nortel/sspfs/bks/rsimpora
```

and pressing the Enter key.

9 Quit the Oracle user by typing

```
$ exit
```

and pressing the Enter key.

10 Remove the tape from the drive and store it in a safe place.

11 Start the server applications that run on the server.

For	Refer to
SESM, SAM21EM and NPM server applications	Configuring the time zone on a Sun server on page 205 Setting up local user accounts on a Sun server on page 192
MG 9000 Manager and mid-tier server applications	the MG9000 Security and Administration document, NN10162-611, if required

12 You have completed this procedure.

Restoring root file systems (pre-SN06.2)

Application

Use this procedure to restore the root file systems from tape on a Sun server (t1400) running the SN05 or SN06 release of the Succession Server Platform Foundation Software (SSPFS).

Note: For systems running the SN06.2 or greater release of the SSPFS, use procedure Performing a full system restore on a Sun server (SN06.2 or greater) on page 220 in this document

Prerequisites

You need the tape on which the data was backed up.

Action

Perform the following steps to complete this procedure.

At the Sun server console

1. Log in to the Sun server through the console using the root user ID and password.
2. Insert the backup tape into the drive.
3. Insert SSPFS CD disk#1 into the CD-ROM drive.
4. Enter the following commands:

   ```
   # metadetach d2 d1
   # metaroot /dev/dsk/c0t0d0s1
   # init 6
   ```

5. When prompted, log on as root.
6. Enter the following commands:

   ```
   # metaclear -r d2
   # metaclear d1
   # init 0
   ```

7. At the ok prompt, boot the system from the CD Rom by typing

   ```
   ok boot cdrom -s
   ```

   and pressing the Enter key.

8 Enter the following commands:

```
# mount /dev/dsk/c0t0d0s1 /a
# cp /a/etc/system /a/etc/system.unmirror
# cp /a/etc/vfstab/ /a/etc/vfstab.unmirror
# cd /a
# ufsrestore rfs /dev/rmt/0 1
```

Note: The system can take between 20 and 45 min. to process the above command.

```
# rm restoresymtable
# cd /
# cp /a/etc/system.unmirror /a/etc/system
# cp /a/etc/vfstab.unmirror /a/etc/vfstab
# umount /a
# fsck /dev/rdsk/c0t0d0s1
# installboot /usr/platform/`uname -i`
/lib/fs/ufs/bootblk /dev/rdsk/c0t0d0s1
```

Note: The above command is entered on one line. There is no space between "`-i`" and "`/lib/fs/ufs/bootblk`".

```
# init 6
```

9 When prompted, log on as root.

Note: The root password required is the restored root password and not the default root password.

10 Enter the following commands:

```
# metainit -f d0 1 1 c0t0d0s1
# metainit d1 1 1 c0t1d0s1
# metainit d2 -m d0
# metaroot d2
# lockfs -fa
# init 6
```

11 When prompted, log on as root.

12 Enter the following commands:

```
# metattach d2 d1
# init 6
```

13 When prompted, log on as root.

14 Remove the tape from the drive and store it in a safe place.

15 Eject the SSPFS CD disk#1 from the CD-ROM drive by entering the following commands:

```
# cd /
# eject cdrom
```

16 You have completed this procedure.

Restoring non-root file systems (pre-SN06.2)

Application

Use this procedure to restore all of the non-root file systems from tape on a Sun server (t1400) running the SN05 or SN06 release of the Succession Server Platform Foundation Software (SSPFS).

Note: For systems running the SN06.2 or greater release of the SSPFS, use procedure Performing a full system restore on a Sun server (SN06.2 or greater) on page 220 in this document.

Prerequisites

You need the tape on which the data was backed up, and you need root user privileges.

Action

Perform the following steps to complete this procedure.

ATTENTION

The root user must be under the Bourne command shell (sh) when performing the whole restore file systems procedure. Do not switch to any other command shell such as the Korn or Bash shell, since under the Korn or Bash command shell, the system will be frozen when you issue the “init 1” command.

At the server console

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

2 If required, change to the Bourne shell as follows:

a Execute the shell change command by typing

```
# passwd -e
```

and pressing the Enter key.

b When prompted for the new shell, specify the Bourne shell by typing

```
# sh
```

and pressing the Enter key.

3 Insert the backup tape into the drive.

4 Enter the following command:

```
# init 1
```

5 When the system prompts you to either enter the root password or press Control-D, enter your root password to continue the maintenance process.

6 Enter the following command:

```
# ufsrestore tfs /dev/rmt/0 1 | grep audio_files
```

If	Do
the response to the command is similar to `321287 ./audio_files`	substep a
the command produces no output	substep b

a Enter the following series of commands:

```
# cd /audio_files
# ufsrestore rfs /dev/rmt/0 2
# rm restoresymtable

# cd /data
# ufsrestore rfs /dev/rmt/0 3
# rm restoresymtable

# cd /opt
# ufsrestore rfs /dev/rmt/0 4
# rm restoresymtable

# cd /opt/nortel
# ufsrestore rfs /dev/rmt/0 5
# rm restoresymtable

# cd /PROV_data
# ufsrestore rfs /dev/rmt/0 6
# rm restoresymtable

# cd /user_audio_files
# ufsrestore rfs /dev/rmt/0 7
# rm restoresymtable
```

```
# cd /var
# ufsrestore rfs /dev/rmt/0 8
# rm restoresymtable
```

Note: The restore time for each filesystem is dependent on the size of the filesystem. Restore can take 60 minutes or more to complete after which the prompt returns. Do not press Ctrl-C as this will interrupt the restore process.

Proceed to step 7

b Enter the following series of commands:

```
# cd /data
# ufsrestore rfs /dev/rmt/0 2
# rm restoresymtable

# cd /opt
# ufsrestore rfs /dev/rmt/0 3
# rm restoresymtable

# cd /opt/nortel
# ufsrestore rfs /dev/rmt/0 4
# rm restoresymtable

# cd /var
# ufsrestore rfs /dev/rmt/0 5
# rm restoresymtable
```

Note: The restore time for each filesystem is dependent on the size of the filesystem. Restore can take 60 minutes or more to complete after which the prompt returns. Do not press Ctrl-C as this will interrupt the restore process.

7 Enter the following command:

```
# init 6
```

8 Remove the tape from the drive and store it in a safe place.

9 You have completed this procedure.

Setting up local user accounts on a Sun server

Application

Use this procedure to add local user accounts on a Sun server and assign them to user groups. Also use this procedure to assign existing user accounts to user groups (see User groups on page 192).

ATTENTION

If upgrading from a release prior to SN06, existing users must be assigned to primary group “succssn” for login access, and to one or more Secondary user groups on page 192 to specify the operations the user is authorized to perform (see step 13 of this procedure).

If you choose to centrally manage your user accounts, refer to procedure “Adding new users” in the Integrated EMS Security and Administration document, NN10336-611.

User groups

Users of the Nortel Networks OAM&P client applications must belong to the primary user group “succssn” for login access. Users must also belong to one or more secondary user groups listed in the table below, which specify the operations a user is authorized to perform.

Secondary user groups

trkadm	lnadm	mgcadm	mgadm	emsadm
trkrw	lnrw	mgcrw	mgrw	emsrw
trksprov	lnsprov	mgcsprov	mgsprov	emssprov
trkmtc	lnmtc	mgcmtc	mgmtc	emsmtc
trkro	lnro	mgcro	mgro	emsro

A secondary user group consists of

- a user group domain
- a user group operation

User group domain

A user group domain defines the range of applications to which a user group applies. The user group domains are listed in the table below.

Domain	Application mapping
trk	trunks, trunk-based services, small trunking gateways (port level), carrier-based services
ln	line services, line cards, small line gateways (port level)
mgc	CS2K, CS3K, USP, GWC, SAM21, IMS, 3PC, Storm, CS 2000 SAM21 Manager, CS 2000 GWC Manager
mg	small and large gateways such as UAS, line gateways, trunk gateways
ems	SDM, MDM, MDP, KDC, device manager, NPM

User group operation

A user group operation dictates the operations a user can perform using the Nortel Networks OAM&P client applications. The user group operations are listed in the table below.

Operation	User role mapping
adm (administration)	Can reconfigure, access all functions, setup fundamental configuration, commission (add, delete, rehome), base frames and systems (SAM21 frames, call servers, large gateways), and run service-impacting diagnostics. The adm user can also do rw, sprov, mtc, and ro user operations.
rw (read/write)	Can view and change configuration and status, commission and reconfigure elements (GWCs, cards, shelves). The rw user can also do sprov, mtc, and ro user operations.
sprov (subscriber provisioning)	Can view status and configuration and change provisioning data, but cannot change maintenance state or do base component configuration. The sprov user can also do ro user operations.

Operation	User role mapping
mtc (maintenance)	Can view status and configuration, make changes to status, and run service-impacting diagnostics. The mtc user can also do ro user operations.
ro (read-only)	Can view status and configuration, but cannot make changes.

When assigning users to secondary user groups, use the tables that follow, which provide a mapping between commands and secondary user groups. The list of the available tables is as follow:

Node provisioning operations

Command	User group				
	mgcadm	mgcrw	mgcmtc	mgcsprov	mgcro
Disassociate a media gateway (MG) from a gateway controller (GWC)		x			
Associate an MG with a GWC		x			
Change the provisioning data for an MG		x			
Query site info					x

Node provisioning operations

Command	User group				
	mgcadm	mgcrw	mgcmtc	mgcsprov	mgcro
Query a GWC					x
Query an MG					x
change MG GWCEM data		x			
Get policy enforcement point (PEP) server data					x
Query a GWC PEP connection					x
Get dynamic quality of service (DQoS) policies data					x
Add or change a network address translations (NAT) device		x			
Query a NATdevice					x
Add, change, delete a media proxy (MP)		x			
Add, change, delete resource usage (RU)		x			
Query RU					x
Add, change, delete limited bandwidth links (LBL)		x			
Query LBL					x
Display call agent identification (ID)					x
Set or change call agent ID		x			
Change root middleboxes		x			
Add, modify, or decommission a SAM21 network element		x			
Reprovision a SAM21 node		x			
Configure IPoA services, ATM PMC addresses		x			
View alarms, cards, subnet, shelf, mate shelf, mate card					x
Lock/unlock a card			x		
Perform diagnostics			x		
Modify provisioning		x			

Node provisioning operations

Command	User group				
	mgcadm	mgcrw	mgcmtc	mgcsprov	mgcro
Perform a swact			x		
Firmware flash			x		
Assign/unassign services		x			

Audit operations

Command	User group				
	mgcadm	mgcrw	mgcmtc	mgcsprov	mgcro
Configure audit	x				
Run audit	x				
Get audit description					x
Get audit configuration					x
Get list of registered audits					x
Retrieve audit report					x
Take action on problem	x				

Carrier provisioning operations

Command	User group				
	trkadm	trkrw	trkmtc	trksprov	trkro
Add carrier		x			
Delete carrier		x			
Get endpoint					x
Get carrier					x
Get carrier by filter					x

Alarm operations

Command	User group				
	emsadm	emsrw	emsmtc	emssprov	emsro
View/filter alarms					x

Internet transparency operations

Command	User group				
	mgcadm	mgcrw	mgcmtc	mgcsprov	mgcro
Query NAT					x
Query media proxy					x
Change associated NAT		x			

Trunk provisioning operations

Command	User group				
	trkadm	trkrw	trkmtc	trksprov	trkro
Get tuple					x
Get tuple range					x
Get CM CLLI					x
Add tuple		x			
Replace tuple		x			
Delete tuple		x			
List all tuples	x				
Suspend application	x				
Restore application	x				

Trunk maintenance operations

Command	User group				
	trkadm	trkrw	trkmtc	trksprov	trkro
Post by trunk CLLI					x
Maintenance by trunk CLLI			x		
Post by gateway					x
Maintenance by gateway			x		
Post by carrier					x
Maintenance by carrier			x		
D-channel Post by trunk CLLI					x
D-channel maintenance by trunk CLLI			x		
ICOT			x		
Set CM CLLI			x		
Set Auto Refresh					x

ADSL provisioning operations

Command	User group				
	lnadm	lnrw	lnmtc	lnsprov	lnro
Get subscriber					x
Add subscriber				x	
Add cross connection				x	
Modify subscriber				x	
Modify cross connection				x	
Delete subscriber				x	
Delete cross connection				x	

Line provisioning operations

Command	User group				
	lnadm	lnrw	lnmtc	lnsprov	lnro
ECHO, QX75, QBB, QBERT, QCM, QCOUNTS, QCPUGNO, QDCH, QDN, QDNA, QGRP, QHLR, QIT, QLEN, QLRN, QLT, QMODEL, QMSB, QPHF, QPRIO, QSCONN, QSCUGNO, QSIMR, QSL, QTOPSPOS, QTP, QWUCR					x
QCUST, QDNSU, QDNWRK, QHA, QHASU, QHU, QLENWRK, QLOAD, QMADN, QNCOS, QPDN	x				
All other supported commands for line provisioning				x	

Line maintenance operations

Command	User group				
	lnadm	lnrw	lnmtc	lnsprov	lnro
Validate line using DN CLLI					x
Validate line using TID CLLI					x
Get line post info					x
Busy line			x		
Return line to service			x		
Force release line			x		
Installation busy line			x		
Cancel deload			x		
Get CM CLLI					x
Get endpoint state					x
GetGwlp					x

V5.2 provisioning operations

Command	User group									
	trkadm	trkrw	trkmtc	trksprov	trkro	lnadm	lnrw	lnmtc	lnsprov	lnro
Add, delete, modify V5.2 interface		x					x			
View all V5.2 interfaces					x					x
View signalling channel information entry, update list (V5Prov)					x					x
Add, modify, delete signalling channel information entry (V5Prov)		x					x			
View ringing cadence mapping, update list (V5Ring)					x					x
Add, modify, delete ringing cadence mapping (V5Ring)		x					x			
View signalling characteristic profile, update list (V5Sig)					x					x
Add, delete, modify signalling characteristic profile (V5Sig)		x					x			
View carrier-to-interface and interface-to-carrier mappings					x					x

Patching operations

Command	User group				
	emsadm	emsrw	emsmtc	emssprov	emsro
apply, remove, activate, deactivate, audit, restart, and image from the NPM GUI or CLUI	x				
Software image from MG 9000 Manager GUI		x			

Prerequisites

To perform this procedure, you need to have the root user ID and password to log in to the server.

Action

Perform the following steps to complete this procedure.

At your workstation

1 Telnet to the Sun server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the Sun 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 Use the following table to determine your next step.

If you are	Do
adding a new user	step 6
assigning an existing user to secondary user groups	step 11

6 Add the user to the primary user group “succssn” by typing

```
# useradd -g succssn <userid>
```

and pressing the Enter key.

where

userid
is a variable for the user name

7 Create a password for the user you just added by typing

```
# passwd <userid>
```

and pressing the Enter key.

where

userid
is the user name you added in the previous step

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

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

9 When prompted, enter the password again for verification.

10 Proceed to step 13.

11 Determine which groups the user currently belongs to by typing

```
# groups <userid>
```

and pressing the Enter key.

where

userid
is a variable for the user name

12 Note the user groups the user currently belongs to.

13 Assign the user to one or more secondary user groups by typing

```
# usermod -g succssn -G <groupA,groupB,...>
<userid>
```

and pressing the Enter key.

where

groupA, groupB,...
are the secondary user groups (see table Secondary user groups on page 192) and any other user groups you noted in step 12 to which the user already belonged (include comma between groups, but no space)

userid
is a variable for the user name

Example input for a user who can perform line and trunk maintenance operations

```
# usermod -g succssn -G lnmtc,trkmtc johndoe
```

Note: The usermod command overwrites any previous user groups. Therefore, anytime you enter this command, specify all the user groups for the user.

14 You have completed this procedure.

Deleting local user accounts from a Sun server

Action

Use this procedure to delete local user accounts from a Sun server.

If you are centrally managing your user accounts, refer to procedure “Deleting users” in the Integrated EMS Security and Administration document, NN10336-611.

DO NOT delete the following critical user IDs from the server:

sshd, maint, npm, npmftp, ptm, mgems, www, patcher, poller, certuser, sam21em, anonymous, image, pfrs, ntssg, FIELD, oracle

ATTENTION
User accounts and passwords are not automatically propagated to the second server in a high-availability (two-server) configuration. Therefore, account management activities such as setting up users, removing users, and changing passwords, must be performed on both servers.

Prerequisites

None

Action

Perform the following steps to complete this procedure.

At your workstation

1 Telnet to the Sun server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the Sun 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 Delete the user from the server by typing

```
# userdel <userid>
```

and pressing the Enter key.

where

userid
is a variable for the user name

6 You have completed this procedure.

Configuring the time zone on a Sun server

Application

Use this procedure to configure the time zone on a Sun server.

Prerequisites

None

Action

Perform the following steps to complete this procedure.

At your workstation

1 Telnet to the Sun server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the Sun server on which you want to configure the time zone

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

4 When prompted, enter the root password.

5 Access the command line interface by typing

```
# cli
```

and pressing the Enter key.

Example response

```
Command Line Interface
 1 - View
 2 - Configuration
 3 - Other

 X - exit

select -
```

6 Enter the number that corresponds to the “Configuration” option in the menu.

Example response

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

 X - exit


Select -
```

7 Enter the number that corresponds to the “Location Configuration” option in the menu.

Example response

```
Location Configuration
 1 - Chg_tz (Change Timezone
 2 - sys_loc (System Location)

 X - exit

select -
```

8 Enter the number that corresponds to the “chg_tz” option in the menu.

Example response

```
=== Executing “chg_tz”

WARNING: Changing the timezone will require a
reboot

Current setting:
Timezone:       US/Eastern

Enter the timezone for this host <default:
US/Eastern>:
```

9 When prompted, enter the correct time zone and press the Enter key.

Example response

```
New setting:
Timezone:       US/Eastern

Enter “ok” to commit changes
Enter “quit” to exit
Enter anything else to re-enter settings
```

10 When prompted, confirm the change by typing

ok

and pressing the Enter key.

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

`select - x`

and pressing the Enter key.

12 You have completed this procedure.

Enabling or disabling the socks security service on a Sun server

Application

Use this procedure to enable or disable the socks security service on a Sun server.

Prerequisites

You must have root user privileges to perform this procedure.

Action

Perform the following steps to complete this procedure.

At your workstation

1 Telnet to the Sun server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the Sun server on which you want to enable socks

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

4 When prompted, enter the root password.

5 Access the command line interface by typing

```
# cli
```

and pressing the Enter key.

Example response

```
Command Line Interface
 1 - View
 2 - Configuration
 3 - Other

 X - exit

select -
```

6 Enter the number that corresponds to the “Configuration” option in the menu.

Example response

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

 X - exit

Select -
```

7 Enter the number that corresponds to the “Security Services Configuration” option in the menu.

Example response:

```
Security Services Configuration
 1 - Socks Configuration


 X - exit

select -
```

8 Enter the number that corresponds to the “Socks Configuration” option in the menu.

Example response:

```
Socks Configuration
  1 - toggle_socks (Toggle - Turn On/Off Socks
      Security Service)
  2 - config_socks (Modify Socks Security
      Service)
  3 - list_socks (List Socks Security Service)


 X - exit

select -
```

9 Enter the number that corresponds to the “toggle_socks” option in the menu.

Example response:

```
Socks is currently disabled. This action will
set the state of socks to enabled.

WARNING: Enabling socks requires a restart of
the system which will make the system
unavailable for a short time. If socks is
enabled now, the application GUIs will not
function properly until the system is restarted.

Do you want to enable socks? [y] [y,n,?,q]
```

10 Use the following table to determine your next step.

If you	Do
want to change the state of socks (enable or disable)	step 11
do not want to change the state of socks	you have completed this procedure

11 Change the state of socks by typing

y

and pressing the Enter key.

Example response:

```
Socks has been enabled, however the system
requires a restart.
Proceed as follows to restart the system:

Log in to the console as root, and restart the
system with the command: "shutdown -i 6 - y".
```

12 Restart the system as follows:

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

b Restart the system by typing

```
# shutdown -i 6 -y
```

and pressing the Enter key.

Note: If you disabled socks and a firewall is in place between the application GUIs and the server, the firewall rules may need to be changed to allow the application GUIs to work.

13 You have completed this procedure.

Performing a data backup on a Sun server (SN06.2 or greater)

Application

Use this procedure to perform a data backup on a Sun server (t1400 or Netra 240) running the SN06.2 or greater release of the Succession Server Platform Foundation Software (SSPFS).

Note 1: For systems running the SN05 or SN06 release of the SSPFS, use procedure Performing a full backup of Oracle data on a Sun server (pre-SN06.2) on page 175 in this document.

Note 2: The data backup is not required for the Core Billing Manager (CBM) product family.

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:

- you must be running SSPFS SN06.2 or greater
- you need a blank 4mm Digital Data Storage (DDS-3) tape of 125m and 12 GB to store the data (t1400 only)
- you need one or more blank DVD-RW of 4.7 GB to store the data (Netra 240 only) - please note that the backup utility limits the storage to 2 GB per DVD-RW

Note: To re-use a DVD-RW, refer to procedure Erasing the contents of a CD/DVD on a Sun server on page 167 in this document.

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

Action

Perform the following steps to complete this procedure.

At the Sun server

1 Insert the blank tape or DVD-RW into the drive.

At your workstation

2 Telnet to the server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or hostname of the Sun server on which you are performing the backup

3 When prompted, enter your user ID and password.

4 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

5 When prompted, enter the root password.

If you are using	Do
a tape	step 6
a DVD-RW	step 7

6 Rewind the tape by typing

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

and pressing the Enter key.

7 Backup the data by typing

```
$ /opt/nortel/sspfs/bks/bkdata
```

and pressing the Enter key.

Example response:

```
Backup Completes Successfully
```

If you are using	Do
a tape	step 8
a DVD-RW	step 9

8 Verify the backup on tape was successful as follows:

a List the content of the tape by typing

```
# tar tvf /dev/rmt/0
```

and pressing the Enter key.

Example response:

```
-rw-rw-rw- root/other  1291264 2003-10-01
15:58 oracle.dmp
-rw-rw-rw- root/other     8192 2003-10-01
15:58 critdata.cpio
```

b Remove the tape from the drive, label it, write-protect it, and store it in a safe place.

9 Verify the backup on DVD-RW was successful as follows:

a List the content of the DVD-RW by typing

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

and pressing the Enter key.

Example response:

```
-rw-rw-rw- root/other  1291264 2003-10-01
15:58 oracle.dmp
-rw-rw-rw- root/other     8192 2003-10-01
15:58 critdata.cpio
```

b Remove the DVD-RW from the drive, label it, and store it in a safe place.

10 You have completed this procedure.

Performing a full backup of file systems (SN06.2 or greater)

Application

Use this procedure to perform a full backup of the file systems on a Sun server (t1400 or Netra 240) running the SN06.2 or greater release of the Succession Server Platform Foundation Software (SSPFS).

Note: For system running the SN05 or SN06 release of the SSPFS, use procedure Performing a full backup of file systems (pre-SN06.2) in this document.

Prerequisites

This procedure has the following prerequisites:

- you must be running SSPFS SN06.2 or greater
- you must perform a data backup prior to performing this procedure (refer to procedure Performing a data backup on a Sun server (SN06.2 or greater) on page 212 in this document, if required)

  Note: The data backup is not required prior to this procedure for the Core Billing Manager (CBM) product family.

- you need a blank 4mm Digital Data Storage (DDS-3) tape of 125m and 12 GB to store the data (T1400 only)
- you need one or more blank DVD-RW of 4.7 GB to store the data (Netra 240 only) - please note that the backup utility limits the storage to 2 GB per DVD-RW

  Note: To re-use a DVD-RW, refer to procedure Erasing the contents of a CD/DVD on a Sun server on page 167 in this document.

Action

At the Sun server

1 Insert a blank tape or DVD-RW into the drive.

At your workstation

2 Telnet to the Sun server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the server on which you are performing the backup

3 When prompted, enter your user ID and password.

4 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

5 When prompted, enter the root password.

If you are using	Do
a tape	step 6
a DVD-RW	step 7

6 Rewind the tape by typing

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

and pressing the Enter key.

7 Backup the file systems by typing

```
# /opt/nortel/sspfs/bks/bkfullsys
```

and pressing the Enter key.

Example response:

```
Backup Completed Successfully
```

Note: If you are using DVD-RW, you may be prompted to insert another blank DVD.

If you are using	Do
a tape	step 8
a DVD-RW	step 9

8 Verify the backup to tape was successful as follows:

a List the content of the tape by typing

```
# gtar tvf /dev/rmt/0
```

and pressing the Enter key.

b Eject and remove the tape from the drive, label it, write-protect it, and store it in a safe place.

9 Verify the backup to DVD was successful as follows:

a List the content of the DVD by typing

```
# gtar tvf /cdrom/*bkfullsys*/*.tar
```

and pressing the Enter key.

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

10 You have completed this procedure.

Performing a data restore on a Sun server (SN06.2 or greater)

Application

Use this procedure to restore data from a backup tape or DVD-RW on a Sun server (t1400 or Netra 240) running the SN06.2 or greater release of the Succession Server Platform Foundation Software (SSPFS).

Note 1: For systems running the SN05 or SN06 release of the SSPFS, use procedure Restoring application data to the Oracle database (pre-SN06.2) in this document.

Note 2: The data restore is not required for the Core Billing Manager (CBM) product family.

Prerequisites

This procedure has the following prerequisites:

- you must be running SSPFS SN06.2 or greater
- you need the tape or the DVD-RW on which the data was backed up

Action

Perform the following steps to complete this procedure.

At the Sun server

1 Insert the backup tape or DVD-RW into the drive.

At your workstation

2 Telnet to the server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the Sun server on which you are performing the data restore

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.

6 Stop the server applications that run on the server.

For	Refer to
SESM, SAM21EM and NPM server applications	Enabling or disabling the socks security service on a Sun server Creating or modifying the login greeting message on a Sun server Deleting local user accounts from a Sun server
MG 9000 Manager and mid-tier server applications	the MG9000 Security and Administration document, NN10162-611, if required

7 Restore the database by typing

```
$ /opt/nortel/sspfs/bks/rsdata
```

and pressing the Enter key.

8 Remove the backup tape or the DVD-RW from the drive, and store it in a safe place.

9 Verify that the database is restored properly.

10 Start the server applications that run on the server.

For	Refer to
SESM, SAM21EM and NPM server applications	Configuring the time zone on a Sun server Setting up local user accounts on a Sun server
MG 9000 Manager and mid-tier server applications	the MG9000 Security and Administration document, NN10162-611, if required

11 You have completed this procedure.

Performing a full system restore on a Sun server (SN06.2 or greater)

Application

Use this procedure to perform a full system restore from a backup tape or DVD-RW on a Sun server (t1400 or Netra 240) running the SN06.2 or greater release of the Succession Server Platform Foundation Software (SSPFS).

Note: For systems running the SN05 or SN06 release of the SSPFS, use procedures Restoring root file systems (pre-SN06.2) on page 186 and Restoring non-root file systems (pre-SN06.2) on page 189 in this document.

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

- Simplex configuration (one server) on page 220
- High-availability configuration (two servers) on page 221

Note: Only the Simplex configuration (one server) is applicable to perform a full system restore from tape on a t1400 server.

Prerequisites

This procedure has the following prerequisites:

- you must be running SSPFS SN06.2 or greater
- you need the backup tape or DVD-RW

Action

Perform the following steps to complete this procedure.

Simplex configuration (one server)

At the server console

1 Log in to the Sun 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 SSPFS CD disk#1 into the CD/DVD drive.

4 At the OK prompt, restore the system by typing

```
OK boot cdrom - restore
```

and pressing the Enter key.

5 When prompted, accept the software license restrictions by typing

ok

and pressing the Enter key.

The system reboots.

6 When prompted, insert the backup tape or Volume 1 of the backup DVD-RW into the drive.

The restore process can run for several minutes and may prompt you for additional Volumes that were generated during the full system backup to DVD-RW.

7 Restore the data. Refer to procedure Performing a data restore on a Sun server (SN06.2 or greater) in the ATM/IP Security and Administration document, NN10402-600, if required.

Note: The data restore is not required for the Core Billing Manager (CBM) product family.

8 Once the data restore is complete, reboot the system by typing

init 6

and pressing the Enter key.

9 You have completed this procedure.

High-availability configuration (two servers)

At the console connected to the inactive node

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

2 Bring the system to the OK prompt by typing

init 0

and pressing the Enter key.

At the console connected to the active node

3 Log in to the active node through the console (port A) using the root user ID and password.

4 Bring the system to the OK prompt by typing

init 0

and pressing the Enter key.

5 Insert SSPFS CD disk#1 into the CD/DVD 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 backup DVD-RW into the drive.

The restore process can run for several minutes and may prompt you for additional Volumes that were generated during the full system backup to DVD-RW.

9 Restore the data. Refer to procedure Performing a data restore on a Sun server (SN06.2 or greater) on page 218 in the ATM/IP Security and Administration document, NN10402-600 if required.

Note: The data restore is not required for the Core Billing Manager (CBM) product family.

10 Once the data restore is complete, reboot the system by typing

```
# init 6
```

and press the Enter key.

11 Re-image the inactive node using the active node's image. Refer to procedure "Cloning the image of one node in a cluster to the other node on page 223".

12 You have completed this procedure.

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

Application

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

Prerequisites

This procedure has the following prerequisites:

- you need the root user ID and password
- you may need console access to the Inactive node

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

Action

Perform the following steps to complete this procedure.

At your workstation

1 Telnet to the Active node by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the Active node in the cluster

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 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
APS                               RUNNING
NPM                               RUNNING
```

6 Use the following table to determine your next step.

If	Do
all applications are running	step 9
one or more applications are not running	step 7

7 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

8 Use the following table to determine your next step.

If	Do
one or more applications do not start	contact your next level of support
all applications are running	step 9

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

```
# pse status
```

and pressing the Enter key.

If PSE is	Do
running	step 11
not running	step 10

10 Start the PSE server application by typing

```
# pse start
```

and pressing the Enter key.

If PSE	Do
does not start	contact your next level of support
starts	step 11

11 Use the following table to determine your next step.

If your server is running the	Do
CS 2000 Management Tools software	step 12
MG 9000 software	step 14

12 Verify that the SESMservice application is fully functional by typing

```
# ptmctl status
```

and pressing the Enter key.

Example response:

```
SESM STATUS
-------------------------
COMPONENT                 STATUS
---------                 ------
Proxy Agent               RUNNING
RMI Registry              RUNNING
Snmpfactory               RUNNING
MI2 Server                RUNNING

  Current number of SESM processes running: 4 (of 4)

  SESM APPLICATION STATUS: All Applications ready
```

13 Use the following table to determine your next step.

If the SESMService is	Do
not fully functional	contact your next level of support
fully functional	step 14

14 Start the cloning process by typing

```
# startb
```

and press the Enter key.

If the system	Do
prompts you for the Ethernet address	step 15
indicates it is using Ethernet address <EthernetAddress>	step 20

At the console connected to the inactive node

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

16 Bring the system to the OK prompt by typing

```
# init 0
```

and pressing the Enter key.

17 At the OK prompt, display the Ethernet address of the inactive node 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.
```

18 Take note of the Ethernet address that is displayed.

At your workstation (telnet session to Acive node)

19 Enter the Ethernet address of the inactive node you noted in step 18.

20 Use the following table to determine your next step.

If the system	Do
prompts you to enter the command “boot net - image”	step 21
does not prompt you to enter the command “boot net - image”	step 23

At the console connected to the inactive node

21 Log in to the inactive node through the console (port A) using the root user ID and password if not already logged in.

22 When prompted, boot the inactive node from the image of the active node by typing

```
OK boot net - image
```

and press the Enter key.

Note: 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
```

At your workstation (telnet session to Acive node)

23 Monitor the progress of the cloning from the active node. Cloning the inactive node takes approximately one hour to complete.

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.
Deleted snapshot 0.
Deleted snapshot 1.
Deleted snapshot 2.
Deleted snapshot 3.
d99: Soft Partition is cleared
```

24 You have completed this procedure.

Displaying customer logs on a Sun server

Application

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

- Succession Element and Sub-element Manager (SESM)
- Gateway Controller (GWC)
- Media Gateway 9000 (MG 9000)
- Succession Server Platform Foundation Software (SSPFS)

Customer logs reside in directory /var/log on the server. For details on customer logs, refer to the Succession Fault Management Log Reference document, NN10275-909.

Prerequisites

None

Action

Perform the following steps to complete this procedure.

At your workstation

1 Telnet to the Sun server by typing

```
> telnet <IP address>
```

and pressing the Enter key.

where

IP address
is the IP address of the Sun 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.

Verifying disk space on a Sun server

Application

Use this procedure to verify disk capacity utilization.

Prerequisites

You must have root user privileges.

Action

Perform the following steps to complete this procedure.

At your workstation

1 Telnet to the Sun server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the Sun server that has the file system you want to increase

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

4 When prompted, enter the root password.

5 Access the command line interface by typing

```
# cli
```

and pressing the Enter key.

Example response

```
Command Line Interface
 1 - View
 2 - Configuration
 3 - Other

 X - exit

select -
```

6 Display the current disk capacity utilization as follows:

a Enter the number next to the “View” option in the menu.

Example response

```
View
  1 - sspfs_soft (Display Software
      Installation Level Of SSPFS)
  2 - chk_sspfs (Check SSPFS Processes)
  3 - sw_conf (The software configuration of
      the znc0s0jx)
  4 - cpu_util (Overall CPU utilization)
  5 - cpu_util_proc (CPU utilization by
      process)
  6 - port_util (I/O port utilization)
  7 - disk_util (Filesystem utilization)

  X - exit

select -
```

b Enter the number next to the “disk_util” option in the menu.

Example response

```
=== Executing "disk_util"

Filesystem             kbytes    used   avail capacity  Mounted on
/dev/md/dsk/d2       4129290 1892027 2195971    47%    /
/proc                      0       0       0     0%    /proc
fd                         0       0       0     0%    /dev/fd
mnttab                     0       0       0     0%    /etc/mnttab
/dev/md/dsk/d8       2053605  155600 1836397     8%    /var
swap                 3505488      40 3505448     1%    /var/run
swap                  524288     448  523840     1%    /tmp
/dev/md/dsk/d11      5161437 1428691 3681132    28%    /opt
/dev/md/dsk/d23      2031999   34313 1936727     2%    /PROV_data
/dev/md/dsk/d24      2031999  169042 1801998     9%    /audio_files
/dev/md/dsk/d20      3080022  294615 2723807    10%    /data
/dev/md/dsk/d25       949455  440344  452144    50%    /user_audio_files
/dev/md/dsk/d21      3080022  275962 2742460    10%    /opt/nortel
/dev/md/dsk/d22     12386331 10337214 1925254    85%    /data/oradata
/dev/md/dsk/d26       122847    1041  109522     1%    /data/qca

=== "disk_util" completed successfully
```

7 You have completed this procedure.